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

Fighting cybercrime is one 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.

Three specific operational action plans are implementing this priority.

The so-called "dark web", understood as underground illegal economy, is a key-enabler for cybercrime and a fertile environment for criminals due to its structural specificities, *i.e.* the possibility to buy and sell anonymously and the fact that this is a digital space without borders. The dark web hosts many of the critical marketplaces for several criminal organisations and individual illegal activities in Europe and around the world.

The European Cybercrime Centre (EC3), launched in January 2013, supports cybercrime investigations in the EU Member States and gathers intelligence on new cybercriminal threats. In order to reduce the size of the dark web, EC3 aims to pool cyber intelligence and resources, share tools, tactics and techniques to fight the most impactful cybercrime networks at the EU level, in close coordination with key law enforcement authorities from third countries.

Fraud and counterfeiting of non-cash means of payment is a threat to security, representing a source of income for organised crime and an enabler for other criminal activities such as terrorism, drug trafficking and trafficking in human beings. The cross-border dimension of that crime is accentuated by an increasing digital component.

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. This has an impact on security. The EU legislation (Council Framework Decision 2001/413/JHA) is currently under revision in order to include further provisions on offences, in particular relating to computer-related fraud, penalties, prevention and assistance to victims and cross-border cooperation.

Parliamentary Dimension

romania2019.eu

Romanian Presidency of the Council of the European Union

31/01/2019