JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)

Fighting cybercrime around the world

- J-CAT infographic
- J-CAT poster

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 thus encounter similar cybercrimes and similar criminal targets, and that calls for a coordinated, international approach to the problem.

The Joint Cybercrime Action Taskforce (J-CAT), which was launched in September 2014. Located at Europol's European Cybercrime Centre (EC3), it helps fighting cybercrime within and outside the EU.

J-CAT OBJECTIVES

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

- cyber-dependent crimes;
- transnational payment fraud;
- online child sexual exploitation;
- cross-crime cyber facilitators (e.g. bulletproof hosting, counter-antivirus services, criminal use of the dark web, etc.).

CONTRIBUTIONS

The taskforce is open to occasional 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 cybercrime case with links to at least two current J-CAT member countries.

It consists of a standing operational team of cyber liaison officers from several EU Member States and non-EU cooperation partners, who are based in Europol headquarters and complemented with EC3 staff. The cyber liaison officers come from:

- 9 EU Member States (Austria, France, Germany, Italy, the Netherlands, Romania, Poland, Sweden and Spain, which is represented by two agencies: Policía Nacional and Guardia Civil));

- 7 non-EU partner countries (Australia, Canada, Colombia, Norway, Switzerland, the United Kingdom, and the United States, which is represented by two agencies: the Federal Bureau of Investigation and Secret Service);
- Europol's European Cybercrime Centre (EC3).

All these officers work from the same office to ensure that they can communicate with each other easily.

In addition, a dedicated National Expert seconded from Eurojust to Europol's EC3 regularly cooperate with EC3 and the J-CAT to discuss cases and projects of mutual interest.

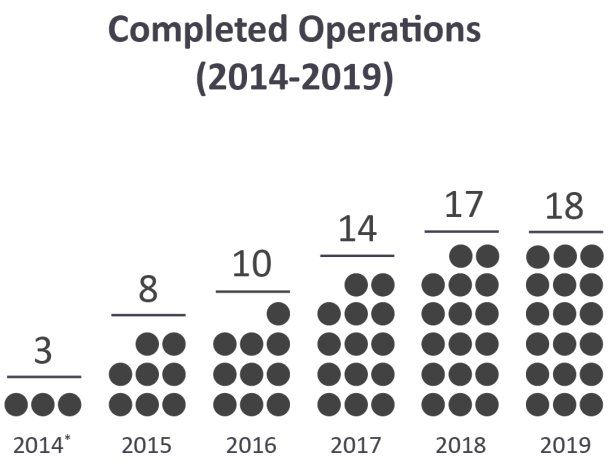
J-CAT chooses and prioritises which cases to pursue based, among other things, on proposals from the country liaison officers. Members:

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 to become a target of law enforcement action — a process that involves consulting with judicial authorities, the identification the required resources, and the allocation of responsibilities.

The 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 J-CAT Board, together with EC3, sets the strategic direction and addresses tactical and operational matters.

SUCCESSES

To date, the Taskforce was involved in multiple high-profile operations, thus contributing significantly to their success.



*The Taskforce was launched in September 2014.

Notable successes include:

- The takedown of the Imminent Monitor Remote Access Trojan (IM-RAT) which was able to give full remote control of a victim's computer to cybercriminals. This tool was used across 124 countries and sold to more than 14 500 buyers. Search warrants were executed in Australia and Belgium against the developer and one employee of IM-RAT, and 13 of the most prolific users of this tool have been arrested at this stage.
- The arrest of a 36-year old individual in the United Kingdom for the theft of around €10 million in the IOTA cryptocurrency from over 85 victims worldwide.
- The arrests in Spain, Italy and France of individuals forming WhatsApp groups to create and exchange child sexual abuse material. That exchange included the creation of emoji 'stickers' of child sexual abuse and other extreme material that were subsequently widely distributed.
- The operation actions against the DDoS marketplace webstresser.org on April 2018 and its prolific users. Webstresser.org was considered the world's biggest marketplace to hire Distributed Denial of Service (DDoS) services, with over 136 000 registered users and 4 million attacks measured by April 2018. The orchestrated attacks targeted critical online services offered by banks, government institutions and police forces, as well as victims in the gaming industry.

In addition to the operational activities, a number of roadshows were organised in 2018 and 2019 in the Netherlands, Switzerland, Norway, Germany and Sweden. These roadshows aimed at raising awareness and strengthening the collaboration with the national, regional and local cyber police units and cyber judiciary members from the current J-CAT member countries. Over 600 cyber law enforcement and judiciary practitioners took part in these roadshows which included practical demonstrations on the tools and services provided by Europol's EC3 in support of cyber cases, as well as the type of support offered by the J-CAT cyber liaison officers.

This programme of roadshows was supplemented by 4 CEPOL webinars, delivered in different languages by the J-CAT members themselves to reach out to cyber investigators at the national and local level in their own language. A further 580 participants from over 30 countries joined these webinars.

Such awareness raising activities have already resulted in concrete operational outcomes, such as an increase in the operational contributions as well as the increased use of the tools provided by Europol.

GENERAL TERMS:	Law Enforcement
CRIME AREAS:	Cybercrime • Child Sexual Exploitation • Forgery of money and means of payment • Payment Fraud
ENTITIES:	European Cybercrime Center (EC3) • Joint Cybercrime Action Taskforce (J-CAT)
TARGET GROUPS:	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists

---