European Cybercrime Centre

Fighting cybercrime in Europe and beyond

Joint Cybercrime Action Taskforce (J-CAT)

EUROPOL BASIC PROTECTION LEVEL
RELEASABLE TO LAW ENFORCEMENT ONLY

EUROPOL | EC3 European Cybercrime Centre

Fighting cybercrime in Europe and beyond

Cybercrime knows no boundaries

Cybercriminals are constantly coming up with new ways to profit from their crimes at the expense of citizens, businesses and governments, across national borders and jurisdictions.

Police forces around the world encounter many forms of complex and innovative cybercrimes, which calls for a swift, coordinated, international approach to the problem.

The J-CAT was launched in September 2014 to respond to that need.

Objective

J-CAT's objective is to drive intelligence-led coordinated actions against key cybercrime threats and targets. This is done by facilitating the joint identification, prioritisation, preparation, initiation and execution of cross-border investigations and operations by its partners.

In particular, it tackles:

- **cyber-dependent crimes** (such as malware, botnets, ransomware and intrusion);
- **transnational payment fraud**
- **online child sexual exploitation**
- **the facilitation of crimes** (such as criminality on the Dark Web, bulletproof hosting, counter-antivirus services, infrastructure leasing and rental, money laundering, including the abuse of virtual currencies).

The Joint Cybercrime Action Taskforce (J-CAT) is a 24/7 permanent taskforce, operating from Europol headquarters together with the European Cybercrime Centre. It helps fight cybercrime within and outside the EU.

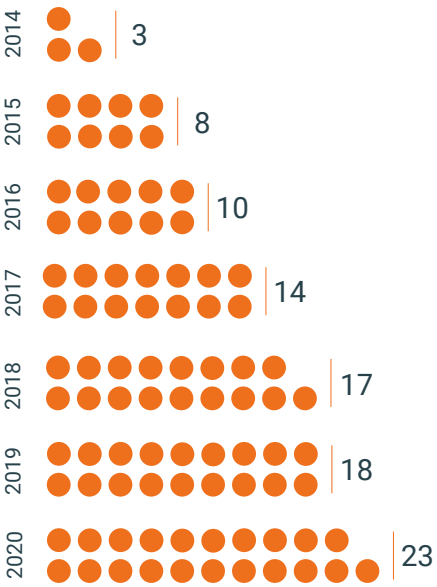
Methodology

J-CAT chooses and prioritises which cases to pursue based, among others, on proposals from the J-CAT members.

They:

1. select the most relevant proposals;
2. share, collect and enrich data on the cases in question;
3. develop an action plan, which is led by the country that submitted the selected proposal;
4. go through all the necessary steps to ensure the case is ready for law enforcement action — a process that involves consulting with judicial authorities when needed, the identification of the required resources, and the allocation of responsibilities.

Completed operations (2014-2020)



Members

J-CAT consists of a standing operational team of cyber liaison officers based at Europol and complemented by Europol's European Cybercrime Centre (EC3) staff.

At present, the liaison officers come from:

- 10 EU Member States (Austria, France, Germany, Italy, the Netherlands, Romania, Poland, Sweden, Belgium, and Spain, which is represented by two agencies: Policia Nacional and Guarda Civil);
- 7 non-EU partner countries (Australia, Canada, Colombia, Norway, Switzerland , the United Kingdom, and the United States, which is represented by three agencies: the Federal Bureau of Investigation, Secret Service and Internal Revenue Service).

The Seconded National Expert who represents Eurojust at the EC3 also attends the weekly J-CAT meetings and facilitates the judicial coordination.

Governance

J-CAT is governed by a Board composed of at least one senior law enforcement representative per participating agency.

The Board is led by a Chair-country and a Vice-Chair-country, directly elected by the Board itself.

The Board together with EC3 sets the strategic direction and addresses tactical and operational matters.

Contributions

The Taskforce is open to contributions on a case-by-case basis from non-participating countries and non-law enforcement partners. This can also be done within the framework of a J-CAT Attachment Scheme, which provides for a temporary attachment to collaborate on a cyber case with links to at least two J-CAT members.