Council of the European Union

Brussels, 5 November 2019
(OR. en)

13752/19

COPEN 422
CRIMORG 149
EUROJUST 179
ENFOPOL 479
EJN 89
GENVAL 26
ENFOCUSTOM 180

COVER NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	12133/18
Subject:	Conclusions of the 15th Annual Meeting of National Experts on Joint Investigation Teams (JITs)

Delegations will find in the Annex the conclusions from the 15th Annual meeting of the National Experts on Joint Investigation Teams (JITs), which was held on 5 and 6 June 2019 at the premises of Eurojust in The Hague.

Conclusions of the 15th Annual Meeting of National Experts on Joint Investigation Teams (JITs)

5 and 6 June 2019, Eurojust, The Hague

The 15th Annual Meeting of National Experts on Joint Investigation Teams (JITs) - organised by the JITs Network Secretariat in close cooperation with Eurojust and Europol - took place at Eurojust in The Hague on 5-6 June 2019. The two-day meeting brought together experts from Member States, newly appointed contact points from Observer States (Republic of North Macedonia and Switzerland), representatives of EU institutions and agencies, as well as other practitioners and stakeholders involved in this area. Moreover, the JIT National Experts were welcomed by their respective Heads of Liaison Bureaux at Europol.

The topic of this year's meeting was *JITs in cybercrime cases: challenges and opportunities*. Through plenary sessions and workshop discussions, JITs practitioners and experts exchanged views on some of the most common legal and practical difficulties encountered in the setting up and operation of JITs in cybercrime, which may still hinder their wider use. These plenary sessions and workshop discussions were complemented by information and discussion about Europol's support for investigations and JITs, including in cybercrime cases.

The meeting was opened by Mr Ladislav Hamran, President of Eurojust, and Ms Catherine De Bolle, Executive Director of Europol, both of whom highlighted the complementary role of Eurojust and Europol in providing support to JITs.

1. Eurojust, Europol, EJCN, COM and other EU partners' support to cybercrime cases

Cybercrime is a global issue that most often does not stay within the EU's borders. Cybercrime cases present very specific challenges regarding the collection of evidence and its admissibility, such as loss of location, differences in legal systems, risk of loss of data, jurisdiction issues and cooperation with third States.

Cybercrime is high on the EU agenda and requires an enhanced law enforcement and judicial response, as well as specific knowledge and tools.

Coordination is especially needed in this field, and therefore the involvement of **Eurojust** in cybercrime investigations having a cross-border nature from the very beginning prove to be essential. Eurojust also provides an opportunity to liaise with third States through its global network of 49 contact points, 11 cooperation agreements and 6 Liaison Prosecutors from third States posted at Eurojust.

In recent years, Eurojust has played an important role in supporting successful cybercrime investigations, including those in which joint investigation teams were set up (since 2010, Eurojust supported 12 new JITs in the cybercrime area). Eurojust works on a number of levels to counteract increasing cyber-criminality by providing legal, practical and operational support to practitioners.

Eurojust cooperates closely with its main stakeholders, particularly through the secondment of Eurojust's National Expert on Cybercrime to the European Cybercrime Centre (EC3), promoting the early involvement of judicial authorities and facilitating the exchange of information, as well as supporting the Joint Cybercrime Action Taskforce (J-CAT).

Eurojust also hosts and supports the **European Judicial Cybercrime Network (EJCN)**, a network of competent national authorities from across the European Union, which meets regularly to exchange expertise and best practice regarding the investigation and prosecution of cybercrime. The broad mandate of the EJCN – relating to cybercrime, cyber-enabled crime and investigations in cyberspace – is cross-cutting by nature and creates synergies with other networks, such as the JITs Network. The EJCN cooperates closely with multiple stakeholders (e.g. EU Commission, Eurojust, EC3, EJN, and Council of the EU) in developing a number of activities on encryption, data retention, Dark Web investigations, etc. Typical questions addressed by the EJCN include direct cross-border access to electronic evidence and cooperation with private actors holding electronic evidence or the seizing of virtual currency.

The EC3 was set up in 2013 at **Europol** to strengthen the law enforcement response to cybercrime. Since its establishment, EC3 has made a significant contribution to the fight against cybercrime: it has been involved in a number of high-profile operations, providing analytical, technical and on-the-spot operational-support.

