Council of the European Union

Brussels, 7 June 2021
(OR. en)

8248/1/21
REV 1

LIMITE

CSC 167
CYBER 116
CIS 62
HYBRID 20

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee (Part 2)
Subject:	Improving the security culture and resilience of EU institutions, bodies and agencies and their information networks against cyber and hybrid threats and malicious activities - state-of-play of the strands of work

I. BACKGROUND

1. The European Union has been confronted in recent years by an increasing level of malicious cyber activities, hybrid threats and disinformation originating from hostile State and non-State actors. A key feature of the Strategic Agenda for 2019-2024 adopted by the European Council in June 2019 is to protect our societies from these threats. In its conclusions, the European Council called in particular on '*the EU institutions, together with the Member States, to work on measures to enhance the resilience and improve the security culture of the EU against cyber and hybrid threats from outside the EU, and to better protect the EU's information and communication networks, and its decision-making processes, from malicious activities of all kinds'*.

2. Since June 2019, this issue has also been the subject of Council conclusions adopted in December 2019[1], June 2020[2] and December 2020[3]. A discussion on the security and resilience of the EU institutions took place in Coreper in 2019, in the context of the synthesis report on working methods under the Finnish Presidency[4]. In 2020, Estonia, France, Latvia and Lithuania drew up a joint non-paper on '*Enhancing the security and resilience of European institutions, bodies and agencies*[5]', and presented their proposals to Coreper (21 October 2020), the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (5 November 2020), the Horizontal Working Party on Cyber Issues (6 November 2020) and the Council Security Committee (7 December 2020).

3. This note reviews ongoing action in EU institutions.

II. SECURITY CULTURE AND THREAT ASSESSMENT

4. As follow-up to the European Council conclusions of June 2019, several issues have already been addressed by the EU institutions. In November 2019 and January 2020, at the initiative of the Secretary-General of the Council, the Secretaries-General of the European Parliament, the Council, the Commission and the European External Action Service (EEAS) met and identified improvement areas to be worked on jointly.

5. An inter-institutional Task Force on human, digital and hybrid counter-intelligence has been put in place, associating the security directorates of the European Parliament, the Council, the Commission, and the EEAS, with a view to facilitating the exchange of knowledge, experience and information between EU institutions, streamlining the way they respond to security incidents and proposing common ways to better coordinate interactions with Member States' services. This Task Force is meant to create a bridge between the EU institutions and allow them to further align their working methods and security standards, as well as to ensure a coherent response to all kind of security incidents.

---

1 14972/19.
2 8910/20.
3 14064/20.
4 15132/19.
5 WK 12201/20 REV 1.

6. Efforts are also underway to promote security awareness among EU staff, mobilising a number of different tools according to the target audience, including inter-institutional events such as the 'Security and Safety Days' which took place online in March 2021. Discussions are ongoing with a view to achieving even more in this area with increased input from Member States willing to share their counter intelligence awareness-raising expertise and participate in actions organised by the institutions.

7. Security directorates are also working to improve their assessment of the security threats to their institutions, in order to be able to take appropriate action and mitigate risks. A case in point is a document entitled 'Landscape of threats to EUCI', produced by the GSC (ORG5) and presented for the first time to the Council Security Committee on 5 December 2019. It is anticipated that INTCEN will be asked to undertake a regular EU-wide assessment of the specific threat to the EU institutions, bodies and agencies, including on the basis of Member States' contributions.

III. RULES ON INFORMATION SECURITY AND CYBERSECURITY

8. The Council Security Committee is continuing the review of the Council Decision on the Security Rules for protecting EU Classified Information (EUCI), a key component of the '*Common approach on sharing EU classified information with EU institutions, agencies, offices and bodies*[6]', together with the intergovernmental agreement concluded between the Member States[7]. This review was launched in early 2020 to take into account experience of these rules use and the new technological challenges since their adoption in 2013. The result of this work is expected to be presented to Coreper and the Council by mid-2022.

9. In order to ensure more coherence across the EU institutions, bodies and agencies in the way they protect their information, as well as in their communication and information systems and networks, the European Commission announced, among other things, in its Communication on the EU Security Union Strategy from July 2020[8], its intention to propose '*common rules on information security and on cybersecurity for all EU institutions, bodies and agencies'*. In December 2020, the Commission issued public consultative 'roadmaps' on two separate legislative proposals on information security rules for the EU institutions, bodies and

---

6 6074/17.
7 OJ C 202 of 8.7.2011, p. 133.
8 10010/20.

agencies, and on cybersecurity rules for the EU institutions, bodies and agencies. The joint communication by the Commission and the High Representative on the EU's cybersecurity strategy for the digital decade[9] confirmed the intention.

10. The Commission is currently organising this preparatory work and impact assessments involving all EU institutions, with a view to bringing forward proposals for regulations based on Article 298 TFEU which would enable work under the ordinary legislative procedure in the European Parliament and in the Council to begin before the end of the year. Consideration will need to be given to the impact of the proposals on the prerogatives of the Council as well as on the Member States as members of the Council.

IV. SECURE COMMUNICATION AND INFORMATION SYSTEMS AND CYBER INCIDENT RESPONSE

11. In light of the COVID-19 pandemic, work is also underway in the Council to address a lack of secure voice communication and secure video-conferencing tools at the highest levels between Member States, the Council, the Commission and the High-Representative. In both cases, the GSC has proposed solutions up to the level SECRET UE/EU SECRET, which will shortly be submitted to Coreper.

12. Work is on track for the deployment in the Council of the agreed High Classified Information (HCI) system for information and document exchanges. By 2022, this system will be used for exchanging information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET within the Council, the EEAS and the Commission. The system uses the same technology as the new high classified system to be deployed in the Commission (with functional and operational separation).

