Council of the European Union

Brussels, 23 June 2021
(OR. en)

10137/21
ADD 1

CYBER 181	RECH 321
JAI 773	COMPET 510
JAIEX 79	IND 180
EJUSTICE 67	COTER 78
COSI 128	ENFOPOL 244
DATAPROTECT 173	COPS 249
COPEN 289	MI 501
TELECOM 272	IXIM 129
PROCIV 78	POLMIL 98
CSC 255	HYBRID 36
CIS 82	CSCI 95
RELEX 590	POLGEN 112

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	23 June 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	JOIN(2021) 14 final - ANNEX
Subject:	ANNEX to the Joint Communication to the European Parliament and the Council Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade

Delegations will find attached document JOIN(2021) 14 final - ANNEX.

Encl.: JOIN(2021) 14 final - ANNEX

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 23.6.2021
JOIN(2021) 14 final

ANNEX

ANNEX

to the

Joint Communication to the European Parliament and the Council

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

Progress in implementing the strategic initiatives

Reference	Initiative	COM/High Representative	Status
(1) Resilience, technological sovereignty and leadership			
1.1	Adoption of **revised NIS Directive**	COM	The position of the Parliament is expected to be finalised towards end 2021. Progress report on negotiations presented by the Council in June. Complementing this and addressing the energy sector-specific rules, a network code on cybersecurity under the Electricity Regulation (EU) 2019/943 is in development to increase the resilience and protection of the energy sector. Regarding the Regulation and Directive on Digital Operational resilience (DORA), the position of the Parliament is expected to be finalised in the second half of 2021. A general approach on the proposal is expected to be reached by the Council in June 2021.
1.2	Regulatory measures for **an Internet of Secure Things**	COM	Ongoing study and consultations on comprehensive rules are ongoing. Progress towards a Delegated Act under the Radio Equipment Directive (Directive 2014/53/EU) for possible adoption in 2021; rules for motor vehicles for all new vehicle types from July 2022 are to be implemented. The Commission is working with stakeholders on the role of cybersecurity certification for products, processes and services in various sectors.
1.3	Implement **investments in cybersecurity** (notably from the Digital Europe Programme, Horizon Europe and the Recovery and Resilience Facility), in particular through the Cybersecurity Industrial, Technology and Research Competence Centre and Network of Competence Centres when available, to reach up to €4.5 billion in public and private investments over 2021-2027	COM	New work programmes for the Horizon Europe and Digital Europe Programme financial mechanisms are shortly to be adopted, to be managed by the new Cybersecurity Industrial, Technology and Research Competence Centre and Network of Competence Centres.
1.4	An EU network of AI-enabled **Security Operations Centres** [The EU '**Cyber Shield'**] and an ultra-secure quantum communication	COM	Member States have been encouraged to develop national operational capability through Security Operations Centres (SOCs). Several Member States intend to use the Recovery and Resilience Facility (RRF) to promote

Reference	Initiative	COM/High Representative	Status
	infrastructure [EuroQCI]		SOCs, and discussions are under way involving Commission and other EU institutions, bodies and agencies and Member States, on how to connect the SOCs and host computing and analytical capacity[1]. Member States continue to work to further the EuroQCI initiative with the Commission and European Space Agency. The EuroQCI Action Plan awaits endorsement by Member States. The first Digital Europe Programme (DEP) calls to support national QCI networks and the development of key technologies needed for the EuroQCI will be launched shortly. The Commission 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. Several Member States have included secure connectivity initiatives in their RRF plans. Actions under the Connecting Europe Facility (CEF2) Digital will support the construction of cross-border links between national networks. Several Member States have included the EuroQCI in their RRF plans.
1.5	Widespread adoption of cybersecurity technologies through **dedicated support to SMEs** under the Digital Innovation Hubs	COM	The Commission is working to ensure cybersecurity content and expertise is provided through the European Digital Innovation Hubs initiative under the DEP and in liaison with national cyber security coordination centres. Cybersecurity stakeholders including European Cyber Security Organisation are developing a "service catalogue" for cybersecurity-focused innovation hubs.
1.6	Development of an **EU DNS resolver service** as a safe and open alternative for EU citizens, businesses and public administration to access the Internet [**DNS4EU**]	COM	Funding for the development of DNS4EU has been earmarked under the Connecting Europe Facility (CEF2) Digital work programme 2021-23[2], and a call for proposals for the project is planned in 2021. Additionally on internet security, the Commission is in discussion with internet stakeholders, and intends to launch a study to define a contingency

[1] Discussions are taking place with the CSIRTs Network, Cyber Crises Liaison Organisation Network (CyCLoNe) and the NIS Coooperation Group.
[2] Agreement on the proposed Connecting Europe Facility (CEF2) was reached by the Parliament and the Council on 12 March 2021.