A representative from the EC3 made a presentation on AP Cyborg for cyber-dependent crimes, which provides support to Member States in preventing and combating different forms of cyber-criminality affecting critical computer and network infrastructures in the European Union. Its particular focus is on cyber-dependent crimes, covering a broad range of high-tech crimes such as malware (code creation and distribution), hacking, phishing, intrusion, etc.

Europol can offer valuable support to cybercrime operations, such as:

- operational support, including analytical and technical support, such as decryption tools, and forensic support, malware analysis, cryptocurrency tracing, etc.;
- SIENA: secure communication and information exchange platform;
- expertise: specifically in the area of cybercrime;
- data transfer: cybercrime cases involve large volumes of data that need to be transferred between the parties involved (Large File Exchange (LFE)); and
- financial support.

The Europol Malware Analysis Solution (EMAS) was also introduced to participants as a tool to provide Member States with a law enforcement-dedicated, secure and automated, complex malware analysis solution that executes malware samples submitted via the Internet in a tightly controlled 'sandbox' environment.

Based upon the experience of EC3, the following challenges related to JITs were identified: definition of the scope of a JIT, handling of large-volume data files, and cooperation with the private sector. The need for judiciary involvement at an early stage was highlighted. Based on practical experience, Europol stressed the need for a JIT partner taking a coordinating role, particularly in relation to the list of agreed actions. A responsible person to be appointed during an operational and/or coordination meeting.

Europol provides support, including a recently launched Virtual Command Post (VCP) tool, which is currently provided for action days. Participants expressed interest in having an EU tool with these features for more extensive use.

The European Commission (DG Justice) presented the state of play of the discussions on two new proposals for EU legal instruments, introducing new rules to make obtaining electronic evidence easier and faster (Commission proposals for a *Regulation on European Production and Preservation Orders for electronic evidence in criminal matters* and a Directive *laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*).

The EJTN presented training opportunities in the cybercrime area, such as: EJTN cybercrime and e-evidence-related legal seminars, EJTN seminars on judicial cooperation in criminal matters, EJTN-CEPOL seminars on JITs, linguistic seminars on the vocabulary of cybercrime and national seminars opened to European audiences.

CEPOL recalled the broadening of its mandate in 2017, now including training for all law enforcement officers, and not limited to police officers. In the area of cybercrime, CEPOL recently established the Cybercrime Academy, offering its state-of-the-art hardware and software, fully configured to train up to 100 participants simultaneously.

The cyber-trainings organised by CEPOL focus on the three main areas of cybercrime: non-cash means of payment, cyberattacks and online child sexual exploitation. In 2019, 16 different courses in these areas were offered to practitioners.

2. Case presentations

The meeting provided a platform to share and discuss some recent operational successes in the cybercrime cases for which JITs were established.

A successful cybercrime investigation into parcel and payment fraud within the framework of a JIT was presented to the participants. Through the JIT, the structure of the criminal network was identified, which would not have been possible through other legal instruments, such as mutual legal assistance (MLA). The presenter underlined that without a JIT, such a complex investigation would not have been possible.

The added value of JITs in cybercrime cases was demonstrated in a case that involved fraudulent bank accounts and money laundering. Cybercrime is constantly developing, leading to difficulties in judicial cooperation. Traditional legal instruments, such as MLA and the European Investigation Order (EIO), offer a response that is much too slow, particularly in cybercrime cases, in which speed is essential. In this case, connecting the testimonies given in victims' hearings in various countries was necessary to arrest the suspected leader of the criminal network. The only effective solution was to establish a JIT. Several action days were coordinated throughout the duration of the JIT, with suspects arrested and laptops and credit cards seized. The main challenges observed were: getting other countries involved in the JIT and the exchange of large amounts of data. The main benefit highlighted was the trust established between the JIT members, which later led to the establishment of a second JIT. Both JITs benefited from the support of Eurojust and Europol.

Another presentation introduced a large-scale cyberattack case, in which attacks were carried out throughout Europe. A JIT was quickly formed among several Member States, and JIT participants decided that each Member State would tackle one of the many crime groups involved. The speaker highlighted the large amount of data that needed to be analysed, which was done with the help of Europol. Via cooperation within the JIT, this data could easily and quickly be shared with all the parties involved.

