# EUROPEAN CYBERCRIME CENTRE - EC3

Combating crime in a digital age

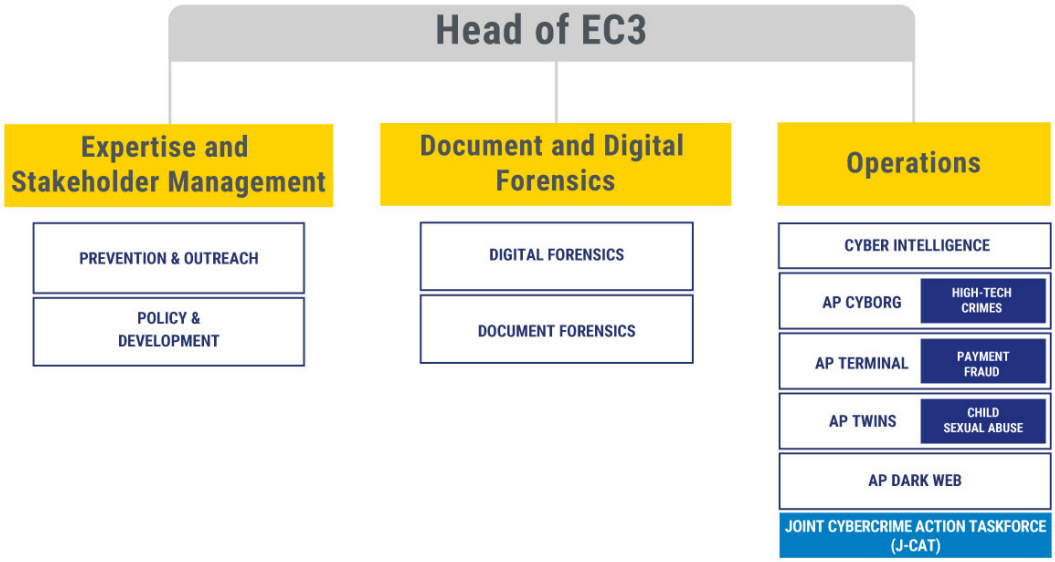
**ABOUTEC3 UPDATES**

Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help 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 billions of euros per year.

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

The IOCTA demonstrates how wide and varied cybercrime is and how EC3 is a key part of Europol's, and the EU's, response. EC3 takes a three-pronged approach to the fight against cybercrime: forensics, strategy and operations.




The EC3 Programme Board provides EC3 with direction as to how to achieve its goals and fulfil its officially assigned tasks, building on partnerships, shared responsibility and cooperation with all board members.

EC3 has two forensics teams, digital forensics and document forensics, each of which focuses on operational support, and research and development.

There are two strategy teams:

1. prevention and stakeholder management, which establishes partnerships, ensures the development of standardised training and coordinates prevention and awareness measures;
2. strategy and development, which is responsible for:
   - strategic analysis;
   - the formulation of policy and legislative measures;
   - internet governance.

At the level of operations, EC3 focuses on the following types of cybercrimes:

- Cyber-dependent crime;
- Online child sexual exploitation;

- Payment fraud.

These activities are also supported by the Cyber Intelligence Team (CIT), whose analysts collect and process cybercrime-related information from public, private and open sources and identify emerging threats and patterns.

Working alongside EC3 is the Joint Cybercrime Action Taskforce (J-CAT), which works on the most important international cybercrime cases that affect EU Member States and their citizens.

EC3 draws on Europol's existing law-enforcement capacity—but it also expands significantly on other capabilities, in particular by offering operational and analytical support to Member States' investigations.

For each of the three categories of cybercrime, EC3:

- serves as the central hub for criminal information and intelligence;
- supports operations and investigations by Member States by offering operational analysis, coordination and its considerable expertise;
- provides a variety of strategic-analysis products that enable informed decision-making at the tactical and strategic levels on combating and preventing cybercrime;
- provides a comprehensive outreach function connecting law-enforcement authorities tackling cybercrime with the private sector, academia and other non-law enforcement partners;
- supports training and capacity-building, in particular for the relevant authorities in Member States;
- provides highly specialised technical and digital forensic support capabilities to investigations and operations;
- represents the EU law-enforcement community in areas of common interest (research-and-development requirements, internet governance and policy development).

The EC3 Programme Board provides EC3 with direction as to how to achieve its goals and fulfil its officially assigned tasks, building on partnerships, shared responsibility and cooperation with all board members.

Cybercrime is one of the EMPACT priorities, Europol's priority crime areas, under the 2018–2021 EU Policy Cycle.

EC3 Programme Board

EC3 Partners

EUCTF

CRIME AREAS

Cybercrime • High-Tech crime • Social engineering • Child Sexual Exploitation • Forgery of money and means of payment • Payment Fraud • Money Muling

Cybercrime is one of the EMPACT priorities, Europol's priority crime areas, under the 2018–2021 EU Policy Cycle.

EC3 Programme Board

EC3 Partners

EUCTF

---

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