EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 16.12.2020
JOIN(2020) 18 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

The EU's Cybersecurity Strategy for the Digital Decade

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

The EU's Cybersecurity Strategy for the Digital Decade

I. INTRODUCTION: A CYBERSECURE DIGITAL TRANSFORMATION IN A COMPLEX THREAT ENVIRONMENT

Cybersecurity is an integral part of Europeans' security. Whether it is connected devices, electricity grids, or banks, aircraft, public administrations or hospitals they use or frequent, people deserve to do so within the assurance that they will be shielded from cyber threats. The EU's economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity. Cybersecurity is therefore essential for building a resilient, green and digital Europe.

Transport, energy and health, telecommunications, finance, security, democratic processes, space and defence are heavily reliant on network and information systems that are increasingly interconnected. Cross-sector interdependences are very strong because networks and information systems, in their turn, depend on a steady supply of electricity to function. Connected devices already outnumber people on the planet, and their number is forecast to rise to 25 billion by 2025[1]: a quarter of these will be in Europe. Digitisation of working patterns has been accelerated by the COVID-19 pandemic, during which 40% of EU workers switched to telework, with likely permanent effects on everyday life[2]. This increases vulnerabilities to cyberattacks[3]. Connected objects are often shipped to the consumer with known vulnerabilities, which further increases the attack surface for malicious cyber activities[4]. The industrial landscape in the EU is increasingly digitised and connected; this also means that cyberattacks can have far greater impact on industries and ecosystems than ever before.

The threat landscape is compounded by geopolitical tensions over the global and open Internet and over control of technologies across the whole supply chain[5]. These tensions are reflected in the increasing number of nation states erecting digital borders. Restrictions of and on the Internet threaten global and open cyberspace, as well as the rule of law,

[1] Estimated by telecommunications trade association GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). The International Data Corporation forecast 42.6 billion connected machines, sensors, and cameras; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] According to a survey in June 2020, 47% of business leaders said they intended to allow employees to work remotely full-time even as it becomes possible to return to the workplace; 82% intended to permit remote working at least some of the time; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] One of the most damaging malware to date, known as Mirai, created botnets of over 600 000 devices that disrupted multiple major websites in Europe and the United States.

[5] Including electronic components, data analytics, cloud, faster and smarter networks with 5G and beyond, encryption, Artificial Intelligence (AI), and new computing and trusted data processing paradigms such as blockchain, cloud-to-edge and quantum computing.

fundamental rights, freedom and democracy – the core values of the EU. Cyberspace is increasingly exploited for political and ideological purposes, and increased polarisation at international level is hindering effective multilateralism. Hybrid threats combine disinformation campaigns with cyberattacks on infrastructure, economic processes and democratic institutions, with the potential for causing physical damage, obtaining unlawful access to personal data, stealing industrial or state secrets, sowing mistrust and weakening social cohesion. These activities undermine international security and stability and the benefits that cyberspace brings for economic, social and political development.

The malicious targeting of critical infrastructure is a major global risk[6]. The Internet has a decentralised architecture with no central structure and a multi-stakeholder governance. It has managed to sustain exponential increases in traffic volumes while being a constant target for malicious attempts at disruption[7]. At the same time, there is increased reliance on the core functions of the global and open Internet, such as the Domain Name System (DNS), and essential Internet services for communications and hosting, applications and data. These services are more and more concentrated in the hands of a few private companies[8]. This leaves the European economy and society vulnerable to disruptive geopolitical or technical events which affect the core of the Internet or one or more of these companies. The increased internet usage and changing patterns due to the pandemic have further exposed the fragility of supply chains that depend on this digital infrastructure.

Concerns about security are a major disincentive to using online services[9]**.** Around two-fifths of EU users have experienced security-related problems and three-fifths feel unable to protect themselves against cybercrime[10]. One-third have received fraudulent e-mails or phone calls asking for personal details in the past three years, but 83% have never reported a cybercrime. One in eight businesses have been affected by cyberattacks[11]. Over half of business and consumer personal computers that have been infected with malware once are re-infected within the same year[12]. Hundreds of millions of records are lost each year through data breaches; the average cost of a breach to a single business rose to over €3.5 million in

[6] World Economic Forum, Global Risks Report 2020.

[7] The pandemic led to a 60% increase in internet traffic according to the Organisation for Economic Cooperation and Development; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. The Body of European Regulators for Electronic Communications and the Commission regularly publish reports on the status of internet capacity during coronavirus confinement measures. According to a report by ENISA, there was a 241% increase in total number of Distributed Denial of Service (DDoS) attacks during Q3 2019 compared with Q3 2018. DDoS attacks are increasing in intensity, with the biggest attack ever occurring in February 2020 and reaching a peak traffic of 2.3 terabits per second. In the 'CenturyLink outage' in August 2020, a routing problem in the US Internet Service Provider led to a 3.5% drop in global web traffic; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

[8] Internet Society, The Global Internet Report: Consolidation in the Internet Economy; https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[10] 2020 Digital Economy and Society Index; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[11] Eurostat Press release, 'ICT security measures taken by vast majority of enterprises in the EU', 6/2020 - 13 January 2020. 'Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation'; WEF, The Global Risks Report 2020.

[12] Source: Comparitech.

2018[13]. The impact of a cyberattack often cannot be isolated, and can trigger chain reactions throughout the economy and society, affecting millions of individuals[14].

The investigation of nearly all types of crime has a digital component. In 2019, the number of year-on-year incidents was reported to have trebled. There are an estimated 700 million new samples of malware – the most frequent means of furthering a cyberattack[15]. The annual cost of cybercrime to the global economy in 2020 is estimated to be €5.5 trillion, double that of 2015[16]. This represents the largest transfer of economic wealth in history, greater than the global drugs trade. For one major incident, the WannaCry ransomware attack in 2017, the cost to the global economy was estimated at over €6.5 billion[17].

Digital services and the finance sector are among the most frequent targets of cyberattacks, along with the public sector and manufacturing, yet cyber readiness and awareness among businesses and individuals remain low[18], and there is a major shortage of cybersecurity skills in the workforce[19]. There were almost 450 cybersecurity incidents in 2019 involving European critical infrastructures like finance and energy[20]. Healthcare organisations and professionals have been hit especially hard during the pandemic. As technology becomes inextricable from the physical world, cyberattacks put lives and the wellbeing of the most vulnerable at risk[21]. Over two-thirds of companies, in particular SMEs, are considered 'novices' in cybersecurity, and European companies are considered less well prepared than companies in Asia and America[22]. An estimated 291 000 posts for cybersecurity professionals in Europe remain unfilled. Hiring and training cybersecurity experts is a slow process leading to greater cybersecurity risks for organisations[23].

The EU lacks collective situational awareness of cyber threats. This is because national authorities do not systematically gather and share information - such as that available from the private sector - which could help assess the state of cybersecurity in the EU. Only a fraction of incidents are reported by Member States, and information sharing is neither

[13] Annual Cost of a Data Breach Report, 2020 Ponemon Institute, and based on quantitative analysis of 524 recent breaches across 17 geographies and 17 industries; https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[14] Report from Joint Research Centre (JRC), 'Cybersecurity, our digital anchor'; https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

[15] Source: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] JRC, Cybersecurity – Our Digital Anchor.

[17] Source: Cyence.

[18] Business awareness remains low also with respect to the cyber-theft of trade secrets, especially among SMEs; PwC, Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets, 2018.

[19] See ENISA Threat Landscape 2020. Also, Verizon Data Breach Investigations Report 2020; https://enterprise.verizon.com/resources/reports/dbir/

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

[21] Ransomware has been used to target hospitals and health records, e.g. Romania (June 2020), Düsseldorf (September 2020) and Vastaamo (October 2020).

[22] PwC, The Global State of Information Security 2018; ESI Thoughtlab, The Cybersecurity Imperative, 2019.

[23] EU Agency for Cybersecurity, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database, December 2019.

systematic nor comprehensive[24]; cyberattacks may be only one facet of concerted malicious attacks against European societies. There is currently only limited mutual operational assistance between Member States, and no operational mechanism is in place between Member States and EU institutions, agencies and bodies, in the event of a large-scale, cross-border cyber incidents or crisis[25].

Improving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information. Cybersecurity is indispensable to the network connectivity and the global and open Internet that must underpin the transformation of the economy and society in the 2020s. It contributes to better and more jobs, more flexible workplaces, more efficient and sustainable transport and farming, and easier and fairer access to health services. It is also essential for the transition to cleaner energy under the European Green Deal[26], through cross-border grids and smart meters and avoiding unnecessary duplication of data storage. Lastly, it is essential to international security and stability and the development of economies, democracies and societies globally. Governments, businesses and individuals need therefore to use digital tools in a responsible, security-conscious manner. Cybersecurity awareness and hygiene must underpin the digital transformation of everyday activities.