Reference	Initiative	COM/High Representative	Status
			plan, supported by EU funding, **for dealing with extreme scenarios** affecting the integrity and availability of the global DNS root system A study on monitoring the development and deployment of key Internet standards in support of EU policies and to accelerate the **uptake of key internet standards** such as Internet Protocol v6 (IPv6) and well-established internet security, standards and good practices for DNS, routing, and email security is under preparation (planned kick-off autumn 2021). Funding under DEP is envisaged to create an **Internet Observatory** within the scope of activities of the European Cybersecurity Industrial, Technology and Research Competence Centre.
1.7	Completion of the **implementation of the 5G Toolbox**	COM	Member States supported by the Commission and ENISA made further progress in implementing the 5G Toolbox, in particular the restrictions on high-risk suppliers. Other actions at EU level include the preparation of an EU candidate certification scheme on 5G networks and the launch by the NIS Cooperation Group of an analysis of security implications of Open RAN.
(2) **Building operational capacity to prevent, deter and respond**			
2.1	Complete the European cybersecurity crisis management framework and determine the process, milestones and timeline for establishing the **Joint Cyber Unit**	COM with HR	The Commission adopted on 23 June 2021 a Recommendation on building the Joint Cyber Unit, addressing milestones, process and timing, and taking into account discussions with Member States.
2.2	Continue implementation of **cybercrime agenda under the Security Union Strategy**	COM	Member States with Commission support are identifying best practices for recording, producing and publishing statistical data on the reports, prosecutions and convictions for cyberattack offences defined in Directive 2013/40/EU on attacks on information systems. The Commission is monitoring progress following the open infringement procedures concerning seven Member States' inadequate transposition of Directive 2013/40/EU. Additional procedures may be opened later 2021. The Commission launched a study on identity theft with results expected by

Reference	Initiative	COM/High Representative	Status
			December 2021. Data collection on crime statistics will be extended in 2021 in line with Article 14 of Directive 2013/40/EU.
2.3	Encourage and facilitate the establishment of a **Member States' cyber intelligence working group residing within the EU Intelligence and Situation Centre (INTCEN)**	HR	The HR continues to encourage and facilitate the establishment of a Member States' cyber-intelligence working group in order to strengthen INTCEN's dedicated capacity in this domain, based on voluntary intelligence contributions from the Member States and without prejudice to their competences. Further discussion is planned between EEAS and Member States.
2.4	Advance the EU's **cyber deterrence posture** to prevent, discourage, deter and respond to malicious cyber activities	HR with COM	The EEAS is reviewing the implementing guidelines of the framework for a joint EU diplomatic response to malicious cyber activities to help develop the cyber diplomacy toolbox[3]. A proposal on the cyber deterrence posture is in preparation with a view to being presented to the Council by the HR, with the involvement of the Commission in line with its competences, in early 2022. A declaration on behalf of the EU was issued on 16 April 2021 expressing solidarity with the United States on the impact of malicious cyber activities, notably the SolarWinds cyber operation[4]. To further advance international cooperation, the EEAS with the Presidency of the Council and the European Union Institute for Security Studies hosted on 17 May 2021 a discussion to improve the mutual understanding of the respective diplomatic approaches to prevent, discourage, deter and respond to malicious cyber activities.
2.5	Review the **Cyber Defence Policy Framework**	HR with COM	The review of the Cyber Defence Policy Framework in liaison with Member States and stakeholders began in May 2021.
2.6	Facilitate the development of an EU "**Military**	HR	The Military Vision and Strategy on Cyberspace as a Domain of Operations

[3] Council Decisions (CFSP) 2020/1127, 2020/1537, and 2020/651 as part of 9916/17.

