Council of the European Union

Brussels, 14 July 2017
(OR. en)

11220/17

LIMITE

ENFOPOL 358
COPEN 236
EUROJUST 120
CT 74
CYBER 115
COSI 164
CATS 79
JAI 688

NOTE

From:	Eurojust and Europol
To:	Delegations
No. prev. doc.:	10472/15
Subject:	Joint Eurojust-Europol Annual Report 2016 to the Council of the European Union and the European Commission

Delegations will find enclosed the above-mentioned Joint Eurojust-Europol Annual Report 2016 to the Council of the European Union and the European Commission.

Joint Eurojust-Europol Annual Report 2016 to the Council of the European Union and the European Commission

Introduction

While Europol and Eurojust have continued a close daily cooperation in their core operational activities in 2016, both organisations have also strengthened discussions at managerial and strategic level through regular Steering Committee meetings and the annual High Level meeting.

The effectiveness of this coordination and cooperation is illustrated by 3 examples in which both organisations jointly supported national authorities. These cases dealt with serious and organised crime, cybercrime and counter terrorism, including a financial crime component.

Furthermore, for the first time since the establishment of either agency, a joint meeting of the management boards of each organisation took place in December to consider strategies for enhancing cooperation.

1. Fighting serious and organised crime

Eurojust and Europol are working together in the majority of the serious and organised crime cross border cases brought by national authorities.

Both organisations are for instance steadily developing their cooperation to counter trafficking in human beings and property crime. Those areas saw a significant increase in number of Eurojust coordination meetings attended by Europol and of joint investigation teams set up. Additionally, in 2016 Eurojust became associated with another Focal Point within serious and organised crime area, namely Apate.

The European Money Mule Action, Payment Card Fraud targeting money mules is further example of such cooperation, in the field of financial crimes.

Money Mule Action

From 22 to 26 February 2016, law enforcement agencies and judicial bodies from Belgium, Denmark, Greece, the Netherlands, the UK, Romania, Spain and Portugal – with further support from Moldova and other countries – joined forces in the first coordinated European action against money muling. The operation was also supported by Eurojust, Europol and the European Banking Federation (EBF).

During the week, Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT), together with Eurojust and EBF, provided operational and analytical support to the involved partners. As a result of the operation, nearly 700 money mules were identified across Europe, and 81 individuals were arrested after 198 suspects were interviewed by law enforcement agencies. With the support of over 70 banks, significant financial losses were discovered and prevented, and over 900 victims of this crime were identified. More than 90 per cent of the reported money mule transactions were linked to cybercrime.

Eurojust and Europol's EC3 organised three operational and coordination meetings in The Hague to discuss the unique approach of each Member State to tackle money muling in their respective countries. During the action days, Europol deployed a mobile office to provide support to the Romanian authorities. The command centre was set up by Europol in cooperation with Eurojust to assist the national authorities, cross-check all incoming data against Europol's databases and collect intelligence for further analysis.

Money mules are individuals recruited by criminal organisations to receive and transfer illegally obtained money between bank accounts and/or countries. Through the money mules, the criminals gain access to the stolen goods or funds without revealing their identity. These fraudulent schemes are often advertised through online postings and social media as seemingly legitimate job opportunities.

The recruited individuals may be willing participants; however, some are unaware that their actions foster the cycle of criminal activity. Money mules may also help perpetuate other crimes beyond money laundering, as the stolen money might go towards funding other forms of organised crime, such as drug dealing and human trafficking.

The European Money Mule Action (EMMA) is a pilot operational project under the flag of the EMPACT Cybercrime Payment Fraud Operational Action Plan, designed to combat online and payment card fraud. EMMA is modelled after a Dutch example successfully employed in recent years in the Netherlands. This action builds upon the effective partnership between the police, the prosecution and the banking sector at national as well as international level.

Discussion and cooperation and coordination facilitated by both organisations ensured the common understanding needed between the law enforcement and the judicial authorities in the Member States.

Eurojust and Europol are also joining forces in tackling EU crime priorities within the EU Policy Cycle. Eurojust has an important role when it comes to supporting the setting up of Joint Investigation Teams (JITs) and coordination meetings in relation to JITs, including promoting judicial support to investigations against high value targets (HVT) identified within the EMPACT projects.