3. JITs in cybercrime cases: challenges and opportunities

Two workshops were held on this topic, while the third workshop provided an opportunity to discuss the general role of Europol's Analysis Projects in supporting JITs.

a. JITs in cybercrime cases: specific challenges and possible solutions

Discussion and conclusions:

Participants first established the scope of 'cybercrime cases' to include, for the purposes of the discussion, cyber-dependent and cyber-enabled crime. The challenges and experience encountered in such cases were discussed, including general challenges of particular relevance in cybercrime cases.

JITs are appreciated as an excellent cooperation tool. However, effective collection of information at the intelligence-gathering stage should be ensured. Therefore, a clear plan of proceedings is needed, including the list of countries that plan to join the JIT and a definition of its scope.

- *Added value of JITs in cybercrime cases*

The advantages of the use of JITs in cybercrime investigations were determined to be:

- Most importantly: the sharing of resources, including expertise, human resources and technical capabilities, e.g. to conduct investigative measures (such as telecommunication source interception or online searches) by one JIT party on the territory of another JIT party, if the latter does not have the technical means to conduct the measure by itself.

- Further advantages:
  - Expeditious cross-border preservation and sharing of electronic evidence between JIT parties;
  - Basis for the development of a joint strategy;
  - Cooperation with private actors/other countries also via other JIT partners; and
  - Capacity-building through mutual learning.

- *Some challenges and possible solutions*

- Defining the scope of the JIT:
  - Large number of countries involved
    - Proposed solution: to use additional cooperation structures, e.g. the Joint Cybercrime Action Taskforce (J-CAT) hosted by EC3.
  - Purpose of the JIT, especially when the development of national investigations cannot be anticipated with sufficient certainty (as occurs frequently in investigations of cyberattacks):
    - Proposed solution: to include 'subsequent proceedings', and/or to consider from the beginning setting up follow-up JITs (in the event the JIT purpose needs to be adjusted).

- Loss of flexibility in the handling of national investigations after having committed to enhanced cooperation within a JIT.

- Time pressure during set-up phase:
  - Proposed solution: to establish guidelines for cooperation in pre-JIT phase dealing with supplementary instruments, e.g. the spontaneous exchange of information according to Article 26 of the Convention on Cybercrime (the Budapest Convention).

b. JITs in cybercrime cases: how to trigger the establishment of JITs more proactively

Discussion and conclusions:

- *Timely setting up of a JIT in cybercrime cases*

Participants considered that a setting-up procedure is very similar regardless of crime type. Different requirements in national legislation can delay the setting up of a JIT (drafting of the agreement, signing process, language requirements).

This situation is particularly problematic in cybercrime cases in which the operational needs require JITs to be set up without delay. The JIT working document (template JIT agreement for cyber-attacks developed by Eurojust) might be useful to accelerate this process, as well as negotiating the JIT agreement in one common language. For urgent cases, the parties might consider agreeing to sign the first version of the JIT agreement in a common language (with translation to follow, if required). Practitioners also mentioned that features such as electronic signatures could – in the future - be highly beneficial in urgent cases.

- *Other challenges related to the setting up of JITs in cybercrime cases*

Participants discussed how the number of countries affected by cyber-criminality, different stages of criminal proceedings or the lack of investigation in a country targeted by a cyber-attack could pose a hardship and affect the setting up of a JIT in a cybercrime case.

While participants agreed that these challenges are not unique to cybercrime cases, participants encouraged Eurojust and Europol to further analyse these issues and assist with advising on best practice. The importance of early identification of cross-matches between overlapping investigations was also highlighted.

- *Raising awareness and spreading knowledge on JITs in cybercrime*

Practitioners with previous experience in cybercrime JITs should share their knowledge and experience to demonstrate that setting up a JIT can help make practitioners' lives easier. Therefore, successes should be showcased.

Participants acknowledged a general lack of knowledge among practitioners about cybercrime. A requirement for training/education programmes on different tools and methods when dealing with cybercrime was expressed, which could be achieved through an update of the CEPOL JIT Online Training Module, by including specific guidance on 'cyber JITs'. Generally, practitioners acknowledged a need for them to further promote this tool among themselves.

The existing tools for practitioners, such as the JITs Practical Guide, JIT Model Agreement and JITs Restricted Area, should also be further promoted. The JITs National Experts play an important role in raising awareness and promoting the establishment of JITs and the supporting tools in their countries.

- *Support by Eurojust, Europol and JITs Network Secretariat*

Participants underlined that best practices and methods must be observed and promoted. Development of a checklist for setting up a JIT in cybercrime cases was suggested.