[4] https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation/

Reference	Initiative	COM/High Representative	Status
	Vision and Strategy on Cyberspace as a Domain of Operations" for CSDP military missions and operations		is to inform national strategies and with this to support the harmonisation of EU efforts in cyber defence. The second EU Cyber Defence Conceptual Development Workshop was held 28-29 April 2021, with a view to presentation before the EU Military Committee in June 2021.
2.7	Support **synergies between civil, defence and space** industries	COM	An action plan for supporting synergies between the sectors was adopted in February 2021.
2.8	Reinforce **cybersecurity of critical space infrastructures** under the Space Programme.	COM	A work programme is in preparation.
(3) Advancing a global and open cyberspace			
3.1	Define a set of **objectives in international standardisation processes**, and promote these at international level	COM	Work on these objectives is ongoing.
3.2	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** in the United Nations	HR	The EU is continuing work to establish the Programme of Action, building on the consensus report of 12 March 2021 from the United Nations Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.
3.3	Offer **practical guidance on the application of human rights and fundamental freedoms** in cyberspace	HR with COM	Building on the Action Plan on Human Rights and Democracy (2020-2024) and its Human Rights Guidelines on Freedom of Expression Online and Offline, the EU will continue to promote further compliance with international human rights law and standards; coordination meetings with relevant stakeholders are planned in the second half of 2021.
3.4	Better **protect children against child sexual abuse and exploitation**, as well as a Strategy on the Rights of the Child	COM	An agreement was reached between the European Parliament and Council in May 2021 on a temporary regulation to ensure that providers of online communications services can continue their voluntary practices to detect and report child sexual abuse online and remove child sexual abuse material. The Commission is developing a proposal for a permanent framework.
3.5	Strengthen and promote the **Budapest**	COM with HR	The Commission is participating in the negotiations for the Second

Reference	Initiative	COM/High Representative	Status
	Convention on Cybercrime, including through the work on the Second Additional Protocol to the Budapest Convention		Additional Protocol on behalf of the EU, with the Protocol potentially to be opened for signature by early 2022.
3.6	Expand EU **cyber dialogue with third countries**, regional and international organisations, including through an informal EU **Cyber Diplomacy Network**	HR with COM	The EU is reflecting on how to strengthen and expand the current set of cyber dialogues. Currently Cyber Dialogues take place with Brazil, China, India, Japan, Republic of South Korea, and U.S. A first EU-Ukraine Cyber Dialogue took place on 3 June 2021. Furthermore, the Trade and Cooperation Agreement (TCA) with the United Kingdom foresees to endeavour the establishment of an EU-UK Cyber Dialogue. With the EU Delegations, as well as in relevant Member States' embassies around the world, preparations are underway to form an informal EU Cyber Diplomacy Network to promote the EU vision on cyberspace, exchange information and regularly coordinate on developments in cyberspace. The Cyber Diplomacy Network is expected to begin work in the second half of 2021.
3.7	Reinforce the **exchanges with the multi-stakeholder community**, notably by regular and structured exchanges with the private sector, academia and civil society	COM with HR	Regular and structured exchanges with stakeholders, including the private sector, academia and civil society should be reinforced, also within the context of reflection on the dialogues infrastructure concerning cyber issues (see 3.6 above).
3.8	Propose an EU External Cyber Capacity Building Agenda and an **EU Cyber Capacity Building Board**	COM with HR	Discussions on setting up the EU Cyber Capacity Building Board are underway. A first kick-off meeting took place in April 2021. Once established, the Board will develop the Agenda.
Cybersecurity in the EU institutions, bodies and agencies			
A.1	Regulation on **Information Security** rules common to all EU institutions, bodies and agencies	COM	The Commission is consulting other institutions, bodies and agencies and Member State national security experts with a view to adopting a proposal in Q4 2021.
A.2	Regulation on **Common Cybersecurity Rules** for EU institutions, bodies and agencies	COM	The Commission with other institutions, bodies and agencies is benchmarking cybersecurity policies and assessing the threat landscape with

Reference	Initiative	COM/High Representative	Status
			a view to adopting a proposal in Q4 2021.
A.3	New **legal base for CERT-EU** to reinforce its stability and funding	COM	The Commission, with other institutions, bodies and agencies, is considering the new common cybersecurity rules as the legal basis to reinforce CERT-EU so as to tackle the rising number of significant incidents, likely to be proposed as part of A.2 above.