**Tackling cybercrime through joint investigation teams**

07/06/2019

**Joint investigation teams are one of the most effective tools for investigators confronted with the challenge of fighting cybercrime. Due to the fast-paced, cross-border nature of cybercrime, judicial and police authorities face specific challenges, such as the need to act quickly, overcome the differences in legislation between countries concerning how to collect and secure e-evidence, ensure swift cooperation with third countries and actors in the private sector, and ensure data security. On 5-6 June, experts on joint investigation teams from national authorities and EU institutions met at Eurojust to explore how to effectively deal with these obstacles in cybercrime investigations and maximise the potential of joint investigation teams to address this growing security concern.**

To effectively tackle cybercrime, investigators in all countries concerned need to work together, map out the different legal requirements, find out how to preserve and collect e-evidence in the right way and jointly decide on the best investigative strategy. To investigate cybercrime more effectively, better cooperation with the private sector and third States is also needed.

The most effective way to ensure close cooperation between judicial authorities in the different countries concerned is to quickly form a joint investigation team (JIT), the most advanced tool in international cooperation in criminal matters. A JIT is a legal agreement between two or more countries to undertake joint transnational criminal investigations during a fixed period of time, which provides for the possibility to directly exchange data and evidence, cooperate in real time and successfully carry out urgent operations. JITs also allows for parties to be present during investigative measures on each other’s territories, and to therefore share their technical and human resources more efficiently.

Eurojust provides financial and operational support to JITs, as well as expertise and judicial analysis. To facilitate the setting up of JITs and increase their effectiveness in cybercrime cases, Eurojust and the JITs Network have developed a special cybercrime JIT template, which adapts the JIT model agreement to the specificities and needs of cybercrime cases.

The two-day expert’s meeting was attended by representatives from Eurojust, the JITs Network and the European Judicial Cybercrime Network (EJCN), which are hosted at Eurojust’s premises in The Hague, Europol and its European Cybercrime Centre (EC3), the European Judicial Training Network (EJTN), the European Union Agency for Law Enforcement Training (CEPOL), the Police Cooperation Convention for Southeast Europe Secretariat (PCC-SEE) as well as the European Commission.

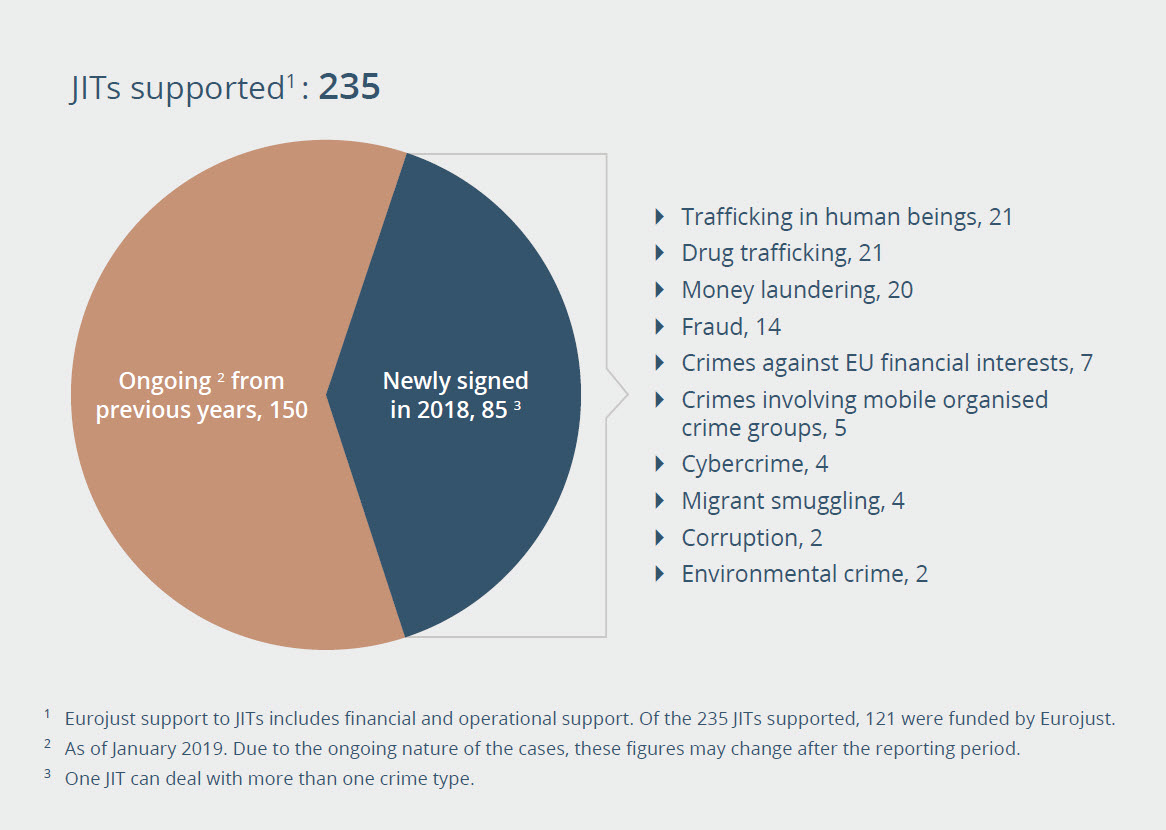
Many examples of cybercrime cases successfully were presented, which were solved also thanks to the valuable assistance offered by JITs. In the course of three workshops, national experts discussed about specific challenges and possible solutions in using JITs in cybercrime cases, such as how to trigger the establishment of JITs more proactively and how to benefit from Europol’s analysis projects in cybercrime JITs. The following advantages were highlighted by practitioners when using JITs in cybercrime cases:

* immediate preservation and exchange of electronic evidence;
* sharing of technical and human resources and expertise to cope with investigative and analytical challenges;
* development of a joint strategy based on mutual understanding of the national legal frameworks applicable for each of the JIT parties;
* close and early distribution of investigative tasks between the JIT parties, including cooperation with private actors; and
* more efficient cooperation with third States (e.g. streamlined and ‘distributed’ among JIT partners to avoid duplicates); and
* efficient handling of jurisdiction issues.

The European Commission presented legislative proposals of new rules that will make it easier and faster for police and judicial authorities to access the electronic evidence they need to catch and convict cybercriminals.

**BACKGROUND**

**Eurojust’s support to joint investigation teams**  
In 2018, Eurojust supported 235 JITs (150 ongoing, 85 newly signed), investigating a range of organised crimes, mainly trafficking in human beings (21), drug trafficking (21) and money laundering (20). One JIT can deal with more than one crime type. Eurojust hosts the JITs Network, a network of competent authorities from across Europe, who meet regularly to exchange expertise and best practice regarding the investigation and prosecution of cybercrime.

[[](http://www.eurojust.europa.eu/press/News/News/PublishingImages/2019-06-07_Chart-JITs-supported-2018-.jpg)](http://www.eurojust.europa.eu/press/News/News/PublishingImages/2019-06-07_Chart-JITs-supported-2018-.jpg)**Eurojust’s support to cybercrime investigations**  
In 2018, Eurojust played an important role in 219 cybercrime investigations, including setting up 4 JITs, 28 coordination meetings and 2 action days on cybercrime cases. Eurojust also works on a number of other levels to counteract cybercrime, including by addressing how to deal with victims of cybercrime, access to data for criminal procedure purposes, and encryption and retention of the data needed as evidence. [[Click here](http://www.eurojust.europa.eu/press/News/News/PublishingImages/2019-06-07_Chart-JITs-supported-2018-.jpg) or on image to view full chart]

Eurojust also hosts the European Judicial Cybercrime Network (EJCN) which was established in 2016 to foster contacts between practitioners specialised in countering the challenges posed by cybercrime, cyber-enabled crime and investigations in cyberspace, and to increase efficiency of investigations and prosecutions. In 2018, the EJCN dealt with victims of cybercrime, access to data, electronic evidence, training, encryption and data retention.