The EU's new Cybersecurity Strategy for the Digital Decade forms a key component of Shaping Europe's Digital Future[27], the Commission's Recovery Plan for Europe[28], the Security Union Strategy 2020-2025[29], the Global Strategy for the EU's Foreign and Security Policy[30], and the European Council Strategic Agenda 2019-2024[31]. It sets out how the EU will shield its people, businesses and institutions from cyber threats, and how it will advance international cooperation and lead in securing a global and open Internet.

II. THINKING GLOBAL, ACTING EUROPEAN

This strategy aims to ensure a global and open Internet with strong guardrails to address the risks to the security and fundamental rights and freedoms of people in Europe. Following the progress achieved under the previous strategies, it contains concrete proposals for deploying **three principal instruments –regulatory, investment and policy instruments –** to address **three areas of EU action – (1) resilience, technological sovereignty and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing a global and open cyberspace.** The EU is committed to supporting this strategy through an **unprecedented level of investment in the EU's digital transition over the next seven**

[24] Member States are required to provide an annual summary report to the Cooperation Group on the notifications received under Article 10(3) of the Directive on security of network and information systems (Directive (EU) 2016/1148).
[25] Standard Operating Procedures are in place for mutual assistance among members of the CSIRTs Network.
[26] The European Green Deal, COM(2019) 640 final.
[27] Shaping Europe's Digital Future, COM(2020) 67 final.
[28] Europe's moment: Repair and Prepare for the Next Generation, COM (2020) 98 final.
[29] The EU Security Union Strategy 2020-2025, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#

years – potentially quadrupling previous levels – as part of new technological and industrial policies and the recovery agenda[32].

Cybersecurity must be integrated into all these digital investments, particularly key technologies like Artificial Intelligence (AI), encryption and quantum computing, using incentives, obligations and benchmarks. This can stimulate the growth of the European cybersecurity industry and provide the certainty needed to ease the phasing out of legacy systems. The European Defence Fund (EDF) will support European cyber defence solutions, as part of the European defence technological and industrial base. Cybersecurity is included in external financial instruments to support our partners, notably the Neighbourhood, Development and International Cooperation Instrument. Preventing the misuse of technologies, protecting critical infrastructure and ensuring the integrity of supply chains also enables the EU's adherence to the UN norms, rules and principles of responsible state behaviour[33].

1. RESILIENCE, TECHNOLOGICAL SOVEREIGNTY AND LEADERSHIP

The EU's critical infrastructure and essential services are increasingly interdependent and digitised. All Internet-connected things in the EU, whether automated cars, industrial control systems or home appliances, and the whole supply chains which make them available, need to be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered. This is fundamental to provide the EU's private and public sector with the possibility to choose from the most secure infrastructures and services. The upcoming decade is the EU's opportunity to lead in the development of secure technologies across the whole supply chain. Ensuring resilience and stronger industrial and technology capacities in cybersecurity should mobilise all necessary regulatory, investment and policy instruments. Cybersecurity by design for industrial processes, operations and devices can mitigate risks, potentially reduce costs to companies as well as to wider society, and thereby increase resilience.

1.1 Resilient infrastructure and critical services

EU **rules on the security of Network and Information Systems (NIS)** are at the core of the Single Market for cybersecurity. The Commission proposes to reform these rules under a revised NIS Directive to increase the level of **cyber resilience of all relevant sectors, public and private, that perform an important function for the economy and society[34].** The review is necessary to reduce inconsistencies across the internal market by aligning scope, security and incident reporting requirements, national supervision and enforcement and the capabilities of competent authorities.

A reformed NIS Directive will provide the basis for more specific rules that are also necessary for strategically important sectors, including energy, transport and health. In order to ensure a consistent approach as announced under the Security Union Strategy 2020-2025,

[32] Investments in the whole digital technology supply chain, contributing to the digital transition or to addressing the challenges resulting from it, should amount to at least 20% - equivalent to €134.5 billion - of the €672.5 billion Recovery and Resilience Facility, consisting of grants and loans. EU funding in the 2021-2027 Multiannual Financial Framework envisaged for cybersecurity under the Digital Europe Programme, and for cybersecurity research under Horizon Europe, with special focus on support for SMEs, could amount to €2 billion overall, plus Member States and industry investment.

[33] https://undocs.org/A/70/174

[34] [*insert reference to NIS proposal*]

the reformed Directive is proposed together with a review of the legislation on the resilience of critical infrastructure[35]. Energy technologies embedding digital components and the security of the associated supply chains are important for the continuity of essential services and for the strategic control of critical energy infrastructure. The Commission will therefore propose measures, including a 'network code' setting rules for cybersecurity in cross-border electricity flows for adoption by end 2022. The financial sector must also strengthen digital operational resilience and ensure an ability to withstand all types of ICT-related disruptions and threats, as the Commission has proposed[36]. In transport, the Commission added provisions on cybersecurity[37] to the EU legislation on aviation security and will continue its efforts to enhance cyber resilience across all transport modes. Strengthening the cyber resilience of **democratic processes and institutions** is a core component of the European Democracy Action Plan for safeguarding and promoting free elections, and democratic discourse and media plurality[38]. Finally, for the security of infrastructure and services under the future Space Programme, the Commission will continue to proceed with a deepening of the Galileo cybersecurity strategy for the next generation of Global Navigation Satellite System services, and other new components of the Space Programme[39].

1.2 Building a European Cyber Shield

With the spread of connectivity and the growing sophistication of cyberattacks, Information Sharing and Analysis Centres, or ISACs, perform a valuable function, including at the sectoral level, in allowing information exchange between multiple stakeholders on cyber threats[40]. In addition to this, networks and computer systems require constant monitoring and analysis to detect intrusions and anomalies in real time. Many private companies, public organisations and national authorities have therefore set up Computer Security Incident Response Teams (CSIRTs) and Security Operations Centres, or 'SOCs'.

Security Operations Centres are vital for collecting logs[41] and isolating suspicious events occurring on the communication networks they monitor. They do this through signal and pattern identification and threat knowledge extraction from the large quantities of data that need to be assessed. They have contributed to the detection of the activities of malicious executables and in turn helped contain cyberattacks. The work required in these centres is highly demanding and fast-paced, which is why AI and in particular machine learning techniques can provide invaluable support to practitioners[42].

---

[35] [insert reference to *proposal* for a directive on resilience of critical entities]
[36] Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM/2020/595 final.
[37] Commission Implementing Regulation 2019/1583.
[38] Communication on the European Democracy Action Plan COM(2020) 790. Under the plan, the European Cooperation Network on Elections, Member State election networks will support the deployment of joint expert teams to counter threats – including cyberthreats - to electoral processes; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en
[39] This includes new governmental satellite communications initiative (GOVSATCOM) and Space Debris (SST)
[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[41] In such a manner that law enforcement and the judiciary can use them as evidence.
[42] Source: survey by Ponemon Institute Research, 'Improving the Effectiveness of the SOC, 2019'; for studies on the use of AI in Security Operation Centres see for example: Khraisat, A., Gondal, I., Vamplew, P. *et al.* Survey of intrusion detection systems: techniques, datasets and challenges, *Cybersecur* 2**,** 20 (2019).

The Commission proposes to build a **network of Security Operations Centres across the EU**[43], and to support the improvement of existing centres and the establishment of new ones. It will also support the training and skill development of staff operating these centres. It could commit, on the basis of a needs analysis conducted with relevant stakeholders and supported by the EU Agency for Cybersecurity (ENISA), over EUR 300 million to support public-private and cross-border cooperation in creating national and sectoral networks, involving also SMEs, based on appropriate governance, data sharing and security provisions.

Member States are encouraged to co-invest in this project. The centres would then be able to more efficiently share and correlate the signals detected and create high-quality threat intelligence to be shared with ISACs and national authorities, and thus enabling a fuller situational awareness. The goal would be to connect, in phases, as many centres as possible across the EU to create collective knowledge and share best practices. Support will be made available to these centres to improve incident detection, analysis and response speeds through state-of-the-art AI and machine learning capabilities and complemented by supercomputing infrastructure developed in the EU by the European High-Performance Computing Joint Undertaking[44].

Through sustained collaboration and cooperation, this network will provide timely warnings on cybersecurity incidents to authorities and all interested stakeholders, including the Joint Cyber Unit (see section 2.1). **It will serve as a real cybersecurity shield for the EU**, providing a solid mesh of watchtowers, able to detect potential threats before they can cause large-scale damage.