Eurojust participated in the Serious and Organised Crime Threat Assessment (SOCTA) Advisory Group meetings organised by Europol which were of particular importance prior to the drafting of the 2017 SOCTA report. Eurojust contributed, as an operational partner of Europol, to this document which was instrumental in shaping the EU Policy Cycle 2018-2021.

It is also important to mention that during 2016, following the Panama Papers leak, Europol and Eurojust contacted all EU MS offering coordination and support to any on-going criminal investigations. One coordination meeting was organised by Eurojust and Europol attended to provide complementary assistance. The International Consortium of Investigative Journalists database was crosschecked with Europol databases. Country packages were prepared by Europol and sent to the relevant EU MS. As a result Europol and Eurojust are currently supporting some on-going criminal investigations.

2. Combatting cybercrime

Eurojust has continued its active participation in the European Cybercrime Centre (EC3) located at Europol through operational work and participation in the different key structures and meetings such as the Programme Board of the Centre, the Heads of Member States' cybercrime divisions (EUCTF) and the Cybercrime Training & Education Group (ECTEG) meetings.

The Eurojust Seconded National Expert specialised in cybercrime ("Eurojust SNE") has been instrumental in strengthening operational cooperation between Europol/EC3 and Eurojust. His presence in Europol's premises has set a good practice between both organisations in an area in which early involvement of judicial authorities in operational cases is key.

The following case, designated Avalanche was jointly presented by Europol and Eurojust in different international and EU fora, is a perfect example of the practical and strategic involvement of Eurojust and Europol in tackling cybercrime.

Operation Avalanche

On 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Lüneburg Police (Germany), in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Eurojust, Europol and global partners, dismantled an international criminal infrastructure platform known as 'Avalanche'.

The Avalanche network was used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns. It has caused an estimated EUR 6 million in damages in concentrated cyberattacks on online banking systems in Germany alone. In addition, the monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide, although exact calculations are difficult due to the large number of malware families managed through the platform.

The global effort to take down this network involved the crucial support of prosecutors and investigators from 30 countries. As a result, five individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware infections were identified in over 180 countries. In addition, 221 servers were put offline through abuse notifications sent to the hosting providers. The operation marks the largest-ever use of sinkholing[1] to combat botnet[2] infrastructures and is unprecedented in its scale, with over 800 000 domains seized, sinkholed or blocked.

On the action day, Europol hosted a command post at its headquarters in The Hague. From there, representatives of the involved countries worked together with Europol's European Cybercrime Centre (EC3) and Eurojust officials to ensure the success of such a large-scale operation.

---

1 Sinkholing is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses. When employed at a 100% scale, infected computers can no longer reach the criminal command and control computer systems and so criminals can no longer control the infected computers. The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and Network Owners.

2 Botnets are networks of computers infected with malware, which are under the control of a cybercriminal. Botnets allow criminals to harvest sensitive information from infected computers, such as online banking credentials and credit card information. A criminal can also use a botnet to perform cyberattacks on other computer systems, such as denial-of-service attacks.

In addition, Europol supported the German authorities throughout the entire investigation by assisting with the identification of the suspects and the exchange of information with other law enforcement authorities. Europol's cybercrime experts produced and delivered analytical products.

Eurojust's Seconded National Expert for Cybercrime assisted by clarifying difficult legal issues that arose during the course of the investigation. Several operational and coordination meetings were also held at both Europol and Eurojust.

Within the Joint Cybercrime Action Taskforce (J-CAT), launched in 2014 within EC3, a number of cases have been identified as investigations where Eurojust's judicial advice and expertise is sought. Therefore, the Eurojust SNE participates in the weekly J-CAT operational coordination meetings and EC3 provides him with a weekly operational highlights report for them (include weekly updates, next steps and way forward, technical information, etc.).

Eurojust is, in addition, a supporting partner in NoMoreRansom project which was launched in July 2016 by the Dutch National Police, Europol, Intel Security and Kaspersky Lab. More than 30 new partners from both the public and private sectors have joined forces to fight ransomware and make decryption tools available, offering new possibilities to victims of ransomware to decrypt their blocked devices for free and learn more about how to protect themselves.

