CyLEEx19: Inside a simulated cross-border cyber-attack on critical infrastructure

Today, ENISA and Europol’s European Cybercrime Centre jointly organise the first exercise of its kind to test the EU Law Enforcement Emergency Response Protocol.

Published on October 31, 2019



Tagged with

* [ENISA](https://www.enisa.europa.eu/search?Subject%3Alist=ENISA)
* [Cyber Attacks](https://www.enisa.europa.eu/search?Subject%3Alist=Cyber%20Attacks)
* [Cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=Cybersecurity)
* [EUROPOL](https://www.enisa.europa.eu/search?Subject%3Alist=EUROPOL)
* [Cyber Crisis Cooperation](https://www.enisa.europa.eu/search?Subject%3Alist=Cyber%20Crisis%20Cooperation)
* [Cyber Crisis Management](https://www.enisa.europa.eu/search?Subject%3Alist=Cyber%20Crisis%20Management)

“Hola bankers. Your time is running out! You have only 5 hours left to pay up the ransom before Armageddon, otherwise we will bring down your e-banking services and exfiltrate your precious data.”

This was one of the tasks set for **CyLEEx19**, the first cyber law enforcement exercise of its kind, which saw 20 cybercrime investigators and cybersecurity experts from the public and private sector come together at Europol’s headquarters on 31 October to test the [EU Law Enforcement Emergency Response Protocol](https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks) in a simulated environment.

Exercise **CyLEEx19**, organised by Europol’s European Cybercrime Centre (EC3) and the European Union Agency for Cybersecurity ([ENISA](https://www.enisa.europa.eu/)), painted a dark scenario, inspired by malicious cyber activities affecting the public and private sector across Europe and beyond. Participants were called upon to react collectively to the simulated large-scale cyber-attacks related to incidents such as misuse of IT resources, unauthorised access to systems, vulnerability exploitations, Distributed Denial of Service (DDoS), and malware infections.

Participants were asked to respond to these cyber incidents and decide on the optimal response measures, including if such threats warrant the triggering of the emergency response procedure. By performing the majority of the processes documented in the Protocol, the participants increased their preparedness in case of a real-life international cyber-attack and identified possibilities for improvement of the process.

Cybercrime investigators from the [Joint Cybercrime Action Taskforce (J-CAT)](https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce), namely France (*Police Nationale*), the Netherlands (*Politie*), Spain (*Policia Nacional*) and Norway (*Politiet*) took part in this exercise, alongside representatives from [EC3’s Advisory Groups](https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners) on financial services (Banco Santander and Citi) and the internet security industry (Palo Alto Networks), together with experts from Europol, ENISA and Eurojust.

**The EU Law Enforcement Emergency Response Protocol**

In the wake of the 2017 WannaCry and NotPetya attacks, the Council of the European Union adopted the new [EU Law Enforcement Emergency Response Protocol](https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks) to address the growing problem of planning and coordinating between governments, agencies, and companies when cyber-attacks occur across international boundaries. The Protocol is part of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises (Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises C/2017/6100).

The EU Law Enforcement Emergency Response Protocol determines the procedures, roles and responsibilities of key players both within the EU and beyond; secure communication channels and 24/7 contact points for the exchange of critical information; as well as the overall coordination and de-confliction mechanism.

This cyber simulation exercise was developed within the EMPACT 2019 Operational Action Plan Cyber Attacks against Information Systems (CAIS) under the leadership of France as action leader. The exercise is also part of the cooperation framework set up under the Memorandum of Understanding signed by European Union Agency for Cybersecurity (ENISA), the European Defence Agency (EDA), the European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU).

The outcomes of the exercise and the feedback provided by the participants in the evaluation stage will be analysed by Europol’s European Cybercrime Centre and ENISA. Detailed lessons learned will be set forth in order to establish a list of actions to improve cyber resilience and the emergency response to large-scale cyber-attacks in Europe and beyond.