EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 23.6.2021
JOIN(2021) 14 final

2021/0166 (NLE)

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade

I. Cyber resilience, operational capacity and openness more essential than ever

Cybersecurity is indispensable to the deployment of smarter and greener technology in the post-pandemic world. It is indispensable overall to the EU's security and it is a pillar of the Security Union. Social, political and economic development requires technological sovereignty and a global, open and secure cyberspace, grounded in the rule of law and respect for human rights and fundamental freedoms. This was the core premise of the Joint Communication of the Commission and High Representative for Foreign Affairs and Security Policy on the EU's Cybersecurity Strategy for the Digital Decade, adopted on 16 December 2020[1]. All critical entities are potential subjects of cyberattacks. The developments in the past six months have vindicated the strategy's focus on stepping up regulatory reforms, on investment and on collective operational response.

Recent cyberattacks have demonstrated, in particular, the increased pervasiveness of ransomware and cyberespionage operations and their growing risk for all sectors of the economy and society at large. The scale of the incidents has been extraordinary: hundreds of thousands of servers affected in the attacks on Microsoft Exchange; 18 000 organisations potentially affected by the SolarWinds Orion campaign; sensitive data on hundreds of patients stolen and medical services disrupted in the ransomware attack on Ireland's health service; a fuel emergency and massive data theft in the cyberattack on the Colonial Pipeline billing system; and disruption of operations of the world's largest beef supplier[2]. While the full extent of the damage remains unclear, each incident highlights the potential far-reaching consequences of malicious exploitation of vulnerabilities in information and communication technology products, services, systems and networks. Such cyberattacks can be expected to increase in impact and frequency and to undermine our security.

It is essential, therefore, for the European Union to accelerate progress on all fronts - legislative, operational, investment-related and diplomatic - as set out in the strategy. The proposals for a Directive on measures for a high common level of cybersecurity across the Union ('the NIS2 Directive')[3], for a Directive on the resilience of critical entities[4], as well as for a Regulation and Directive on Digital Operational Resilience[5], should be adopted as soon as possible. In this context, it

[1] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18.

[2] SolarWinds, a major US information technology firm, was the subject in 2020 of a cyberattack that spread to its clients and went undetected for months, giving hackers access to thousands of companies and government offices that used its products Orion product, including six EU institutions, bodies and agencies. From January 2021 a number of zero-day exploits were discovered in Microsoft Exchange Server affecting email systems around the world. In May the Health Service Executive of the Republic of Ireland was subject to an attack that had a significant impact on service continuity. Colonial Pipeline, the largest US fuel pipeline operator, had to halt operations on 7 May after discovering a breach through a cybersecurity attack that had affected their main IT systems, and on June 2021, JBS USA Holdings Inc., the US-based branch of the largest meat supplier in the world by sales, was successfully attacked by ransomware, causing severe interruptions of operations.

[3] Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/1148, COM (2020) 823.

[4] Proposal for a Directive on the resilience of critical entities, COM (2020) 829.

[5] 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; Proposal for a directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, COM(2020) 596.

is essential to pursue an ambitious approach notably regarding supply chains, in view of how vulnerabilities in recent cyberattacks were traced back to software vendors, and to take measures ensuring the resilience of public administrations and the swift notification of incidents. The need to establish a network of Security Operations Centres (or 'SOCs') for early detection of signals of cyberattacks has become more pressing than ever, as has the need to develop a credible, effective and collective EU response, including at operational level, to major incidents through the Joint Cyber Unit[6]. Given the increase of cyberattacks conducted by state or state-sponsored actors, responsible state behaviour must continue to be promoted in the United Nations, as well as through cyber dialogues and structured exchanges with regional organisations, including the African Union, the ASEAN Regional Forum, the Organisation of American States (OAS), and the Organisation for Security Cooperation in Europe (OSCE), along with effective diplomatic action to prevent, discourage, deter and respond to malicious behaviour in cyberspace. Of particular importance will be cooperation with like-minded third countries and the priorities of the transatlantic agenda; notably the EU-US cooperation on specific cybersecurity aspects should be further explored, including on information sharing and combatting ransomware.