Eurojust can help combine practical experience and legal expertise in this area. The JITs Network Secretariat can provide assistance in gathering best practice and providing practical support. Participants suggested that a manual on best practice in cybercrime cases could be very helpful.

The role of Europol in cybercrime JITs was considered of significance and the involvement of dedicated experts in each cybercrime JIT was encouraged. Europol's Platform for Experts (EPE) Space was promoted as a secure and collaborative web platform for law enforcement specialists in the cybercrime area.

c. Experience of Europol Analysis Projects in supporting JITs

Europol's added value in supporting a JIT is not only present at the preparatory stage; it is equally helpful throughout all phases of a JIT.

Discussion and conclusions:

- *Europol products and services (experience)*

The importance of Europol's involvement during the intelligence phase was highlighted, particularly to identify important targets and countries involved, and to collect sufficient information and made them available to the involved countries, potentially leading to the establishment of a JIT.

Participants were generally positive about support provided by Europol, despite some challenges encountered, such as miscommunication, lack of understanding of working methods in a JIT and insufficient information provided on how to best involve Europol.

High Value Targets/Operational Task Forces: a new prioritisation mechanism at Europol was discussed, with participants underlining that more information on this mechanism should be provided.

- *Direct and secure exchange of information*

To support the needs of JITs for the direct and secure exchange of information and evidence, the following possibilities were identified:

- SIENA; some national systems provide only for centralised use of the system, which is not an optimal option when cooperating in a JIT;

- Large File Exchange (LFE) system, which allows for secure transmission of large amounts of data;
- Virtual Command Post, a new tool available at Europol that allows for direct and secure communication and exchange of information during the action day; and
- Meetings of the JIT partners (Europol operational meetings, Eurojust coordination meetings).

The need for a permanent and real-time secure communication tool similar to the Virtual Command Post was highlighted, and participants suggested that Europol look into the development of such a tool for the benefit of all Member States.

As part of the JIT funding scheme, Eurojust offers the possibility to lend equipment, such as laptops and mobile telephones with accounts allowing for the secure exchange of information. As not all practitioners are aware of this possibility, awareness needs to be raised on national level.

- *Management of information flow among the JIT parties*

To allow for smooth and effective cooperation, discussion and agreement on the information flow prior to the setting up of a JIT is recommended, possibly by inclusion of a specific clause in the JIT agreement.

Participants confirmed that face-to-face communication in JITs is essential and effective; however, it is also costly and time-consuming. The better utilisation of secure videoconferencing systems should be further explored.

- *Effective communication and efficient allocation of resources*

Participants discussed how to ensure good communication leading to efficient allocation of resources (intensity of support depending on various stages of JIT, e.g. in preparation, operational phase, action day, follow-up phase).

Clear and effective communication at key moments on needs and expected support should allow for a transparent and informed decision-making process. Flexibility is also required.

The best practice identified during the discussion was ‘expectation management’: parties should be clear on the support needed from Eurojust and Europol, and should submit information via SIENA to Europol for analysis purposes.

The participants recommended upgrading the catalogue of services available at Eurojust and Europol to support JITs, including an explanation of the different priority levels, the criteria for each priority level and the respective level of service associated with each priority (e.g. the criteria that need to be fulfilled for a case to be prioritised at Europol, what is needed to identify a suspect as the High Value Target, etc.). Additionally, the organisation of awareness sessions for practitioners was recommended.

4. Visit to Liaison Bureaux at Europol

The JIT National Experts were invited to Europol to meet the respective Heads of the Liaison Bureaux. Their discussions were related to the role of Liaison Bureaux and national experts in JITs, taking into account the specific situation in each country. Establishing better links between the Liaison Bureaux and JIT national experts would contribute to identification of potential JITs, as recommended in the Conclusions from the14th Annual Meeting of National Experts on JITS.

5. Police Cooperation Convention for Southeast Europe Secretariat (PCC-SEE) – Presentation of JIT-related activities

The representative of the Secretariat of the Police Cooperation Convention for Southeast Europe (PCC-SEE) introduced their recent activities and explained the benefits of cooperating on JIT cases with non-EU States in the Western Balkan region. Although PCC-SEE constitutes more of a law enforcement and police cooperation mechanism rather than a judicial one, it also highlights the strong focus and benefits of JITs.

