Parliamentary Dimension

romania2019.eu
Romanian Presidency of the Council of the European Union

European Cybercrime Centre (EC3): State of play and activity report including support against counterfeiting of non-cash means of payment, monitoring and countering dark web crimes

Europol set up the European Cybercrime Centre **(EC3)** in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus help to protect European citizens, businesses and governments from online crime. Since its establishment, EC3 has made a significant contribution to the fight against cybercrime: it has been involved in tens of high-profile operations and hundreds on-the-spot operational-support deployments resulting in hundreds of arrests, and has analysed hundreds of thousands of files, the vast majority of which have proven to be malicious. While it is difficult to provide reliable estimates, some industry reports suggest that the global cybercrime costs are in the hundreds of billion of euros per year[1].

Each year, EC3 publishes the Internet Organised Crime Threat Assessments **(IOCTA),** its flagship strategic report on key findings and emerging threats and developments in cybercrime.

Fighting cybercrime is the first out of ten of Europol's priorities of the four-year Policy Cycle for the 2018-2021 period. This priority is performed by:

1. Disrupting the criminal activities related to attacks against information systems;
2. Combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material; and
3. Targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities.

The patchwork of separate, territorially defined national jurisdictions in the area of fight against cybercrime causes difficulties in determining the applicable law in transnational interactions and gives rise to legal uncertainty, thereby preventing police and judicial cooperation across borders, which is necessary to deal efficiently with cybercrime.

In September 2017, the Commission adopted a new package on cybersecurity with a wide-ranging set of measures to reinforce the EU's resilience and response to cyber-attacks. The package comprises several elements that are of direct relevance to Europol, as outlined in the Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[2] , the proposal for a Directive on Non-Cash Payment Fraud[3] and the Recommendation "on Coordinated Response to Large Scale Cybersecurity Incidents and Crises"[4].
21/02/2019

---

1 Source: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

2 JOIN(2017) 450 final

3 Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (COM(2017) 489 final) 4 Commission Recommendation of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (C(2017) 6100 final)

4 Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area, 6 June 2016, Council Secretariat file no. 9368/1/16