II. Overview of first six months of implementation

A number of strategic actions are already well advanced.

II.1 Resilience, Technological Sovereignty and Leadership

Around the world, supply chains and critical infrastructure, including hospitals battling the COVID-19 pandemic, are now at constant risk of cyberattack. The Commission is supporting the co-legislators to ensure the swift adoption of the proposed reform of the NIS Directive, which will in particular expand coverage of the health sector including research labs and manufacturing of critical medical devices and medicines, and new energy sector activities such as hydrogen production, district heating, electricity production and central oil stockholding.

The Regulation setting up the Cybersecurity Competence Centre and the Network of National Coordination Centres was adopted on 20 May 2021[7]. It will pool resources from the EU, Member States and industry to improve and strengthen technological and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy, and offering a possibility to consolidate part of the cybersecurity-related activities funded under Horizon Europe, the Digital Europe Programme and the Recovery and Resilience Facility – funding streams totalling up to EUR 4.5 billion over the next six years[8]. This will support the development by 2023 of an EU Cyber Shield for early detection of cyberattacks composed of a network of Security Operations Centres, which may be public or private and will leverage Artificial Intelligence-powered tools. Several Member States have included the development of such national centres under their respective Recovery and Resilience plans. The Commission will complement these efforts by allocating funds from the Digital Europe Programme and support their phased connection. The financial programmes will also support the EuroQCI initiative to build a secure quantum communication infrastructure spanning the whole EU[9], including its overseas territories, using the best combination of ground-based and space-based technologies, and a specific budget line to support cyber resilience in the health sector.

[6] [JCU recommendation]

[7] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

[8] The Cybersecurity Competence Centre will do this in particular by deciding on and managing cybersecurity funds from the Digital Europe Programme and the Horizon Europe Programme, as well as from Member States.

[9] https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

Ensuring 5G cybersecurity is a continuous process that will accompany the gradual deployment of 5G and implementation of the EU 5G Toolbox [10]. Most Member States have already - or soon will have - in place frameworks for imposing appropriate restrictions on 5G suppliers. Requirements on mobile network operators are being reinforced through the transposition of the Electronic Communications Code, and the EU Agency for Cybersecurity, ENISA, is preparing a candidate EU cybersecurity certification scheme for 5G networks[11]. Looking at new trends and developments in the 5G supply chain, Member States authorities have decided to launch an in-depth analysis of the security implications of open, disaggregated and interoperable network technology solutions ('Open RAN') under the EU toolbox. The result of this work will further contribute to the EU's concerted approach to the security of 5G networks.

Greater efforts are required, notably through the EU's Digital Education Action Plan, to address the massive skills shortage predicted to reach almost two million unfilled cybersecurity posts globally by 2022 and 350 000 in Europe alone, and the severe underrepresentation of women – women make up only 11% of the global cybersecurity workforce and even less - 7% - in Europe[12]. Other ongoing policy initiatives include preparatory work for future initiatives for security of the Internet of Things and, on internet standards, the development of a non-profit domain name resolution service ('DNS4EU').

II.2 Building Operational Capacity to Prevent, Deter and Respond

With the rise in state and state-sponsored as well as criminal attacks on networks and information systems, and the increasing reliance on databases of sensitive information, the EU requires closer interconnection of the cyber communities. They need to respond coherently to the civilian, criminal, diplomacy and defence aspects of large-scale cyberattacks that many sensitive economic sectors have recently been experiencing. Efforts by all communities are therefore necessary to complete the four steps outlined in the Commission's Recommendation on building the Joint Cyber Unit, adopted at the same time as this report, as a mechanism for further coordination and filling gaps in the EU's response to cyber threats[13]. In the fight against cybercrime, political agreement was reached on the temporary regulation against child sexual abuse online, which will shortly be adopted[14], and the Commission's new Organised Crime Strategy[15] focuses on the need to equip law enforcement with the digital tools they need. The Commission also adopted in February 2020 an Action Plan on synergies between civil, defence and space industries which identifies a new flagship project for the establishment of an EU space-based global secure connectivity system. It aims to "enable access to high-speed connectivity for everyone in Europe, and provide a resilient connectivity system allowing Europe to remain connected whatever happens"[16].