1.3 An ultra-secure communication infrastructure

The European Union Governmental Satellite Communications[45], a component of the Space Programme, will provide secure and cost-efficient space- based communication capabilities to ensure the security- and safety- critical missions and operations managed by the EU and its Member States, including national security actors and EU institutions bodies and agencies.

Member States have committed to working together with the Commission towards the deployment of a secure quantum communication infrastructure (QCI) for Europe[46]. The QCI will 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. It will have two main components: existing terrestrial fibre communication networks linking strategic sites at national and cross-border levels; and linked space satellites covering the whole EU, including its overseas territories[47]. This initiative to develop and

[43]More detailed arrangements for governance, operation principles and funding of these Centres, and how they will complement existing structures such as Digital Innovation Hubs, will be developed.
[44]https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking
[45]GOVSATCOM is a component of the Space Programme of the Union
[46]The EuroQCI Declaration has been signed by most Member States and development and infrastructure deployment are to take place in 2021-2027, with funding from Horizon Europe and Digital Europe, and the European Space Agency, subject to appropriate governance arrangements; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network
[47]The development of a space component is necessary to achieve long distance point-to-point connections (>1000 km) that ground-based infrastructure cannot support. By exploiting the properties of quantum mechanics, the QCI will initially enable parties to securely share random secret keys to be used to encrypt and decrypt messages. It will also incorporate the deployment of a testing and compliance infrastructure, for assessing the compliance of European quantum communication devices and systems with the QCI infrastructure

deploy new and more secure forms of encryption, and to devise new ways of protecting critical communication and data assets, can help keep sensitive information and, in turn, critical infrastructures safe.

In this perspective, and going further, the Commission will explore the possible deployment of a multi-orbital secure connectivity system. Building on GOVSATCOM and QCI, it would integrate cutting edge technologies (Quantum, 5G, AI, edge computing) adhering to the most restrictive cybersecurity framework in order to support secure-by-design services such as reliable, secure and cost-effective connectivity and encrypted communication for critical governmental activities.

1.4 Securing the next generation of broadband mobile networks

EU citizens and companies using advanced and innovative applications enabled by **5G and future generations of networks** should benefit from the highest security standard. Member States, together with the Commission and with the support of ENISA, have established with the EU 5G Toolbox[48] of January 2020 a comprehensive and objective risk-based approach to 5G cybersecurity that is based on an assessment of possible mitigation plans and identification of the most effective measures. Moreover, the EU is consolidating its capabilities in 5G and beyond to avoid dependencies and to foster a sustainable and diverse supply chain.

In December 2020, the Commission published a report on the impacts of the Recommendation of 26 March 2019 on the Cybersecurity of 5G networks[49]. It showed that considerable progress has been made since the Toolbox was agreed, and that most Member States are on track to complete a significant part of the Toolbox implementation in the near future, albeit with some variations and remaining gaps as already identified in the Progress report published in July 2020[50].

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'[51].

Looking forward, the EU and its Member States should ensure that the identified risks have been mitigated adequately and in a coordinated way, in particular as regards the objective of minimising the exposure to high risk suppliers and of avoiding dependency on these suppliers at national and Union level, and that any new significant development, or risk, is taken into account. Member States are invited to make full use of the Toolbox in their investments in digital capacities and connectivity.

Based on the report of the impacts of the 2019 Recommendation, the Commission encourages Member States to accelerate the work towards completing the implementation of the main

---

and their certification and validation before their integration in the QCI. It will be designed to support additional applications as they reach the necessary technological maturity level. The current OpenQKD pilot (https://openqkd.eu/) is a precursor to this testing and compliance infrastructure.

[48]Communication on Secure 5G deployment in the EU - Implementing the EU Toolbox, COM(2020) 50.

[49]Commission Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks, 15 December 2020.

[50]Report by the NIS Cooperation Group on the implementation of the Toolbox, of 24 July 2020.

[51]EUCO 13/20, Special meeting of the European Council (1 and 2 October 2020) – Conclusions.

Toolbox measures by the second quarter of 2021. It also calls on Member States to continue monitoring together progress made and ensuring further alignment of approaches. At EU level, three main objectives will be pursued in order to support this process: ensuring further convergence in risk mitigation approaches across the EU, supporting continuous exchange of knowledge and capacity building, and promoting supply chain resilience and other EU strategic security objectives. Concrete actions related to these key objectives are set out in the dedicated Appendix to this Communication.

The Commission will continue to work closely with Member States to fulfil these objectives and actions with the support of ENISA (see Annex).

The EU's 5G Toolbox approach has, moreover, raised interest in non-EU countries currently developing their approaches securing their communications networks. The Commission services together with the European External Action Service and the network of EU delegations, stands ready to provide additional information if requested on its comprehensive, objective and risk-based approach to authorities around the world.

1.5 An Internet of Secure Things

Every connected thing contains vulnerabilities that can be exploited with potentially widespread ramifications. Internal Market rules include safeguards against insecure products and services. The Commission is already working to ensure **transparent security solutions and certification under the Cybersecurity Act** and to incentivise safe products and services without compromising on performance[52]. It will adopt its first Union Rolling Work Programme in the first quarter of 2021 (to be updated at least once every three years) to allow industry, national authorities and standardisation bodies to prepare in advance for future European cybersecurity certification schemes[53]. As the Internet of Things proliferates, enforceable rules require strengthening, both to ensure overall resilience and boost to cybersecurity.

The Commission will 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**[54]. Such rules could include a **new duty of care for connected device manufacturers** to address software vulnerabilities including the continuation of software and security updates as well as ensuring, at the end of life, deletion of personal and other sensitive data. These rules would bolster 'the right-to-repair obsolete software" initiative presented in the Circular Economy Action Plan and complement ongoing measures which address specific types of products, such as mandatory requirements to be proposed for market access of certain wireless products **(**through the adoption of a delegated

[52] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 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). The Cybersecurity Act promotes ICT certification at EU level, with a European Cybersecurity Certification Framework for the establishment of voluntary European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as reducing the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union. In parallel, cybersecurity 'ratings' companies tend to be based outside the EU with limited transparency and oversight; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[53] Required by Article 47(5) of the Cybersecurity Act.

[54] Council Conclusions call for horizontal measures on the cybersecurity of connected devices; 13629/20, 2 December 2020.

act under the Radio Equipment Directive[55]), and the objective to implement cybersecurity rules for motor vehicles for all new vehicle types as from July 2022[56]. They would, moreover, build on the proposed revision of general product safety rules, which do not directly address cybersecurity aspects[57].

1.6 Greater global Internet security

A set of core protocols and supporting infrastructure ensures the functionality and integrity of the Internet worldwide[58]. This set includes the DNS and its hierarchical and delegated system of zones, starting, at the top of the hierarchy, with the root zone and the thirteen DNS root servers[59] on which the World Wide Web depends. The Commission intends to develop **a contingency plan, supported by EU funding, for dealing with extreme scenarios affecting the integrity and availability of the global DNS root system**. It will work with ENISA, the Member States, the two EU DNS root server operators[60] and the multi-stakeholder community, to assess the role of these operators in guaranteeing that the Internet remains globally accessible in all circumstances.

For a client to access a resource under a particular domain name on the Internet, its request (typically for a Uniform Resource Locator, or URL) needs to be translated or 'resolved' into an IP address, through reference to DNS name servers. However, people and organisations in the EU increasingly rely on a few public DNS resolvers operated by non-EU entities. Such consolidation of DNS resolution in the hands of few companies[61] renders the resolution process itself vulnerable in case of significant events affecting one major provider, and makes it more difficult for EU authorities to address possible malicious cyberattacks and major geopolitical and technical incidents[62].

With a view to reducing security issues related to market concentration, the Commission will encourage relevant stakeholders including EU companies, Internet Service Providers and browser vendors to adopt a DNS resolution diversification strategy. The Commission also intends to contribute to secure Internet connectivity by supporting the development of a public **European DNS resolver service.** This 'DNS4EU' initiative will offer an alternative, European service for accessing the global Internet. DNS4EU will be transparent, conform to

[55]Directive 2014/53/EU

[56] Follows the UN Regulation adopted in June 2020; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[57] Revision of current general product safety rules (Directive 2001/95/EC); proposed adapted rules are also planned on liability of producers in the digital context within the scope of the EU liability regulatory framework.

[58]'The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. ENISA should support the security of the public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular DNS, BGP, and IPv6), the operation of the domain name system (such as the operation of all top-level domains), and the operation of the root zone'; Recital 23 Cybersecurity Act.

