Council of the European Union

Brussels, 7 January 2022
(OR. en)

5076/22

LIMITE

CYBER 1
COPS 6
RELEX 8
JAIEX 1
TELECOM 1
COSI 5
JAI 7
IPCR 1

PUBLIC

NOTE

From:	Presidency
To:	Permanent Representatives Committee
Subject:	EU Cyber Crisis Linking Exercise on Solidarity (EU CyCLES)

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (18.02.2022)

Delegations will find in the Annex a courtesy translation of the above information note.

Courtesy translation

Introduction

1. During its meeting on the 21-22 of October 2021, the European Council addressed the marked increase in malicious cyber activities aimed at undermining our democratic values and the security of the core functions of our societies. It stressed the need for effective coordination and preparedness in the face of cybersecurity threats. Finally, it emphasised the importance of further developing the EU cybersecurity crisis management framework and an efficient EU-level response to large-scale cybersecurity incidents and crises, including through exercises[1].

2. In 2017, the Commission submitted a recommendation (known as "Blueprint") suggesting that Member States and the European institutions reach an agreement on cooperation procedures and exchanges at EU level for the management of major incidents and cyber crisis. Three levels of crisis management were identified: technical, operational and political. The Council then called, in June 2018[2], for the establishment of a European cooperation framework for cyber crisis management respecting the competencies of the Member States.

3. At the internal level, coordination between national cybersecurity authorities is currently based on the CSIRTs network (at the technical level) and the CyCLONe[3] network (at the operational level), both of which providing a relevant framework for coordination in the event of a cyber incident. The multiplication of discussions in these formats has already made it possible to create favourable conditions for genuine European coordination in the event of large-scale incidents.

---

1 European Council meeting (21 and 22 October 2021) – Conclusions. EUCO 17/21.
2 EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises - Council conclusions (26 June 2018). 10086/18
3 *Cyber Crisis Liaison Organisation Network*

4. The latest major events (Solarwinds and Microsoft Exchange compromises) have also shown the interest for Member States to be able to conduct a relevant assessment of the severity and impact of an attack targeting them within a limited timeframe. In addition, in order for the European Union to be able to respond effectively in the event of a major crisis, it seems necessary to more closely link these newly established networks of Member states with the Council entities, in particular the Horizontal Working Party on Cyber Issues (HWPCI), the Political and Security Committee (PSC) for matters relevant to its work, as well as COREPER.

5. On the external side, the adoption in 2017 and implementation of the Cyber Diplomatic Toolbox[4] has enabled the EU to signal several times the inadmissibility of cyber malicious activities conducted from abroad. The EU has adopted a horizontal sanctions regime in May 2019, used twice in July and October 2020. However, in order to respond to the multiplication of cyber malicious activities, essentially below the threshold of armed attacks, but which could go as far as a situation corresponding to an armed attack as defined in the United Nations Charter, it seems urgent to go further and reflect on the articulation between the EU cybersecurity crisis management framework, the cyber diplomacy toolbox and the provisions of Article 42(7) TEU[5].

6. At this stage, the EU does not have an integrated framework for the effective implementation of mechanisms for mutual assistance, cooperation and coordinated response in the event of a major cyber crisis. It is in this context that the Presidency will conduct a large-scale exercise in the first trimester of 2022.

---

[4] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017. 10474/17

[5] Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade. 6722/21

DELETED FROM THIS POINT UNTIL THE END OF THE DOCUMENT (page 5)