EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

© Shutterstock

© Yarche - Fotolia

COMBATING CRIME IN A DIGITAL AGE

© Shutterstock

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

A collective EU response to cybercrime

Following a feasibility study conducted by Rand Corporation Europe, the European Commission decided to establish a European Cybercrime Centre (EC^3) at Europol. The Centre will be the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. It will support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners.

EC^3 officially commenced its activities on 1 January 2013 with a mandate to tackle the following areas of cybercrime:

a. That committed by organised groups to generate large criminal profits such as online fraud
b. That which causes serious harm to the victim such as online child sexual exploitation
c. That which affects critical infrastructure and information systems in the European Union

Cybercrime


© Shutterstock

In line with the Budapest Convention on Cybercrime, the scope of EC[3] encompasses those crimes that are directed against our computer and network infrastructures as well as crimes committed online. This covers all crimes from malware, hacking, phishing, intrusion, manipulation, identity theft and fraud, to the grooming and online sexual exploitation of children.

Focal Point (FP) Cyborg supports EU Member States in preventing and combating different forms of cyber criminality, especially those cybercrimes associated with organised criminal groups or organisations.

Cyborg can support the Member States' investigations into cyber incidents, in particular with regard to attacks targeting critical infrastructures.

Child Sexual Exploitation


© Shutterstock

'Child sexual exploitation' refers to the sexual abuse of a human being below the age of 18. It includes the production of child abuse images and their online dissemination as particularly serious forms of crime committed against children.

FP Twins aims to identify perpetrators and establish cross-links within the participating Member States. It further identifies cross-border modus operandi and analyses the methods of communication of criminal networks, with a view to dismantling those networks.

The FP focuses also on the identification of the victims, with a view to stopping potentially on-going exploitation and to make it possible to initiate care measures by the competent authorities. FP Twins cooperates on an operational level via the Europol Liaison Officers' (ELO) network, provides strategic and operational analytical support, and supports international projects such as COSPOL Internet Related Child Abuse Material Project (CIRCAMP) and the European Financial Coalition (EFC).

Payment Card Fraud


© Ludovic - Fotolia

Payment card fraud (PCF) is a low risk and highly profitable criminal activity which brings organised crime groups (OCGs) originating from the EU a yearly income of around 1.5 billion euros.

Focal Point Terminal provides support to EU law enforcement authorities (LEAs) in hundreds of international PCF investigations. The specialised team produces analytical reports and facilitates cooperation to combat PCF crimes. Analysis reports provide LEAs with findings, such as relations between persons, phone numbers and communication tools, as well as intelligence gaps and hypotheses. Support is given on the spot through the mobile office, which allows access to Europol databases via a secure connection. In addition a universal forensic extraction device kit (UFED) can be deployed, which is capable of obtaining data from digital data storage devices, e.g. phones, PDAs, navigation devices and SIM cards. A card reader enables a quick check of data on a payment card and a database with card numbers can give information on the card issuer.

Data Fusion

The Data Fusion Centre ensures information collection on cybercrime from the widest array of public, private and open sources in order to enrich available police data. It acts as an analytical hub, processing and analysing, critical information from various sources on an ongoing basis. The goal is to broaden the information picture on cybercrime in Europe over time so as to rapidly identify emerging threats.

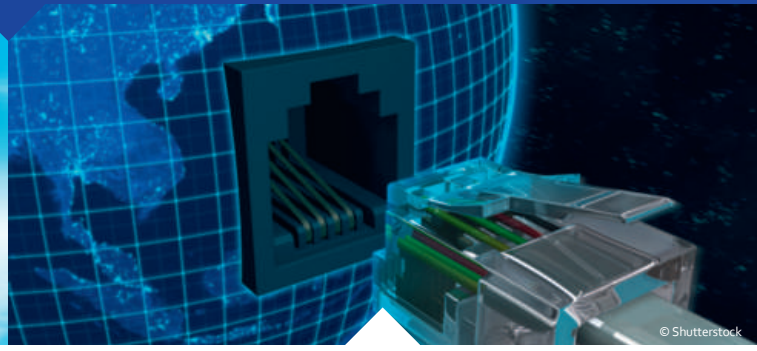
By offering state-of-the-art technology, the Data Fusion Centre will connect law enforcement authorities, the Computer Emergency Response Team (CERT) community, private sector specialists and academia. It will serve as the primary point of contact to report cybercrime investigations. This will enable Member States' investigators to benefit from each others information in investigations. Law enforcement, public and private partners can turn to the Centre to support their multidisciplinary cyber investigations and deliver emergency services.