[59]https://www.iana.org/domains/root/servers

[60]The i.root-servers operated by Netnod in Sweden and k.root-servers operated by RIPE NCC in the Netherlands.

[61]Consolidation in the DNS resolver market – how much, how fast how dangerous? (), Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services ( )

[62] There is also evidence showing that DNS data can be used for profiling purposes, with an impact on privacy and data protection rights.

the latest security, data protection and privacy by design and by default standards and rules and form part of the European Industrial Alliance for Data and Cloud[63].

The Commission will also, in liaison with Member States and industry, **accelerate the uptake of key internet standards including IPv6**[64] **and well-established internet security standards and good practices for DNS, routing, and email security**[65], not excluding regulatory measures like a European sunset clause for IPv4 to steer the market if there is insufficient progress towards their adoption. The EU should promote (as for example under the EU-Africa Strategy[66]) the implementation of these standards in partner countries as a way to support the development of the global and open Internet and to counteract closed and control-based models of the Internet. Finally, the Commission will consider the need for a mechanism for more systematic monitoring and gathering of aggregated data on Internet traffic and for advising on potential disruptions[67].

1.7 A reinforced presence on the technology supply chain

With its planned financial support for cyber-secure digital transformation over the 2021-2027 Multiannual Financial Framework, the EU has the unique opportunity to pool its assets to propel its Industry Strategy[68] 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. Public sector intervention should rely on the tools provided by the EU public procurement regulatory framework and Important Projects of Common European Interest. Beyond this, it can unlock private investments through public-private partnerships (including building on the experience of the contractual public private partnership on cybersecurity and its implementation through the European Cyber Security Organisation), venture capital in support of SMEs or industrial alliances and strategies on technology capacities.

Special focus will be put also on the Technical Support Instrument[69] and best use of the latest cybersecurity tools by SMEs - especially those not falling under the scope of the revised NIS Directive - including through dedicated activities under the Digital Innovation Hubs in the Digital Europe Programme. The objective is to trigger a similar amount of investments by the Member States, to be matched by industry under a partnership co-governed with Member States in the proposed **Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN)**. The CCCN should play a key role, with input from industry and academic communities, in developing the EU's technological sovereignty in cybersecurity, building capacity to secure sensitive infrastructures such as 5G, and reduce dependence on other parts of the globe for the most crucial technologies.

---

[63] Joint Declaration: Building the next generation cloud for businesses and the public sector in the EU; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[64] IPv6 deployment is more advanced now with the severe depletion of supply and rise in cost of IPv4 addresses. However, IPv6 deployment is uneven across the EU.

[65] Such standards include DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE and routing norms and good practices e.g. Mutually Agreed Norms for Routing Security (MANRS).

[66] Joint Communication Towards a comprehensive strategy with Africa, 9.3.2020 JOIN(2020) 4 final.

[67] Such an 'Internet Observatory' could be within scope of activities of the European Cybersecurity Industrial, Technology and Research Competence Centre; Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, COM(2018) 630 final.

[68] Communication on a New Industrial Strategy for Europe, COM/2020/102 final.

[69] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:0409:FIN .

The Commission intends to support, potentially with the CCCN, the development of a dedicated cybersecurity Masters programme, and contribute to a common European Cybersecurity Research and Innovation Roadmap beyond 2020. Investments through the CCCN would also build on the cooperation in research and development performed by networks of cybersecurity excellence centres, bringing together Europe's best research teams with industry to design and implement common research agendas, in line with the European Cyber Security Organisation roadmap[70]. The Commission will continue to rely on the research work done by ENISA and Europol, and will also continue supporting, as part of Horizon Europe, individual Internet innovators developing privacy-enhancing and secure communication technologies based on open source software and hardware, as currently under the Next Generation Internet initiative.

1.8 A Cyber-skilled EU workforce

The EU's efforts to upskill the workforce, to develop, attract and retain the best cybersecurity talent and to invest in world class research and innovation, form an important component of protecting against cyber threats generally. This field offers great potential. Hence specific attention must be paid to developing, attracting and retaining more diverse talent. The Revised Digital Education Action Plan will raise cybersecurity awareness among individuals, especially children and young people, and organisations, especially SMEs[71]. It will also encourage women's participation in science, technology, engineering, and mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills. In addition, the Commission will, together with the EU Intellectual Property Office at Europol, ENISA, Member States and the private sector, develop awareness tools and guidance to increase the resilience of EU businesses **against cyber-enabled intellectual property theft**[72].

Education – including Vocational Education and Training (VET), awareness and exercises - should also further increase cybersecurity and cyber defence skills at EU level. To this end, the relevant EU actors such as the ENISA, the European Defence Agency (EDA), the European Security and Defence College (ESDC)[73] should seek synergies between their respective activities.

Strategic initiatives

The EU should ensure:

- Adoption of revised NIS Directive;
- Regulatory measures for an Internet of Secure Things
- Through the CCCN investment in cybersecurity (notably through the Digital Europe Programme, Horizon Europe and recovery facility) to reach up to €4.5 billion in public and private investments over 2021-2027;
- An EU network of AI-enabled Security Operation Centres and an ultra-secure communication infrastructure harnessing quantum technologies;

[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[72] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2187
[73] Through the Cyber Education Training Exercise and Evaluation Platform (ETEE).

- Widespread adoption of cybersecurity technologies through dedicated support to SMEs under the Digital Innovation Hubs;
- Development of an EU DNS resolver service as a safe and open alternative for EU citizens, businesses and public administration to access the Internet; and
- Completion of the implementation of the 5G Toolbox by the second quarter of 2021(see Annex).

2. BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND

Cyber incidents, whether accidental or the deliberate action of criminals, state and other non-state actors, can cause enormous damage. Their scale and complexity, often involving the exploitation of third-party services, hardware, and software to compromise a final target, make the EU's collective threat environment hard to counter without systematic and comprehensive information sharing and cooperation on a common response. The EU aims, **through the full implementation of regulatory tools, mobilisation and cooperation**, to support Member States in defending their citizens, as well as their economic and national security interests, in full respect of fundamental rights and freedoms and the rule of law. Several communities, composed of networks, EU institutions, bodies and agencies, as well as Member State authorities, are responsible for preventing, discouraging, deterring and responding to cyber threat, using their respective instruments and initiatives[74]. These communities include: (i) NIS authorities, such as CSIRTs, and disaster response; (ii) law enforcement and judicial authorities; (iii) cyber diplomacy; and (iv) cyber defence.

2.1 A Joint Cyber Unit

A Joint Cyber Unit would serve as a virtual and physical platform for cooperation for the different cybersecurity communities in the EU, with a focus on operational and technical coordination against major cross border cyber incidents and threats**.**

The Joint Cyber Unit would be an important step forward towards completing the **European cybersecurity crisis management framework**. As outlined in the Commission President's Political Guidelines[75], the Unit should enable Member States and EU institutions, bodies and agencies to make full use of existing structures, resources and capabilities and promote a '**need-to-share**' mind-set. It would provide the means to consolidate the progress made so far in the implementation of the 2017 Recommendation on a coordinated response to large-scale cybersecurity incidents and crises ('Blueprint')[76]. It would also provide the opportunity to

[74]Including the European Union Agency for Cybersecurity (ENISA) support to operational cooperation and crisis management; the CSIRTs network; the Cyber Crises Liaison Organisation Network (CyCLONe, to become EU-CyCLONe as proposed under the revised NIS Directive); the NIS Cooperation Group; 'rescEU'; the European Cybercrime Centre and the Joint Cybercrime Action Task Force at Europol and the Law Enforcement Emergency Response Protocol; the EU Intelligence and Situation Centre (EU INTCEN) and the Cyber Diplomacy Toolbox); the Single Intelligence Analysis Capacity (SIAC); the cyber projects under the Permanent Structured Cooperation (PESCO), notably the 'Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity' (CRRT).

[75]'A Union that strives for more: My agenda for Europe', Political guidelines for the next European Commission 2019-2024 by candidate for President of the European Commission Ursula von der Leyen.

[76]Blueprint Recommendation C(2017) 6100 final of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.

further reinforce the cooperation around the Blueprint architecture and harness the progress achieved notably within the NIS Cooperation Group and the CyCLONe Network.

This could address **two main gaps** that currently increase vulnerabilities and create inefficiencies in the response to cross-border threats and incidents affecting the Union. Firstly, civilian, diplomatic, law enforcement and defence cybersecurity **communities** do not yet have a common space to nurture structured cooperation and facilitate operational and technical cooperation. Secondly, relevant cybersecurity stakeholders have not yet been able to tap into the full **potential** of operational cooperation and mutual assistance within existing networks and communities. This includes the absence of a platform allowing for operational cooperation with the private sector. The Unit should improve and accelerate coordination and allow the EU to face up and respond to large-scale cyber incidents and crises.