Finally, EC3 and Eurojust published a joint challenges to cybercrime investigations paper in January 2016. Additionally, Eurojust joined as observer the EC3-ENISA joint Working Group on Safety and Security Online and contributed to the development of the Training Governance Model.

3. Countering terrorism

The involvement of Eurojust in supporting national authorities in the investigation and prosecution of terrorist activities is growing, following a similar path to the increased operational support Europol is delivering to MS investigations since the launch of ECTC in January 2016.

In 2016 Eurojust became associated with the counter-terrorism Focal Point Hydra, adding to its recent association with FP Traveller. This constitutes a significant development in joint cooperation in this crime area. Eurojust's potential association to the counter-terrorism Focal Points Dolphin and Check the web is still pending awaiting Member States' approval.

Similarly to previous years, Eurojust contributed statistics and details on terrorist arrests, sentences and prosecutions in support of Europol's annual Terrorism Situation and Trend Report (TE-SAT) and is a member to the TE-SAT Advisory Board.

The case described below demonstrates the added value of the organisations in supporting the national authorities in the counter terrorism case.

Europol and Eurojust had a very close cooperation in the case opened by the French investigative judges after the terrorist attacks committed in Paris and Saint-Denis on 13 November 2015. While Europol has created the Taskforce "Fraternité" in order to process large amounts of information transmitted by all concerned Member States, including the French and Belgian investigation services (more than 18 Terabytes of data received) and to provide them with new investigation leads, the French Desk of Eurojust has opened a case in order to facilitate mutual legal assistance with 13 Member States and the USA. The two agencies have signed the French-Belgian joint investigation team agreement one month later with the aim to facilitate the exchange of all information relevant to the investigation. Since the opening of the case, Eurojust has organized 6 coordination meetings with the judicial authorities and the police services of the Member States concerned as well as representatives of Europol's counter-terrorism centre (ECTC). Europol organised or took part in 14 operational meetings with the investigators; the comprehensive operational analysis conducted by Europol/ECTC enabled the identification of new investigation leads.

4. Organisational perspectives

A number of joint activities have been carried over from previous years, and some have been started in 2016:

- The Steering Committee met twice. It discussed a number of operational and strategic topics, including Eurojust's support to Europol Focal Points, cooperation on strategic projects such as non-conviction based forfeiture and data retention, and the joint organisation of a meeting between the two organisations' management boards. These two meetings where complemented by number of smaller meetings of steering committee members delegated to coordinate the joint management board meeting.

- Three visits of the Eurojust-Europol Exchange Programme took place in 2016, attended in total by more than thirty representatives from each organisation. Participants, in their evaluation forms, maintained and praised the usefulness of these visits.

- Eurojust and Europol have discussed the possibilities of increasing synergies and cooperation, in particular at procurement level as a result of the move of Eurojust to a location closer to Europol. Both organisations decided to communicate their 2017 tender and procurement planning in view of assessing the feasibility of carrying out joint tender procedures in 2017/2018 in particular in the areas of general services and facilities. A general discussion on the possibility of sharing some services in the future was also launched.

- In conjunction with the re-organisation of the Operations Department at Europol, which also had an impact on the clustering of the Focal Points Eurojust rationalised its Contact Points structure to the Focal Points not only to better align them to the new structures at Europol, but also to their own priorities, teams and administrative structure.

- Finally, for the first time in history of both organisations, following the initiative of the Europol Management Board Chairman, a Joint Management Board meeting was organised on 12 December 2016 between the College of Eurojust and the Management Board of Europol. The event aimed at promoting a closer understanding of the respective mandates of both organisations under current and future legal frameworks and discussing mutual operational cooperation through the joint presentations of operational cases. The aspiration was to ensure that the respective activities are complementary, appropriately designed to best serve the interest of national authorities. It also gave a unique opportunity for those members to establish contacts.

5. Conclusion

The establishment and maintenance of effective lines of communication at operational, strategic, and senior management levels has engendered an effective dialogue ensuring constant evaluation and improvement of cooperation, including the further development of coordination techniques.