Council of the
European Union

Brussels, 7 January 2022
(OR. en)

5131/22

LIMITE

CYBER 4
COPS 7
RELEX 17
JAIEX 2
TELECOM 3
COSI 8
JAI 23
IPCR 4

NOTE

From:	Presidency
To:	Delegations
Subject:	EU Cyber Crisis Linking Exercise on Solidarity (EU CyCLES)

Delegations will find in Annexes I and II information on the EU Cyber Crisis Linking Exercise on Solidarity (EU CyCLES) and Summary of the planned sequence of events, respectively.

ANNEX I

SCENE SETTER FOR THE HWPCI DISCUSSION (21 JANUARY 2022)

Introduction to the exercise

The scenario will confront the players to a large-scale supply chain cyber-attack, with cross-border effects. Two Members States will be directly impacted from the beginning of the exercise, with critical infrastructures operators affected. A number of other Member States will not be directly targeted but will be affected (thereafter 'impacted Member States') by socio-economic impacts, a significant socio-political pressure and a large presence of the vulnerable module across countries infrastructure, potential incident therefore looming on their own critical infrastructure.

The intensity and impact of the attack will rise gradually and lead progressively to the saturation of response capabilities of several Member States, prompting a request for mutual assistance and for the elaboration of a comprehensive coordinated response.

The main objective of the exercise will be to test the cooperation between the technical, operational and political level in case of a major cyber incident[1]. Therefore, the scenario will essentially focus on the EU crisis management mechanisms (internal dimension) and on the political response the EU can provide to the attack and the attacker (external dimension, with notably the activation of the cyber diplomacy toolbox). To be realistic, the scenario is based on situations that have already occurred in real life or that we fear could occur in a near future[2] in order to address challenges the EU should tackle through a large-scale supply chain cyber attack. The kinetic of the attack will involve technical and operational as well as strategic/political consultations at the different stages of the scenario. Contribution at the technical level will be ensured by the CSIRT Network (simulated), coordination at the operational level by the CyCLONe Network and at the strategic/political level by the HWPCI/PSC, COREPER and finally at the level of Foreign Affairs Ministers.

[1] Based on the Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises. The so-called Blueprint sets out the objectives and modes of cooperation between the Member States and EU Institutions in responding to such incidents and crises.

[2] Wannacry, Not Petya (2017), Solarwinds (2020), Kaseya (2021), Microsoft Exchange (2021)

The question of attribution will be discussed but will not be central in the exercise. At the final phase, the fictitious crisis will escalate to a level where the attack could be considered an armed aggression with options including the opportunity for a Member State to invoke article 42.7 TEU. The elaboration of an adequate crisis response will be sought in the framework of the cyber diplomatic toolbox, as well as beyond due to the gravity of the crisis.

Socio-economic context and main actors of the EU CyCLEs scenario

The COVID-19 is still ongoing, with a similar situation as the one in the fall 2021. Neither a surge nor disappearance of the pandemic is considered. The scenario takes place in the first quarter of 2022.

At the same period, the demand for energy is high, due to demand from consumers for home heating in the winter and a surge of industrial demand due to the economic upturn after the COVID-19 crisis.

Actors typology

Targeted supply chain actor

IMCO (Industrial Manufacturer Company) is a company providing industrial systems, systems that support the conversion of raw materials into finished products, for a wide range of industries. IMCO has a strong foothold in the EU market. Its systems are widely used in the energy, industrial and transportation sector, but can also be found in the health and naval systems. Its main product line is a composition of software and hardware components involved in SCADA systems. A Supervisory Control And Data Acquisition (SCADA) system helps to monitor and control the production by industrial systems in factories or output in the energy system.

Threat actors

OT-Powner is a criminal group focusing on the search of vulnerabilities in and unlawfully accessing industrial systems. Its main source of revenue is the sale of this unlawful access to industrial systems to threat actors, including State-sponsored actors. It sells access per geographical area. Sale is restricted to threat actor groups with knowledge in industrial system attacks, so as to minimise exposure risk. OT-Powner only sells access and does not sell any 0-day vulnerability or exploit.