The Joint Cyber Unit would not be an additional, standalone body, nor would it affect the competences and powers of national cybersecurity authorities or EU participants. Rather, the Unit would act as a backstop where the participants can draw on one another's support and expertise, especially in the event that various cyber communities are required to work closely together. At the same time, recent events show the necessity for the EU to step up its level of ambition and readiness to face the cyber threats landscape and realities. As part of their contribution to the JCU, the EU actors (Commission and EU agencies and bodies) will therefore be ready to increase significantly their resources and capabilities, so as to level up their preparedness and resilience.

The Joint Cyber Unit would fulfil three main objectives. Firstly, it would ensure **preparedness** across cybersecurity communities; secondly, through information sharing it would provide continuous shared situational **awareness**; thirdly, it would reinforce coordinated **response** and recovery. To achieve these objectives, the Unit should build on well-defined **blocks and goals**, such as guaranteeing **secure and rapid information sharing**, improving **cooperation** among participants, including interaction between Member States and relevant EU entities, establishing structured **partnerships with a trusted industry** base and facilitating a coordinated approach to **cooperation with external partners**. In order to do so, based on a mapping of available capabilities at national and EU level, the Unit could facilitate the development of a cooperation framework.

For the Joint Cyber Unit to become the heart of EU cybersecurity operational cooperation, the Commission will work with Member States and relevant EU institutions, bodies and agencies, including ENISA, CERT-EU and Europol, to promote an **incremental and inclusive approach**, in full respect of competences and mandates of all those involved. In line with this approach, the Unit could contribute to further cooperation between constituents of a specific cyber community, where those constituents deem it necessary.

Four main steps are proposed to deliver the Joint Cyber Unit:

- *Define*, by mapping available capabilities at national and EU level;
- *Prepare*, by establishing a framework for structured cooperation and assistance;
- *Deploy*, by implementing the framework drawing on resources provided by participants so that the Joint Cyber Unit becomes operational;
- *Expand*, by strengthening coordinated response capacity with input from industry and partners.

Building on the outcome of the consultation with Member States, EU institutions, bodies and agencies[77], the Commission, with the involvement of the High Representative, in line with his competences, will by February 2021 present the process, milestones and timeline for **defining, preparing, deploying and expanding the Joint Cyber Unit**.

2.2 Tackling cybercrime

Our dependence on online tools has exponentially increased the attack surface for cyber criminals, and led to a situation where the investigation of nearly all types of crime has a digital component. Furthermore, core parts of our society are threatened by cyber actors and by those using cyber tools to plan and execute their illegal actions. There are therefore close links to the EU's overall security policy, as reflected in the cyber elements in its 2020 Security Union Strategy and in the EU's Counter-Terrorism Agenda[78].

Tackling cybercrime effectively is a key factor in ensuring cybersecurity: deterrence cannot be achieved through resilience alone but also requires identification and prosecution of offenders. It is therefore essential to foster the cooperation and exchange between cybersecurity actors and law enforcement. At EU level, therefore, Europol and ENISA have already built strong cooperation where they have organised joint conferences and workshops and provided joint reports to the Commission, Member States and other stakeholders on cybersecurity threats and technological challenges. The Commission will continue to support this integrated approach to ensure a coherent and effective response, based on a comprehensive information picture.

As one important element of that response, EU and national authorities need to expand and improve the capacity of law enforcement to investigate cybercrime, fully respecting fundamental rights and pursuing the required balance between various rights and interests. The EU should be able to tackle cybercrime through fully implemented legislation that is fit-for-purpose, with a particular focus on combating child sexual abuse online, and on digital investigations, including criminality on the 'darknet'. Law enforcement must be fully equipped for digital investigations. The Commission will therefore put forward an action plan to improve digital capacity for law enforcement agencies, by providing them with the necessary skills and tools. In addition, Europol will further develop its role as a centre of expertise to support national law enforcement authorities combatting cyber-enabled and cyber-dependent crime, contributing to the definition of common forensic standards (through Europol's Innovation Lab and Hub).All these activities require appropriate take-up by Member States, which are encouraged to make use of the Internal Security Fund's national programmes and to propose projects in response to calls for proposals as part of the Thematic Facility.

The Commission will use all appropriate means, including infringement proceedings, to ensure that the 2013 Directive on attacks against information systems[79] is fully transposed and implemented, including the provision of statistics by Member States. It will better prevent the abuse of domain names, including where appropriate for the distribution of illegal

[77]Consultation of Member States (including during the Blue OLEx20 exercise gathering the heads of national cybersecurity authorities), EU institutions, bodies and agencies conducted between July-November 2020.
[78]Communication A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9.12.2020, COM(2020) 795 final..
[79]Directive 2013/40/EU on attacks against information systems.

content, and pursue the availability of accurate registration data by continuing to engage with the Internet Corporation for Assigned Names and Numbers (ICANN) and other stakeholders in the internet governance system, notably through the Public Safety Working Group of ICANN's Governmental Advisory Committee. The proposal in the revised NIS Directive accordingly envisages the maintaining of accurate and complete databases of domain names and registration data, or 'WHOIS data', and providing lawful access to such data as essential to ensuring the security, stability and resilience of the DNS.

The Commission will also continue to work to provide appropriate channels and clarify rules to obtain cross-border access to electronic evidence for criminal investigations (needed in 85% of investigations, with 65% of the total requests going to providers based in another jurisdiction), by facilitating the adoption and subsequent implementation of the 'e-evidence package' and practical measures[80]. The swift adoption by the European Parliament and Council of the e-evidence proposals is key to provide practitioners with an efficient tool. Electronic evidence must be readable, thus the Commission will further work on the support to law enforcement capacity in the area of digital investigations, including dealing with encryption when encountered in criminal investigations while fully preserving its function to protect fundamental rights and cybersecurity.

2.3 EU cyber diplomacy toolbox

The EU has been using its **cyber diplomacy toolbox**[81] to prevent, discourage, deter and respond to malicious cyber activities. After introducing the legal framework for targeted restrictive measures against cyber-attacks in May 2019[82], the EU listed six individuals and three entities responsible for, or involved in, cyber-attacks affecting the EU and its Member States under the regime in July 2020[83]. Another two individuals and one body were listed in October 2020[84]. Malicious cyber activities, including those of a slow-burning nature, should be tackled by an effective and comprehensive joint EU diplomatic response, using the full range of measures available at EU level.

[80]COM(2018) 225 and 226; C(2020) 2779 final. In particular, the SIRIUS project recently received additional funding under the Partnership Instrument to improve channels to obtain lawful cross-border access to electronic evidence for criminal investigations (needed in 85% of investigations into serious crimes, with 65% of the total requests going to providers based in another jurisdiction), and establishing compatible rules at international level.

[81] https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[82]Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 129I 17.5.2019, p. 13); and Council Regulation (EU) 2019/796
of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 129I 17.5.2019, p. 1) 1)

[83] Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (ST/9564/2020/INIT) (OJ L 246, 30.7.2020, p. 12–17); and Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (ST/9568/2020/INIT) (OJ L 246, 30.7.2020, p. 4–9).

[84] Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 351I , 22.10.2020, p. 5–7); and Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 351I, 22.10.2020, p. 1–4).

A swift and effective joint EU diplomatic response requires solid shared situational awareness and the ability to prepare rapidly a joint EU position. The High Representative of the Union for Foreign Affairs and Security Policy will encourage and facilitate the establishment of a **Member States' EU cyber intelligence working group** residing within the EU Intelligence and Situation Centre (INTCEN) to advance strategic intelligence cooperation on cyber threats and activities. This work will further support EU situational awareness and decision-making on a joint diplomatic response. The working group is to engage with existing structures[85], including, where necessary, those covering the wider threat of hybrid and foreign interference, to collect and assess situational awareness.

