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

NOTE

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

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

Elements of the scenario

1. The scenario of the EU CyCLES exercise will present a situation of gradual escalation towards a major cyber crisis and, in the final phase, an attack that could qualify as armed aggression according to the United Nations Charter.

2. From January 2022 onwards, players will be confronted with a supply chain cyber-attack progressively leading to the saturation of the incident response capacities of two particularly targeted Member States.

3. In this scenario, the crisis will also have socio-economic effects in several other Member States. However, effects outside the digital sphere will remain relatively limited until the last stage of the scenario. One of the objectives will be to highlight the importance of EU cooperation at this precise moment, when facing an imminent, while the crisis is still a cyber crisis but could generate much more severe effects if the vulnerabilities are not addressed, including possibly through cyber mutual assistance at operational level.

4. The second phase of the exercise will focus more on the diplomatic response to identified malicious cyber activities. The main objective will be to strengthen the EU's capacity and preparedness to use its diplomatic tools in response to a major cyber crisis.

5. In order to be as realistic as possible, the scenario will be based on incidents that have already occurred or could occur in the near future, so as to take into account the challenges that the European Union ought to be able to tackle.

Conduct phase at the EU Council

1. The exercise will be held in the Council from 14 January to 21 February 2022. It will involve the Horizontal working party on Cyber issues (HWPCI), the Political and Security Committee (PSC) for matters relevant to its work, and COREPER. Some meetings will be played while some others will only be simulated and included in the scenario injects.

2. In the first part, the focus will be on the EU's internal response to this type of crisis, in particular to identify the progress to be made in improving the framework for cooperation between Member States, as well as the role that the Institutions could play.

3. The issue will be raised at COREPER on 14 January 2022 by a Member State that has agreed to play the role of the Member State under attack. On 12 January 2022, the Presidency will present the expectations for COREPER and the other bodies that will be involved in this first phase.

   The aim will also be to initiate a discussion in COREPER (on 4 February) on the means to ensure that the political level has, in the event of a major incident, a detailed and objective analysis of the severity and impact of the cyber crisis facing one or more Member States. In this respect, the exercise will highlight the role that can be played by the cyber crisis management strategic cooperation network CyCLONe, set up in 2020.

   In the second part, information will be provided on the origin of the attack so that the crisis.The exercise will then involve activating the various bodies concerned in preparing a diplomatic response, including public attribution of responsibility for the attack and the mutual assistance mechanisms that could be activated in response to a final cyber-attack with significant kinetic effects and casualties.

   The final phase of the exercise will be played out by Foreign Ministers in the margins of the Foreign Affairs Council of 21 February 2022.