Blueland is a State in the neighbourhood of the European Union.

- At the political level, the EU and Blueland's views are diverging. After a revolution in 1960 and the setting up of a democratic regime, Blueland's political system has been recently shifting towards an authoritarian State. It has been dominated for the last eight years by an authoritarian leader. In November 2019, the leader has extended the length of its political mandate and is now able to govern the country without any term limitation. In parallel, political repression over the democratic opposition has been increasing and has led several opposition leaders (and former Members of Parliament) to leave Blueland and seek asylum in EU Member States. Several key leaders have sought asylum in EU Member States (the two main leaders of the opposition movement have settled in Finland and in Czech Republic since 2016). The EU has already made various declarations to politically support the democratic opposition movements. As an answer, Blueland regularly contests the European values and principles through political declarations and relations have deteriorated as a result in the past two years.

- Over the last months, the two leaders based in Finland and the Czech Republic have gained credit by openly denunciating the lack of credibility of the authoritarian leader (populism, disinformation). They encourage the population to express peacefully its discontent by putting green ribbon at their windows. The democratic opposition campaign is gaining more and more weight and Blueland fears this is the beginning of a larger scale discontent.

  At the economic level, Blueland has relative economic interdependence with the EU, especially in the sector of electronic components exports to the EU. Blueland has engaged in the negotiation of a deep and comprehensive free trade agreement (DCFTA) with the EU since 2011 but has not yet concluded it. Despite a recent economic crisis that weakened the country's economy, and particularly its financial system, Blueland positions itself as a global power aiming to strengthen its influence worldwide;

  The export of critical components will be blocked at the beginning of February due to rising tensions between Blueland and the EU.

- Visa liberalisation's talks have also started in 2016 but are on hold;

BlueDawn is a threat actor that is known for compromising a large variety of companies across sectors. It is a criminal group whose ties to Blueland have been highlighted in the past at several occasions (used as a proxy in some cyber campaign aiming at destabilising some political opponents to Blueland).

Timeline for the start of the exercise

Sat, 08/01/22	**Incident detection**	Simulated
The initial attack is discovered by Finland and consists in the installation of a backdoor in a widely distributed industrial SCADA software produced by a private company (IMCO) and used in many sectors (energy, automotive, naval, industrial, health etc.). Following a notification from a power company in Finland with an unknown code identified during a routine security assessment on the 8th of January, the cyber security agency of Finland issues an alert to its constituency (cf. Annex 2). On the same day, IMCO releases a security advisory on its websites (cf. Annex 3).		

Mon, 10/01/22	**CSIRTs network alert and first assessments**	Simulated
The cybersecurity agency of Finland shares its alert with the CSIRT Network to notify members of a critical vulnerability in the SCADA component of IMCO. Some members of the CSIRTs Network raise concerns that the attack might simultaneously target several essential sectors to the functioning of the economy and of the society.		

<table>
<tr><th>Fri, 14/01/22</th><th>COREPER Meeting (AOB)</th><th>Played</th></tr>
<tr><td colspan="3">During an AOB, Finland informs the Council that irregularities in power generation have occurred within its territory and can be linked to the installation of a backdoor in a widely distributed industrial SCADA software produced by a private company (IMCO) and used in many sectors (energy, automotive, naval, industrial, health etc.). It also warns of likely vulnerabilities in other Member States and possible cross-border effects.

The COREPER is foreseen to ask the HWPCI to provide a general assessment of the severity and impact of the crisis across the EU and to report back by quickly mobilizing the relevant actors to provide shared situational awareness.</td></tr>
</table>

<table>
<tr><th>Fri, 21/01/22</th><th>HWPCI Meeting</th><th>Played</th></tr>
<tr><td colspan="3">The Presidency reports on the AOB in COREPER and Finland gives an update on the situation. Czech Republic also shares its concerns on the incidents affecting their health sector. Two of their principal hospitals have faced irregularities affecting equipment for supervising fire protection but also equipment more specific to their core activities, such as consoles for supervising imaging modalities (scanner, MRI, etc.) analysis equipment, systems for supervising sterilisation chains or temperatures of refrigerated cabinets, etc.