[10] Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks, SWD(2020) 357 final, 16 December 2020.

[11] Preparation of the scheme follows the support of the NIS Cooperation Group and in line with Article 48 of the Cybersecurity Act; Regulation (EU) 2019/881 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. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-commission-requests-eu-cybersecurity-agency-develop-certification

[12] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

[13] [The Joint Cyber Unit would enable a coordinated response to and recovery from large-scale cyber incidents and crises and help ensure mobilization of resources for assistance. It would involve experts across cybersecurity communities to build a shared situational awareness and ensure necessary preparedness. It would also coordinate assistance mechanisms on request from one or more Member States.]

[14] https://www.europarl.europa.eu/news/it/press-room/20210430IPR03213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse

[15] Organised Crime Strategy 2021-2025, COM(2021) 170 of 14.04.2021.

[16] COM (2021) 70 of 22.02.2021.

From the international perspective, in line with the ambition set under the Strategic Compass[17], the High Representative is currently preparing the review of the Cyber Defence Policy Framework that is to be presented to Member States in the second half of 2021. The High Representative has worked to improve the EU's ability to prevent, discourage, deter and respond to malicious cyber activities, including by strengthening international cooperation. On 17 May 2021, the European External Action Service (EEAS), in cooperation with the Portuguese Presidency and the European Union Institute for Security Studies (EUISS), organised a scenario-based discussion with EU Member States and international partners to improve the mutual understanding of the respective diplomatic approaches to prevent, discourage, deter and respond to malicious cyber activities, and to identify opportunities for further reinforcing international cooperation to this end[18]. To strengthen further the EU's cyber diplomacy toolbox, the EEAS is collecting lessons learnt and may review the implementing guidelines of the framework for a joint EU diplomatic response to malicious cyber activities.

As announced in the EU cybersecurity strategy for the digital decade, the Commission is launching a study to develop awareness-raising tools aimed at improving the preparedness and resilience of EU businesses against cyber-enabled intellectual property theft.[19] The Commission also intensified enforcement actions in relation to the 2013/40/EU Directive on Attacks against information systems by launching additional infringement proceedings against several Member States in June 2021.[20] The Commission will consider further action as necessary. Improving the availability of cybersecurity skills in the EU's workforce will also be key; the Cybersecurity Competence Centre will deliver key actions in this respect with the aim of improving knowledge and capacity and of encouraging interdisciplinary skills to be developed in the area of cybersecurity.

II.3 Advancing a Global and Open Cyberspace

The threat landscape is compounded by geopolitical tensions over the global and open Internet and over technologies across the whole supply chain. Restrictions of and on the Internet, the increase in malicious cyber activities and those affecting the security and integrity of information and communication technology products and services, are a threat to a global and open cyberspace, as well as the rule of law, human rights, fundamental freedom and democratic values. The High Representative, together with Member States, is therefore working to advance responsible state behaviour in cyberspace, notably by establishing a Programme of Action (PoA) to Advance Responsible State Behaviour at United Nations level, together with the 53 other co-sponsors, building on the recommendation of the 12 March 2021 consensus report from the United Nations Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security[21]. The EU is working on strengthening and expanding the relations with third countries, international and regional organisations as well as the multi-stakeholder community through cyber dialogues, as set out in the strategy, by the establishment of an EU Cyber Diplomacy Network. Furthermore, the EU Cyber Capacity Building Board[22] is being set up, allowing EU institutions, bodies and agencies to better coordinate and cooperate on the EU's external cyber capacity-building efforts.