Forensics

The EC^3 can provide a variety of forensic support services. This includes specialist tools and an analysis laboratory from where digital, network and mobile device forensic analysis are carried out. EC^3 further provides:

- Computer forensic infrastructure and a digital forensic lab
- Faraday environment
- Mobile lab – a vehicle equipped with (semi) portable laboratory equipment and on-the-spot investigation equipment
- Technical investigation on raw materials and printing devices used for counterfeiting of banknotes and documents
- Suspected counterfeit banknotes examination (we are running for an accreditation following the ISO17025 standard, which is the highest measurable standard available)
- (Secure) document examination, e.g. tax stamps, brand labels and ID documents
- Additional visual CSI services such as crime light sources to indicate and inform Member States about additional forensic traces at a crime scene
- Forensic CSI photography to support Member States on the spot is currently being developed.

Outreach



The outreach function develops and maintains all partnerships that can contribute to the EU response to cybercrime. This service includes the proactive identification of new partners where required and cooperation with law enforcement agencies, EU institutions, international organisations, private industry, the public sector and academia.

Outreach ensures that EC^3 communicates with its partners with one voice by providing a framework for engagement. It will also build an overview of the Member States' capacity to combat cybercrime, including the development of forums and projects and Public Private Partnerships at national and international levels. This will assist EC^3 in targeting assistance to where it is most needed and avoiding unnecessary overlaps in anti-cybercrime initiatives.

Strategy


© James Steidl - Fotolia

The purpose of EC^3 Strategy & Prevention is to make the citizens and businesses of the EU safer through increased insight, knowledge and awareness raising. The EC^3 analyses large amounts of data from a variety of sources - both crime data and open sources - to understand how cybercriminals, child sex offenders and fraudsters think and operate. What we learn not only helps law enforcement target its operations more effectively: it also informs changes in policy and legislation and, most important of all, is the basis for our advice to citizens and businesses on how to protect themselves from online threats.

Cybercrime evolves on a daily basis - there are always new vulnerabilities, new criminal methods, new environments for offending and new victims. That's why Strategy & Prevention monitors developments in emerging technologies, and scans the horizon to find out what's coming next. Currently we're leading Project 2020, a strategic foresight initiative for the International Cyber Security Protection Alliance (ICSPA) on the future of cybercrime.

Research & Development


© Photosani - Fotolia

Needs in Research & Development (R&D) are considerable. Understanding, mitigating and preventing online threats all depend on fundamental research. EC^3 will actively coordinate R&D input as part of the Commission's Program Horizon 2020.

Capitalising on all law enforcement cyber investigators, EC^3 will participate in streamlining R&D activities in line with the reality of this very dynamic threat.

At the same time, EC^3 will support the community-based development of some tools for law enforcement.

Training


© Iceteaimages - Fotolia

Cybercrime is in itself a very demanding topic for public services. Today not all Member States have reached a level of knowhow required to start an effective fight against cybercrime.

Cyber units sometimes do not have the hardware and the software they need to perform simple forensic extractions. EC^3 will support Member States' capacity building by linking EU funding with law enforcement actors.

Training will be facilitated, in line with ECTEG norms, and in cooperation with CEPOL. The advanced high level training organised in Selm will remain a cornerstone of the layout.

A European Union free from cybercrime

EC³ aims to become the focal point in the EU's fight against cybercrime, through building operational and analytical capacity for investigations and cooperation with international partners in the pursuit of an EU free from cybercrime.

The European Cybercrime Centre is hosted by Europol; the European law enforcement agency in The Hague, The Netherlands, and thus EC³ can draw on Europol's existing infrastructure and law enforcement network. Europol is already Europe's specialist law enforcement centre for operational support, coordination and expertise in cybercrime. The European Cybercrime Centre will provide a more collaborative response in cooperation with:

- EU Member States;
- key EU stakeholders;
- non-EU countries;
- international organisations;
- internet governance bodies and service providers;
- companies involved in internet security and the financial sector;
- academic experts;
- civil society organisations;
- National Computer Emergency Response Teams (CERTs) and the CERT-EU.

EC³ Programme Board

The advisory role of the EC³ Programme Board is to assist the centre in its governance process.

The members of the Programme Board are currently:

EUCTF (European Union Cybercrime Taskforce)
CIRCAMP (COSPOL Internet Related Child Abusive Material Project)
ENISA (European Network and Information Security Agency)
ECTEG (European Cybercrime Training and Education Group)
CEPOL (European Police College)
EUROJUST (European Union's Judicial Cooperation Unit)
CERT-EU (Computer Emergency Response Team)
INTERPOL (International Criminal Police Organization)
European Commission
EEAS (European External Action Service)

QL-01-13-551-EN-C

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

Visitor address:
Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

Postal address:
P.O. Box 90850
2509 LW The Hague
The Netherlands

Telephone:
+31 70 302 5000

E-mail:
ec3@europol.europa.eu

www.europol.europa.eu/ec3