All Member States are invited to comment on and indicate what course of action they recommend, in particular as regards the mobilization of relevant networks, including CyCLONe.</td></tr>
</table>

Guiding questions for the 21 January HWPCI

1. *What is your current assessment of the situation based on the information available?*

2. *What should be priorities and next steps to further develop shared situational awareness on the current incidents? What role would you see for CyCLONe to develop common situational awareness?*

3. *What other EU actors would you recommend to task in order to have a full picture of the crisis and to start preparing a coordinated response?*

ANNEX II

Summary of the planned sequence of events (*Color key : Blue = simulated ; green = played ; yellow = scenario injects ; White = post exercise work)*

Date	Events
8 January	Incident is detected
11 January	CSIRTs network alert
14 January	**COREPER meeting** (launch of the exercise) Finland raises an AOB and COREPER is expected to task the HWPCI to prepare a general assessment of the impact of the crisis
	Objectives: • ***Establish from the start a high political level of handling of this cyber incident in order to underline the severity of the incident that justifies the quick activation of all actors involved***
21 January	**HWPCI meeting** Discussion on actions for building shared and common situational awareness
	Objectives : • ***Emphasize the role of the HWPCI as information hub for Member States during a cyber crisis*** • ***Underline the contribution of CyCLONe in assessing the severity of the crisis, in addition to those of INTCEN, CERT-EU and other stakeholders involved***
27 January	**CyCLONe executives meeting** Exchange on the European report
	Objectives : • ***Discuss common needs regarding mutual assistance in case of a major crisis and possible paths for action for an more efficient EU-level response*** • ***Better define CyCLONe's interactions with the Council***

27 January	IPCR activated in information exchange mode
4 February	**COREPER meeting** European report is presented – Discussion and COREPER is foreseen to task the HWPCI with the follow-up
	Objective : • ***Raise awareness on the stakes of a large-scale Cyber crisis at COREPER level***
4 February	Inject gives information on the origin of the attack
8 February	**HWPCI meeting** Discussion on EEAS options note – issue raised to PSC due to impact and need to have horizontal view on EU relations with the attacker
	Objectives : • ***Underline the necessity to link a comprehensive assessment of the impact and severity of the crisis and the determination of the diplomatic response*** • ***Further test the capacity of the HWPCI to use the cyber diplomacy toolbox in response to a large-scale cyber crisis***
10 February	**PSC meeting** Discuss a possible diplomatic response – foreseen to agree on initial actions, including an HR Declaration on behalf of the EU
	Objectives : • ***Raise awareness at PSC ambassadors level on how cyberattacks can be used to threaten the security of the EU and its MS*** • ***Underline how the EU and Member States could use the cyber diplomacy toolbox to respond to a large-scale cyberattack***

11 February	Inject raises significantly the impact and severity of the attack, with kinetic effects and casualties IPCR activated in full mode
11 February (evening)	Emergency meeting of the COREPER
14 February	Meeting of the Interior ministers
21 February	**FAC meeting** Discuss the impact and severity of the cyber crisis, and agree on the EU response, including CFSP tools as part of the cyber diplomacy toolbox, as well as possible actions by the Commission and/or Member States.
	<u>Objectives</u> : • ***Raise awareness at Foreign Ministers' level on the stakes of a large-scale cyber crisis as well as the possible EU response tools and mechanisms*** • ***Start a discussion on possible MS contributions in response to a possible invocation of 42.7 TEU following a cyberattack with kinetic effects and causing casualties***
21 February	Press release about the exercise CyCLES
March	Preparation of an After Action Report
7-9 June	*Cyber Europe* (ENISA-led exercise)