Council of the European Union

Brussels, 28 January 2022
(OR. en)

5795/22

LIMITE

CYBER 34
COPS 39
RELEX 111
JAIEX 9
TELECOM 32
COSI 31
JAI 114
IPCR 15

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	5131/22
Subject:	EU Cyber Crisis Linking Exercise on Solidarity (EU CyCLES)

Delegations will find in the Annex the Cyber exercise scene setter, for discussion in the HWPCI on 1st February 2022 and in COREPER II on 4 February 2022.

1. 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.

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.

2. 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.

---

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)

3. 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).

5. Materials

For these meetings, HWPCI delegates will be given:

– The scene setter updated with latest events ;

– A European report written by CyCLONe executives assessing the situation (sent through CyCLONe officers channel) ;

- An executive summary of ISAA report (IPCR).

4. Updated timeline of events

Sat, 08/01/22	**Incident detection**	Simulated
The initial attack was discovered by Finland and consisted 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 issued an alert to its constituency (cf. Annex 2). On the same day, IMCO released 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 shared 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.		

Fri, 14/01/22	**COREPER Meeting (AOB)**	Played
During an AOB, Finland informed 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 tasked the HWPCI to provide a general assessment of the severity and impact of the crisis across the EU and to report back after quickly mobilizing the relevant actors to provide shared situational awareness.		

Fri, 21/01/22	**HWPCI Meeting**	Played

The Presidency reported on the AOB in COREPER and Finland gave an update on the situation. Czech Republic also shared 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.

- Member States pointed out the need to develop common situational awareness including through the preparation of a situation report by CyCLONe ;
- They also flagged the need to mobilize CERT-EU, INTCEN and EUROPOL in order to collect further information on the incidents;
- The HWP Chair asked EEAS to stand ready to produce an options note for the implementation of the cyber diplomacy toolbox when more information is available on the origin of the attack.

Sat, 22/01/22	**Compromising of ACER**	Simulated
The Agency for the Cooperation of Energy Regulators (ACER) is affected by the lateralization of this attack with an impact on the continuity of some of its activities within the sector (inability to control the volumes of energy traded on the European market, temporary loss of some internal tools).		

Tue, 25/01/22	**Internal alert from ENTSO-E**	Simulated
Upon suggestion from some of its members, the Secretariat of the European Network of Transmission System Operators for Electricity (ENTSO-E) notified its members of the vulnerability of IMCO modules and encouraged investigation by all grid operators.		

Tue, 25/01/22	**First CyCLONe report on IMCO vulnerability**	Simulated
First working-level exchanges held within CyCLONe in anticipation of CyCLONe extraordinary meeting showed the following elements: - Several MS face a situation of potential crisis, due to the large presence of the vulnerable component on their critical infrastructure. Moreover, investigations carried out in other Member States and by the CERT-EU shows that the backdoor is widely present in EU Member States. - The attacks worsen in already affected Member States, with major incidents across several organisation, thus stirring reflections on the qualification and management of its impact. - No evidence of exploitation was detected at this stage in other countries than Finland and Czech Republic. Crisis mechanisms are (or are planned to be) activated in about ten EU MS as major actors in several sectors (transportation, water sectors and also in the energy and health sectors as in **Finland** and **Czech Republic)** report the presence/use of IMCO's modules. - The outlook of the crisis is rather uncertain, with many MS reporting the situation as stable as of now, but many anticipating an uncertain or worsening future for the incident.		

Wed, 26/01/22	**Report of Finland Energy Administration**	Simulated
Energy administration of Finland noted short outages on its power grid. Controlled outages are planned to balance the grid, also affecting neighbouring states.		

Thu, 27/01/22	**Executive CyCLONe Meeting**	Played (Virtual)

In order to assess the severity of crisis and identify possible cooperation needs amongst EU MS cybersecurity authorities to mitigate the impact of the crisis, CyCLONe Executives met for an extraordinary meeting. During the meeting, CyCLONe Executives shared views on the anticipated evolution of the situation and further possible impacts. Based on the possible needs for solidarity/ mutual assistance expressed, CyCLONe Executives exchanged views on possible tools and mechanisms to be used and/or developed to meet those needs. After the meeting, Member States agreed on a consolidated European report to be presented to HWPCI and COREPER.

Fri, 28/01/22	**Activation of IPCR**	Simulated
Taking into consideration the reported impact of the crisis across the EU and in coordination with the most affected Member States, the Presidency of the EU Council decides to activate IPCR in information exchange mode and ask the Commission and the EEAS to prepare an ISAA report.		

6. Guiding questions for the HWPCI meeting of 1st of February

1. *What is your assessment of the situation at this stage? What kind of measures would you take at the national level to mitigate the impact of the crisis and prepare to respond to most affected Member States if they expressed needs for assistance? What further steps could be taken at the EU level, including by the institutions?*

2. *What further information would you need in order to have a detailed analysis of the severity and impact of the crisis? How do you assess the role of CyCLONe in such a situation and what more could it do?*