To strengthen its ability to prevent, discourage, deter and respond to malicious behaviour in cyberspace, the High Representative, with the involvement of the Commission in line with its competences, will present a proposal for the EU to further define its **cyber deterrence posture**. Building on the work under the cyber diplomacy toolbox to date, the posture should contribute to responsible state behaviour and cooperation in cyberspace, and should give particular direction on countering those cyber-attacks that have the most significant effect, notably those affecting our critical infrastructure, democratic institutions and processes[86], as well as supply chain-attacks and cyber-enabled theft of intellectual property. The posture should outline how the EU and Member States could leverage their political, economic, diplomatic, legal and strategic communication tools against malicious cyber activities, as well as should address how the EU and Member States could advance their ability to attribute malicious cyber activities. In addition, together with the Council and the Commission, the High Representative aims to look into **additional measures under the cyber diplomacy toolbox**, including the possibility for further options for restrictive measures as well as by exploring **qualified majority voting (QMV) for listings under the horizontal sanctions regime against cyber-attacks.** In addition, the EU should undertake further efforts to **strengthen the cooperation with international partners**, including NATO, to advance the shared understanding of the threat landscape, develop cooperation mechanisms and identify cooperative diplomatic responses.

The High Representative, with the involvement of the Commission, will as well propose an update of the **implementing guidelines of the cyber diplomacy toolbox[87]**, including in view of increasing the efficiency of the decision-making process, and continues to organise exercises as well as assessments on the cyber diplomacy toolbox on a regular basis. In addition, the EU should further **integrate the cyber diplomacy toolbox in EU crisis mechanisms**, seek synergies with efforts to counter hybrid threats, disinformation and foreign interference under the Joint Framework on countering hybrid threats[88] and European Democracy Action Plan. In this context, the EU should reflect upon the interaction between the cyber diplomacy toolbox and the possible use of Article 42.7 TEU and Article 222 TFEU[89].

[85] Such as the EU Single Intelligence Analysis Capacity (SIAC), and, where necessary, the relevant projects established under PESCO, as well as the 2018 Rapid Alert System (RAS) that has been set up to support the EU's overall approach to tackling disinformation.
[86] Notably by seeking synergies with the initiatives under the European Democracy Action Plan.
[87] 13007/17
[88] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN
[89] Respectively the mutual defence clause, solidarity clause.

2.4 Boosting cyber defence capabilities

The EU and Member States need to increase their ability to prevent and respond to cyber threats in line with the EU Level of Ambition derived from the 2016 EU Global Strategy[90]. To this end, the High Representative, in cooperation with the Commission, will present a **review of the Cyber Defence Policy Framework (CDPF)** to enhance further coordination and cooperation between EU[91] actors, as well as with and between Member States, including as regards the Common Security and Defence Policy (CSDP) missions and operations. The CDPF should inform the upcoming Strategic Compass[92], ensuring that cybersecurity and cyber defence are further integrated into the wider security and defence agenda.

In 2018, the EU identified cyberspace as a domain of operations[93]. An upcoming **'Military Vision and Strategy on Cyberspace as a Domain of Operations'** by the EU Military Committee should further define how cyberspace as a domain of operations enables EU CSDP military missions and operations. The **Military CERT-Network**[94], being set up by the European Defence Agency (EDA), will further contribute to significantly increase cooperation among Member States. In addition, to ensure cybersecurity of critical space infrastructures under the responsibility of the Space Programme, the European Agency for the Space Programme and in particular the Galileo Security Monitoring Centre will be reinforced and its mandate extended to other critical assets of the Space Programme.

The EU and Member States should provide further impetus for the **development of state-of-the-art cyber defence capabilities** through different EU policies and instruments, notably the CDPF, and where appropriate, building on the work of the EDA. This requires a strong emphasis on the development and use of key technologies such as AI, encryption and quantum computing. In line with the 2018 EU Capability Development Priorities[95] and based on the findings of the first full Coordinated Annual Review on Defence (CARD) report[96], the EU should further foster cooperation among Member States on **cyber defence research, innovation and capability development**, encouraging Member States to make use of the full potential of the **Permanent Structured Cooperation (PESCO)[97]** and **EDF[98].**

The forthcoming **Commission Action Plan on synergies between the civil, defence, and space industries** to be presented in the first quarter of 2021, will include actions to further

[90] Council conclusions (14149/16) on implementing the EU Global Strategy in the area of security and defence.
[91] Notably the EEAS, including the EU Military Staff (EUMS), European Security and Defence College (ESDC), the Commission, and EU agencies, notably the European Defence Agency (EDA).
[92] Council Conclusions on Security and Defence of 17 June 2020 (8910/20)
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf
[94] The setup of an EU Military CERT-Network responds to an objective identified in the 2018 Cyber Defence Policy Framework and aims at promoting active interaction and information exchange between EU Member States military CERTs.
[95] In June 2018, Member States agreed in the EDA Steering Board to guide defence cooperation at EU level.
[96] Approved by Defence Ministers in the EDA Steering Board in November 2020.
https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)
[97] There are currently several cyber-related PESCO projects, notably the Cyber Threats and Incident Response Information Sharing Platform, Cyber Rapid Response Teams and Mutual Assistance in Cyber Security, the EU Cyber Academia and Innovation Hub and the Cyber and Information Domain Coordination Centre (CIDCC).
[98] Under the EDF, the Commission already identified opportunities for potential collaborative cyber defence research and development actions aimed at strengthening cooperation, innovation capacity and the competitiveness of the defence industry.

support synergies at the level programmes, technologies, innovation and start-ups, in line with the governance of the respective programmes[99].

In addition, relevant synergies and interfaces should be developed between cyber defence initiatives taken forward in other frameworks, including the cyber-related collaborative projects[100] by Member States under PESCO, as well as with the EU cybersecurity structures, to support information sharing and mutual support.

Strategic initiatives

The EU should:

- Complete the European cybersecurity crisis management framework and determine the process, milestones and timeline for establishing the Joint Cyber Unit;
- Continue implementation of cybercrime agenda under the Security Union Strategy;
- Encourage and facilitate the establishment of a Member States' cyber intelligence working group residing within the EU INTCEN;
- Advance the EU's cyber deterrence posture to prevent, discourage, deter and respond to malicious cyber activities;
- Review the Cyber Defence Policy Framework;
- Facilitate the development of an EU "Military Vision and Strategy on Cyberspace as a Domain of Operations" for CSDP military missions and operations;
- Support synergies between civil, defence and space industries; and
- Reinforce cybersecurity of critical space infrastructures under the Space Programme.

3. ADVANCING A GLOBAL AND OPEN CYBERSPACE

The EU should continue to work with international partners to promote a political model and vision of cyberspace grounded in the rule of law, human rights, fundamental freedoms and democratic values that bring social, economic and political development globally, and contribute to a Security Union. International cooperation is essential to keeping cyberspace global, open, stable and secure. The EU should to this end continue to work with third countries, international organisations as well as the multi-stakeholder community, to develop and implement a coherent and holistic international cyber policy, mindful of the increasing interconnection between economic aspects of new technologies, internal security and foreign, security and defence policies. The EU, as a strong economic and trading bloc founded on core democratic values, respect for the rule of law and fundamental rights, is also uniquely placed to lead in defining and promoting international norms and standards.

[99] Such as Horizon Europe, Digital Europe and the EDF.
[100] https://pesco.europa.eu/

3.1. EU leadership on standards, norms and frameworks in cyberspace

Stepping up on international standardisation

To promote and defend its vision of cyberspace at the international level, the EU needs to **step up its engagement in, and leadership on international standardisation processes, and enhance its representation in international and European standardisation bodies as well as other standard development organisations**[101]. As digital technologies are developing at a fast pace, international standards are of increasing importance in complementing traditional regulatory efforts in areas such as AI, cloud, quantum computing and quantum communication. International standardisation is increasingly used by third countries to advance their political and ideological agenda, which often does not correspond with the values of the EU. In addition, there is a growing risk of competing frameworks for international standardisation, leading to fragmentation.

Shaping international standards in the areas of emerging technologies and the core internet architecture in line with EU values is essential to ensure that the Internet remains global and open, that technologies are human-centric, privacy-focused, and that their use is lawful, safe and ethical. As part of its upcoming Standardisation Strategy, the EU should define its **objectives for international standardisation,** and conduct proactive and coordinated outreach to promote these at international level. Stronger cooperation and burden sharing should be sought with like-minded partners and European stakeholders.