[9] 14133/20.

13. Another strand of work relates to the Computer Emergency Response Team (CERT-EU)[10]. In the course of several external assessments since it was first established, CERT-EU has demonstrated its value and positive contribution to enhancing the IT security posture of EU institutions, bodies and agencies by helping them to improve their IT infrastructure and better prevent, detect, respond to and recover from IT security incidents. In their recent joint communication on '*the EU's Cybersecurity Strategy for the Digital Decade*[11]', the Commission and the High Representative announced their intention to propose '*a new legal base for CERT-EU to reinforce its mandate and funding'*. In view of the limits to the current financial model of CERT-EU, the institutions are also considering how to make it more sustainable and whether to address the question of budget resources and posts as part of the 2022 budget proposal.

V. USE OF EU TECHNOLOGIES

14. EU institutions, bodies and agencies are actively exploring the possibilities of using state-of-the-art cybersecurity frameworks which would rely on EU technology or services.

15. In the particular area of classified information, the Council Security Rules and their implementing policies and guidelines already provide that the Commission, the EEAS and the GSC use EU-developed and EU-approved cryptographic products and equipment for EU classified networks. Member States may only use nationally approved cryptographic products and equipment for the protection of information classified up to CONFIDENTIEL UE/EU CONFIDENTIAL in their national communication and information systems (CISs).

16. With a view to reinforcing the protection of EUCI, work is ongoing in the Council Security Committee on a policy which would define rules and schemes concerning the qualification and selection of non-cryptographic security products and equipment.

---

10 OJ C 12 of 13.1.2018, p. 1.
11 16.12.2020 JOIN(2020) 18 final, pp. 24 et sq.

17. Making progress in this area requires efforts across the institutions, including strengthening staff, facilities, CISs and the protection of critical assets, and thus additional resources. However, it also raises the broader policy question of how to ensure an increased offer of software and equipment from EU industries located in the EU, given the dominance or even monopoly of non-EU hardware or software providers and, with regard to cloud technology for example, a lack of EU-located, owned and operated services which could meet all relevant operational and security requirements.

VI. WAY-FORWARD

18. Coreper is invited to take note of the ongoing efforts of the EU institutions to strengthen their security and resilience as well as to encourage the work done within the relevant existing Council preparatory bodies to contribute to that important objective.

19. Coreper will be regularly updated on the progress on the different strands of work.

ANNEX

Table security initiatives and proposals

Topic	Proposal or initiative	Objective	Responsible body/department	Estimated target
Security culture and threat assessment	Inter-institutional task-force on human, digital and hybrid counter-intelligence	Improving exchange of knowledge, experience and information between the EU institutions, making joint recommendations to streamline response to incidents, and proposing common ways to coordinate interactions with Member States' intelligence and security services	Security directorates of EP, GSC, EC and EEAS	Meeting every 2 months
	Security awareness-raising	Improving each EU institution security-awareness programmes and building on them to organise joint interinstitutional action, such as the Security and Safety Days	Security directorates of EP, GSC, EC and EEAS, possibly involving other EUIBAs and voluntary MS	Second edition of Security and Safety days in Spring 2022
	Security threat assessment	Building on each EU institution threat assessment capabilities to deliver a regular EU-wide assessment of the specific threat to the EU institutions, bodies and agencies, including on the basis of Member States' contributions through INTCEN	Security directorates of EP, GSC, EC and EEAS, possibly involving INTCEN and voluntary MS	2022
Rules on Information security and cybersecurity	Revision of the Council security rules (Decision 2013/488)	Taking into account experience of these rules use and the new technological challenges since their adoption in 2013	Council (Security Committee)	The revision started at the beginning of 2020 and is to be submitted to Coreper by mid-2022

	Proposal for a Regulation on common rules on information security for EUIBAs	Ensuring more coherence across the EU institutions, bodies and agencies in the way they protect their information	COM, EP and Council (ordinary legislative procedure)	Adoption of the proposal by the Commission foreseen in December 2021
	Proposal for a Regulation on common rules on cybersecurity for EUIBAs	Ensuring more coherence across the EU institutions, bodies and agencies in the way they protect their communication and information systems and networks	COM, EP and Council (ordinary legislative procedure)	Adoption of the proposal by the Commission foreseen in December 2021
Secure communication and information systems and cyber incident response	Secure voice communication (sVC) tool	Providing to the European Council and the Council the use of the existing solution developed by EEAS for secure voice communication up to the level SECRET EU/EU SECRET	GSC	End of 2021
	Secure video-conferencing (sVTC) tool	Providing an end-to-end video conferencing platform for discussions that are very sensitive or classified up to the level of SECRET EU/EU SECRET or their national equivalents, for EU Member States governments and EU institutions, bodies or agencies, in the context of the EU decision-making process	GSC	2022
	High-Classified Information (HCI) information exchange system	Replacing CORTESY for the exchange of documents and information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET within the Council, the MS, the EEAS and the Commission	GSC	End of 2022

	New legal base for CERT-EU	Reinforcing the mandate and funding of CERT-EU (in the framework of the proposed regulation on cybersecurity - see above)	COM, EP and Council (ordinary co-legislative process)	Adoption of the proposal by the Commission foreseen in December 2021
Use of EU technologies	New policy on non-cryptographic products and equipment for EUCI systems	Defining rules and schemes concerning the qualification and selection of non-cryptographic security products and equipment	Council (Security Committee, incl. sub-committee on Information Assurance)	Council approval first quarter 2022
	Encouraging an increased offer of software and equipment from EU industries located in the EU	Using cybersecurity frameworks relying on EU technology or services for non classified information	MS and COM	