In the framework of the United Nations, on 26 May 2021, the General Assembly adopted modalities of work for the ad hoc committee established by Resolution 74/247 on 'countering the use of

[17] Council Conclusions on Security and Defence of 17 June 2020 (8910/20)

[18] https://eeas.europa.eu/headquarters/headquarters-homepage/98588/cyberspace-strengthening-cooperation-promoting-security-and-stability_en

[19] COM (2020) 760 of 25.11.2020

[20] The Member States in question are Austria, Belgium, Czech Republic, Estonia, Luxembourg, Poland and Sweden.

[21] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[22] https://www.eucybernet.eu/

information and communication technologies for criminal purposes'.[23] The modalities as finally adopted include important elements to ensure inclusive decision-making procedures and stronger participation of civil society in the works of the ad hoc committee. The first negotiating session of the process that will lead to a new UN convention will take place in New York in January 2022.

At the 28 May 2021 plenary meeting of the Committee of State Parties to the Council of Europe 'Budapest' Convention on Cybercrime, State Parties finalised discussions and adopted a draft text of the Second Additional Protocol to the Convention[24], which should enhance cooperation on cybercrime and electronic evidence in criminal investigations. The Commission participated in the discussions on behalf of the EU[25]. This should provide a basis for the formal conclusion of the negotiations in the course of the second half of 2021, and for the subsequent opening for signature of the Second Additional Protocol in the beginning of 2022.

The EU, with its partners in June 2021, reiterated its determination to work together to address the urgent and escalating threat from criminal ransomware networks that pose risks to our citizens and companies, to further a common understanding of how existing international law applies to cyberspace and to promote this approach at the UN and other international fora, calling on all states to urgently identify and disrupt ransomware criminal networks operating from within their borders, and hold those networks accountable for their actions.[26]

II.4 Cybersecurity in the EU institutions, bodies and agencies

The EU is on course to raise standards for cybersecurity and information security in the EU institutions, bodies and agencies. The Commission is undertaking stakeholder consultation and benchmarking of current policies with a view to adopting proposals before the end of 2021.

III. Background to this report

The Commission and the High Representative adopted the EU's Cybersecurity Strategy on 16 December 2020. It sets out priorities and key actions to build up Europe's resilience, autonomy, leadership and operational capacity in the face of growing and complex threats to its network and information systems, and to advance a global and open cyberspace and its international partnerships thereof. The Commission and the High Representative undertook to monitor progress of the strategy implementation.

The European Council, in its statement of 26 February 2021, invited the Commission and the High Representative to report on the implementation of the strategy by June 2021[27]. The Council, in conclusions adopted on 9 March 2021, welcomed the strategy, highlighting that cybersecurity was essential for building a resilient, green and digital Europe and encouraging the Commission and the High Representative to establish a detailed implementation plan setting the priorities and the schedule

[23] https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html
[24] https://rm.coe.int/0900001680a2aa42
[25] The Second Additional Protocol to the Budapest Convention on Cybercrime 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; Council Decision of June 2019 (ref 9116/19)
[26] EU-US Summit Statement, 15 June 2021; https://www.consilium.europa.eu/media/50443/eu-us-summit-joint-statement-15-june-final-final.pdf. Carbis Bay G7 Summit Communiqué: Our Shared Agenda for Global Action to Build Back Better, 13 June 2021; https://www.consilium.europa.eu/media/50361/carbis-bay-g7-summit-communique.pdf
[27] https://www.consilium.europa.eu/media/48625/2526-02-21-euco-statement-en.pdf

of planned actions[28]. The strategy is under consideration by relevant committees of the European Parliament, including a particular focus on the risk of fragmented regulation and the opportunity to strengthen European industry as it digitises[29]. The European Economic and Social Committee adopted on 27 April an Opinion which welcomed the strategy as a positive step towards protecting from global cyber threats and safeguarding economic growth[30].

This report responds to these developments and in particular to the invitation from the European Council.

[28] https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

[29] (2021/2568(RSP))

[30] https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/communication-cybersecurity-strategy