Advance Responsible State Behaviour in Cyberspace

The EU continues to work with international partners to advance and promote a global, open, stable and secure cyberspace where **international law, in particular the United Nations (UN) Charter**[102]**, is respected,** and the **voluntary non-binding norms, rules and principles of responsible state behaviour**[103] are adhered to. With the deterioration of an effective multilateral debate on international security in cyberspace, there is a clear need for the EU and Member States to take a more proactive stance in the discussions in the UN and other relevant international fora. The EU is best placed to **advance, coordinate and consolidate Member States' positions in international fora**, and should **develop an EU position on the application of international law in cyberspace**. The High Representative, together with the Member States, also aims to take forward their inclusive and consensus-based proposal for a political commitment on a **Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA)**[104] in the UN. Building on the existing acquis as endorsed by the UN General Assembly[105], the PoA offers a platform for cooperation and exchange of

[101] E.g. the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), International Telecommunication Union (ITU), the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardization (CENELEC), the European Telecommunications Standards Institute (ETSI), the Internet Engineering Task Force (IETF), 3rd Generation Partnership Project (3GPP) and the Institute of Electrical and Electronics Engineers (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] As reflected in the relevant reports of the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGEs), endorsed by the UNGA, notably the 2015, 2013 and 2010 reports.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] As reflected in the relevant reports of the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGEs), endorsed by the UNGA notably the: 2015, 2013 and 2010 reports.

best practices within the UN, and proposes to establish a mechanism to put in practice the norms of responsible state behaviour and promote capacity building. In addition, the High Representative aims to strengthen and encourage the implementation of **confidence-building measures** between states, including sharing best practices at regional and multilateral levels and contributing to cross-regional cooperation.

Increased global connectivity should not lead to censorship, mass surveillance, data privacy breaches and repression against civil society, academia and citizens. The EU should continue to lead on the protection and promotion of **human rights and fundamental freedoms** online. To this end, the EU should promote further compliance with international human rights law and standards[106], and operationalise its Action Plan on Human Rights and Democracy 2020-2024[107], and advance its Human Rights Guidelines on Freedom of Expression Online and Offline[108], **offering a new impetus on the practical application of EU instruments**. The EU should make sustained efforts to **protect human rights defenders, civil society and academia working on issues such as cybersecurity, data privacy, surveillance and online censorship.** To this end, the EU should provide further practical guidance, promote best practices and step-up its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies. The EU should also continue to fight for the protection of the most vulnerable members of society online, by putting forward legislation to better protect children against child sexual abuse and exploitation and a Strategy on the Rights of the Child.

The Budapest Convention on Cybercrime

The EU continues to support third countries that wish to accede to the **Council of Europe Budapest Convention on Cybercrime**, and work to finalise the **Second Additional Protocol to the Budapest Convention** that includes measures and safeguards to improve international cooperation between law enforcement and judicial authorities, as well as between authorities and service providers in other countries, and for which the Commission participates in the negotiations on behalf of the EU[109]. The current initiative for a new legal instrument on cybercrime at UN level risks to amplify divisions and slow down much needed national reforms and related capacity building efforts, potentially hindering effective international cooperation against cybercrime: the EU does not see a need for any new legal instrument on cybercrime at UN level. The EU continues to engage in the **multilateral exchanges on cybercrime** to ensure the respect of human rights and fundamental freedoms, through inclusiveness, transparency, and taking into account available expertise, with the goal of delivering added value for all.

3.2 Cooperation with partners and the multi-stakeholder community

The EU should **strengthen and expand its cyber dialogues with third countries** to promote its values and vision for cyberspace, sharing best practices, and seeking to cooperate more effectively. The EU should also establish **structured exchanges with regional organisations** such as the African Union, the ASEAN Regional Forum, the Organisation of

[106] Notably the UN Charter and the Universal Declaration of Human Rights.
[107] https://www.consilium.europa.eu/en/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/
[108] https://www.consilium.europa.eu/media/28348/142549.pdf
[109] Council Decision of June 2019 (ref 9116/19)

American States, and the Organization for Security Cooperation in Europe. At the same time, the EU should endeavour to find common ground, where possible and opportune, with other partners based on issues of common interest. Working with the EU Delegations, as well as where relevant Member States' embassies around the world, the EU should form an informal **EU Cyber Diplomacy Network** to promote the EU vision of cyberspace, exchange information and regularly coordinate on developments in cyberspace[110].

Building on the Joint Declarations of 8 July 2016[111] and 10 July 2018[112], the EU should continue to advance **EU-NATO cooperation,** notably on cyber defence interoperability requirements. In this context, the EU should further pursue the affiliation of relevant CSDP structures to NATO's Federated Mission Networking, allowing network interoperability with NATO and partners when necessary. In addition, cooperation between the EU and NATO on education, training and exercises should be further explored, including by seeking synergies between the European Security and Defence College and the NATO Cooperative Cyber Defence Centre of Excellence.

In line with its values, the EU strongly supports and promotes the **multi-stakeholder model for Internet governance**. No single entity, government, or international organisation should seek to control the Internet. The EU should continue to engage in fora[113] to enhance cooperation and ensure the protection of fundamental rights and freedoms, notably the right to dignity, privacy and freedom of expression and information. To advance multi-stakeholder cooperation on cybersecurity issues, the Commission and High Representative, in line with their respective competences, aim to reinforce **regular and structured exchanges with stakeholders**, including the private sector, academia and civil society, underlining that the interconnected nature of cyberspace requires all stakeholders to exchange upon, and take their specific responsibilities to maintain a global, open, stable and secure cyberspace. These efforts will provide valuable input for potential key actions at EU level.

3.3. Strengthening global capacities to increase global resilience

To ensure that all countries are able to reap the social, economic and political benefits of the Internet and the use of technologies, the EU continues to support its partners to increase their cyber resilience and capacities to investigate and prosecute cybercrime and address cyber threats. In order to ensure overall coherence, the EU should develop an **EU External Cyber Capacity Building Agenda** to steer these efforts in line with its External Cyber Capacity Building Guidelines[114] and the Agenda 2030 for Sustainable Development[115]. The Agenda should leverage the expertise of Member States and relevant EU institutions, bodies and agencies and initiatives, including the EU's Cyber Capacity Building Network[116], in line with their respective mandates. An **EU Cyber Capacity Building Board,** shall be created to encompass relevant EU institutional stakeholders, and to monitor progress, as well as the identification of further synergies and potential gaps. It can furthermore support enhanced

[110] It could where relevant also leverage the activities of the informal EU Digital Diplomacy Network incorporating Member States' foreign ministries.
[111] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Such as the Internet Cooperation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

cooperation with Member States, as well as with public and private sector partners and other relevant international bodies to ensure coordination of efforts and avoid duplications.

EU cyber capacity building should continue to focus on the Western Balkans and in the EU's neighbourhood, as well as on partner countries experiencing a rapid digital development. The EU efforts should support the development of legislation and policies of partner countries in line with relevant EU cyber diplomacy policies and standards. In this context, EU capacity building efforts in the field of digitalisation should include cybersecurity as a standard feature. To this end, the EU should develop a training programme dedicated to EU staff in charge of the implementation of EU digital and cyber external capacity building efforts. The EU should also assist these countries in tackling the growing challenge of malicious cyber activities that harm the development of their societies and the **integrity and security of democratic systems,** in line with the efforts under the European Democracy Action Plan. Peer-to-peer learning between EU Member States as well as relevant EU agencies and third countries could be particularly useful in this respect.

Finally, within the context of the 2018 Civilian CSDP Compact[117], civilian CSDP missions can also contribute to the EU's wider response to tackle cyber security challenges, notably by strengthening the rule of law within, as well as law-enforcement and civilian administrations' capabilities of, partner countries.

Strategic initiatives

The EU should:

- Define a set of objectives in international standardisation processes, and promote these at international level;
- Advance international security and stability in cyberspace, notably through the proposal by the EU and its Member States for a Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA) in the United Nations;
- Offer practical guidance on the application of human rights and fundamental freedoms in cyberspace;
- Better protect children against child sexual abuse and exploitation, as well as a Strategy on the Rights of the Child;
- Strengthen and promote the Budapest Convention on Cybercrime, including through the work on the Second Additional Protocol to the Budapest Convention;
- Expand EU cyber dialogue with third countries, regional and international organisations, including through an informal EU Cyber Diplomacy Network;
- Reinforce the exchanges with the multi-stakeholder community, notably by regular and structured exchanges with the private sector, academia and civil society; and
- Propose an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board.

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/en/pdf

III. CYBERSECURITY IN THE EU INSTITUTIONS, BODIES AND AGENCIES

Given their high political profile, their critical missions to coordinate highly sensitive issues, and their role in managing large sums of public money, **the EU institutions, bodies and agencies are regular targets of cyberattacks**, particularly cyber-espionage. However, the level of cyber resilience and ability to detect and respond to malicious cyber activities varies significantly across these entities in terms of maturity. It is thus necessary to improve the overall level of cybersecurity through consistent and homogeneous rules.

In the area of information security, progress has been made towards more consistency of the **rules for the protection of EU classified information as well as sensitive non-classified information**. However, the interoperability of classified information systems remains limited, preventing a seamless transfer of information between the different entities. Further progress should be made to enable an inter-institutional approach to the handling of EU classified information and sensitive non-classified information, which could also serve as a model for interoperability across Member States. A baseline should also be established to simplify procedures with Member States. The EU should also further develop its ability to communicate in a secure manner with relevant partners, building to the extent possible on existing arrangements and procedures.

