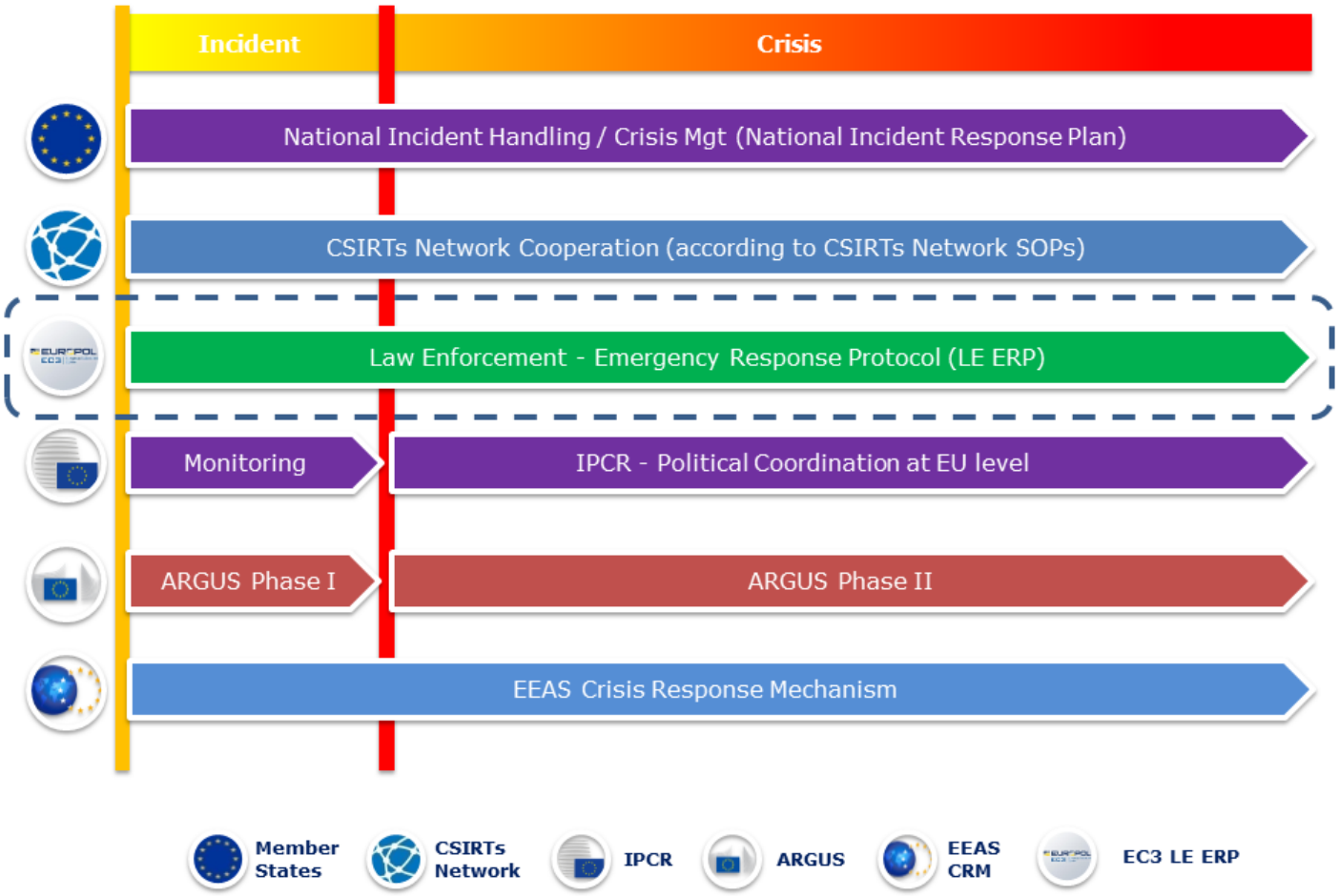
LAW ENFORCEMENT AGENCIES ACROSS THE EU PREPARE FOR MAJOR CROSS-BORDER CYBER-ATTACKS

18 Mar 2019

Press Release



The possibility of a large-scale cyber-attack having serious repercussions in the physical world and crippling an entire sector or society, is no longer unthinkable. To prepare for major cross-border cyber-attacks, an EU Law Enforcement Emergency Response Protocol has been adopted by the Council of the European Union. The Protocol gives a central role to Europol's European Cybercrime Centre (EC3) and is part of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises[1]. It serves as a tool to support the EU law enforcement authorities in providing immediate response to major cross-border cyber-attacks through rapid assessment, the secure and timely sharing of critical information and effective coordination of the international aspects of their investigations.

In 2017, the unprecedented WannaCry and NotPetya cyber-attacks underlined the extent to which incident-driven and reactive responses were insufficient to address rapidly evolving cybercriminal modus operandi effectively.

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. It strives to complement the existing EU crisis management mechanisms by streamlining transnational activities and facilitating collaboration with the relevant

EU and international players, making full use of Europol's resources. It further facilitates the collaboration with the network and information security community and relevant private sector partners.

Only cyber security events of a malicious and suspected criminal nature fall within the scope of this Protocol; it will not cover incidents or crises caused by a natural disaster, man-made error or system failure. Therefore, in order to establish the criminal nature of the attack, it is fundamental that the first responders perform all required measures in a way to preserve the electronic evidence that could be found within the IT systems affected by the attack, which are essential for any criminal investigation or judicial procedure.

MULTI-STAKEHOLDER PROCESS

The protocol is a multi-stakeholder process and entails in total seven possible core stages from the early detection and the threat classification to the closure of the Emergency Response Protocol.

"It is of critical importance that we increase cyber preparedness in order to protect the EU and its citizens from large scale cyber-attacks", Wil van Gemert, Deputy Executive Director of Operations at Europol, said. "Law enforcement plays a vital role in the emergency response to reduce the number of victims affected and to preserve the necessary evidence to bring to justice the ones who are responsible for the attack."

As the EU Agency for law enforcement cooperation, Europol is mandated to support the Member States' endeavours to effectively detect, investigate, disrupt and deter large-scale cyber incidents of a suspected criminal nature.

--

[1]Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises C/2017/6100

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
SUPPORT & SERVICES	Operational coordination • Operational support

---