As announced in the Security Union Strategy, the Commission will therefore make proposals for **common binding rules on information security and for common binding rules on cybersecurity for all EU institutions, bodies and agencies in 2021**, based on ongoing EU inter-institutional discussions on cybersecurity[118].

Current and future trends of teleworking will also necessitate further investments in secure equipment, infrastructures and tools that allow to work remotely on sensitive and classified files.

In addition, the increasingly hostile cyber threat landscape and the increased incidence of more sophisticated cyberattacks affecting the EU institutions, bodies and agencies drives the need for increased investments to reach a high level of cyber maturity. A Cyber Awareness Programme is being set up for all EU institutions, bodies and agencies to raise staff's awareness, cyber hygiene and support a common cyber security culture.

The **reinforcement of CERT-EU with an improved funding mechanism** is necessary to increase its ability to help EU institutions, bodies and agencies to apply the new cybersecurity rules, improve their cyber resilience. The mandate of CERT-EU must also be strengthened to provide it with a stable means to meet these objectives.

Strategic initiatives

1. Regulation on Information Security in the EU institutions bodies and agencies
2. Regulation on Common Cybersecurity Rules for EU institutions, bodies and agencies

[118] A regular EU inter-institutional discussions on cybersecurity form part of wider exchanges on the opportunities and challenges of digital transformation for the EU institutions.

3. A new legal base for CERT-EU to reinforce its mandate and funding.

IV. CONCLUSIONS

The concerted implementation of this strategy will contribute to a cybersecure digital decade for the EU, to the achievement of a Security Union, and to the strengthening of the EU's position globally.

EU should drive standards and norms for world class solutions and standards of cybersecurity for essential services and critical infrastructures, as well as the development and application of new technologies. Every organisation and individual using the Internet is part of the solution in ensuring a cyber-secure digital transformation.

The Commission and the High Representative, in line with their respective competences, will monitor progress under this strategy and develop criteria for evaluation. Inputs to this monitoring should include the reports from ENISA, and the Commission's regular Security Union reports. The results will contribute to the upcoming Digital Decade objectives[119]. In line with their respective competences, the Commission and the High Representative will continue to liaise with Member States to identify practical measures to bridge the four cybersecurity communities in the EU of critical infrastructure and internal market resilience, justice and law enforcement, cyber diplomacy and cyber defence, where necessary. In addition, the Commission and the High Representative will continue to engage with the multi-stakeholder community, underlining the need for everyone who uses the Internet to play their part in maintaining a global, open, stable and secure cyberspace, where everyone can safely live their digital lives.

[119] As announced in the Commission Work Programme 2021.

Appendix: Next steps on cybersecurity of 5G networks

Based on the results of the review of the Commission Recommendation on the Cybersecurity of 5G networks[120], the next steps in the coordinated work at EU level should focus on three key objectives and on main actions for the short and mid-term set out in the table below, to be implemented by Member States authorities, the Commission and ENISA.

The first priority for the next phase is to **complete the implementation of the Toolbox at national level and to address the issues identified in the Progress report of July 2020**. In this context, some of the Toolbox Strategic measures would benefit from **enhanced coordination work or exchange of information** within the NIS Work Stream, as already identified in the Progress report, which could potentially lead to the development of **best practices or guidance**. As regards Technical measures, ENISA could provide further support, building on the work they have already done and investigating certain topics more in-depth, as well as **developing a comprehensive overview of all relevant guidelines on 5G cybersecurity requirements for mobile network operators.**

Secondly, Member States emphasised the importance of keeping abreast of developments through the **continuous monitoring of evolutions in the technology, 5G architecture, threats and 5G use cases and applications, as well as external factors,** in order to be able to **identify and address new or emerging risks**. Moreover, a number of aspects in the initial risk analysis should be looked into further, notably to ensure it addresses the entire 5G ecosystem, including all relevant parts of the network infrastructure and of the 5G supply chain. While the Toolbox has been designed as a flexible and adaptable instrument, if necessary, steps could be taken in the medium term to augment or amend it, in order to ensure it remains comprehensive and up-to-date.

Thirdly, **EU-level actions** should continue to be taken to support and complement the Toolbox objectives and to fully integrate them into relevant Union and Commission policies, notably following up on the actions announced by the Commission in its Communication on the Toolbox of 29 January 2020[121] in a broad range of areas (e.g. EU funding for secure 5G networks, investments in 5G and post-5G technologies, trade defence instruments and competition to avoid distortions in the 5G supply market, etc.).

Where appropriate, detailed arrangements and milestones for the main actions set out below should be agreed by the lead actors in early 2021.

Key objective 1: Ensuring convergent national approaches for effective risk mitigation across the EU		
Areas	**Main short- and mid-term actions**	**Lead actors**
Toolbox implementation by Member States	Complete the implementation of the measures recommended in the Toolbox conclusions by the second quarter of 2021, with periodic stocktaking within the NIS Work Stream.	Member States authorities
Exchange of	Intensify exchanges of information and consider possible	Member

[120] Commission Report on the impacts of the Commission Recommendation 2019/534 of 26 March 2019 on the Cybersecurity of 5G networks.

[121] Commission Communication COM (2020)50, Secure 5G deployment in the EU - Implementing the EU toolbox, 29 January 2020.

information and best practices on strategic measures related to suppliers	best practices, in particular about: - Restrictions on high-risk suppliers (SM03) and measures related to the provision of managed services (SM04); - Supply chain security and resilience, notably following up on the survey conducted by BEREC about SM05-SM06.	States authorities, Commission
Capacity building and guidance on technical measures	Conduct technical deep-dives and develop common guidance and tools, including: - A comprehensive and dynamic matrix of security controls and best practices for 5G security; Guidance in support of implementation of selected technical measures from the Toolbox.	ENISA, Member States authorities
Key objective 2: Supporting continuous exchange of knowledge and capacity building		
Areas	**Main short- and mid-term actions**	**Lead actors**
Continuous knowledge building	Organise knowledge building activities on technology and related challenges (open architectures, 5G features – e.g. virtualisation, containerisation, slicing etc.), threat landscape evolutions, real-life incidents, etc.	ENISA, Member states authorities, other stakeholders
Risk assessments	Update and exchange information on updated national risk assessments	Member States authorities, Commission, ENISA
Joint EU-funded projects to support the Toolbox implementation	Provide financial support to projects supporting the Toolbox implementation using EU funding, notably under the Digital Europe Programme (e.g. capacity building projects for national authorities, test beds or other advanced capacities, etc.)	Member States authorities, Commission
Cooperation among stakeholders	Foster collaboration and cooperation between national authorities engaged in 5G cybersecurity (e.g. NIS Cooperation Group, cybersecurity authorities, telecom regulatory authorities) and with private stakeholders	Member States authorities, Commission, ENISA
Key objective 3: Promote supply chain resilience, and other EU strategic security objectives		
Areas	**Main short- and mid-term actions**	**Lead actors**
Standardisation	Define and implement a concrete action plan to enhance EU representation in standard setting bodies as part of the next steps of the work of the NIS sub-group on standardisation, in order to achieve specific security objectives, including the promotion of interoperable interfaces to facilitate diversification of suppliers.	Member States authorities
Supply chain resilience	- Conduct an in-depth analysis of the 5G ecosystem and supply chain to better identify and monitor key assets and potential critical dependencies - Ensure the functioning of the 5G market and supply chain is in line with EU trade and competition rules and objectives, as defined in the Commission Communication of 29 January, and that FDI screening is applied to investment developments potentially affecting the 5G value chain,	Member States authorities, Commission

	taking into account the objectives of the Toolbox. - Monitor existing and expected market trends and assess the risks and opportunities in the field of Open RAN, notably through an independent study	
Certification	Initiate preparations of relevant candidate certification scheme(s) for key 5G components and suppliers' processes, to help address certain risks related to technical vulnerabilities, as defined in the Toolbox risk mitigation plans.	Commission, ENISA, national authorities, other stakeholders
EU capacities and secure network roll-outs	- Invest into R&I and capacities, notably through the adoption of the Smart Networks and Services Partnership. - Implement relevant security conditions for EU funding programmes and financial instruments (internal and external), as announced in the Commission Communication of 29 January.	Member States, Commission, 5G industry stakeholders
External aspects	Respond favourably to third country requests who would like to understand and potentially use the Toolbox approach developed by the EU.	Member States, Commission EEAS, EU Delegations