The EU Member States can approach Western Balkan countries through the PCC-SEE Secretariat, since it possesses the proper framework to facilitate cooperation with these third States.

Several JITs were already established between EU Member States and Western Balkan countries, including Serbia, Bosnia and Herzegovina, North Macedonia, and, recently, between Italy and Albania. A successful JIT established between Bosnia and Herzegovina and France was presented to the participants by the Bosnian prosecutor, who highlighted the benefits of this tool – previously unknown in Bosnia and Herzegovina – in a complex cross-border THB and money laundering case.

6. Latest developments in JITs Network projects

Following a question by a national expert, the UK National Member at Eurojust confirmed the UK position regarding JITs. All JITs involving the UK will be founded on a single legal basis, i.e. one that all members of the JIT are a party to. In preparation for the UK's exit from the European Union, all UK JITs are now founded on a non-EU legal basis.

The JITs Network Secretariat updated the participants on ongoing projects and activities.

a. Observers and associate partners to the JITs Network Secretariat

As a follow-up to the adoption of the JITs Network Guidelines during the14th Annual Meeting of National Experts on JITs (6-7 June 2018), the JITs Working Group that met on 20-21 March 2019 discussed the approach with regard to the granting of status of the observers and associate partners to the JIT Network.

The JITs Network agreed to offer observer status to all third States that have already posted Liaison Prosecutors at Eurojust: Norway, Switzerland, the USA, North Macedonia, Montenegro and Ukraine. The decision to grant them observer status was taken based on the interest displayed so far by these Liaison Prosecutors in the activities of the Network, and their efforts in promoting the use of JITs in their respective cases. By the date of the 15th Annual Meeting of National Experts on JITs, Switzerland, Norway, North Macedonia, Montenegro and Ukraine had already appointed their contact points, who will be included in the list of contacts points of the JITs Network.

Furthermore, the JITs Network agreed to grant associate status to the bodies already listed in paragraph 34 of the JITs Network Guidelines, based on previously established cooperation with the JITs Network. These are the bodies listed:

- The European Judicial Network (EJN);
- The European Union Agency for Law Enforcement Training (CEPOL);
- The European Judicial Training Network (EJTN);
- The Police Cooperation Convention for Southeast Europe Secretariat (PCC-SEE Secretariat); and
- The Council of Europe (CoE).

By the day of the 15th Annual Meeting of National Experts on JITs , CEPOL, EJTN and PCC-SEE appointed their contact points.

b. 'Fiches Espagnoles'

Since 2014, the JITs Network Secretariat has been developing summaries of national legislation on JITs (*Fiches Espagnoles)* to facilitate the setting up and functioning of JITs. During the 14th Annual Meeting of National Experts on JITs, the national experts acknowledged that legislation in some States may have changed and, as a result, some of the summaries would need to be updated.

For this reason, the JITs Network Secretariat asked national experts to review the already existing *Fiche* regarding their country and inform them whether any relevant change in their national legislation should be reflected.

The updates to several summaries were already provided and the updated *Fiches* will be published in the JITs Restricted Area.

c. JITs evaluation

At the end of this year, the Third JITs Evaluation Report is due. To meet this deadline, experts were invited to communicate possible new evaluations until 31 October 2019. As was the situation with the second edition, this project will be carried out in cooperation with Eurojust.

Considering the increase in the number of JITs with involvement of third States, Eurojust decided that its contribution to the third JITs Evaluation Report will specifically address Eurojust' s experience in JITs with third States from an operational perspective.

Additionally, the progress on a new JITs Evaluation Module, which is currently under development, was presented. A dedicated team is trying to determine the best solution for practitioners, including the availability of the evaluation directly after the end of a JIT and the use of the online form instead of the cumbersome procedure of exchanging PDF files via e-mail.

d. Guidelines on JITs involving third States

Participants were presented with the Guidelines on JITs involving third States, prepared by Eurojust and the JITs Network Secretariat, and finalised in December 2018. The objective of this document is to provide guidance to practitioners from the EU Member States when considering setting up a JIT with third States. The document was distributed to the National Desks at Eurojust and published on the JITs Restricted Area for the use of JIT practitioners.

e. JITs Funding

The JITs Network Secretariat presented recent trends and statistics regarding JIT funding. In 2018, a total of 239 applications were received (some of them relating to the same JIT, for operations spread over subsequent action periods); 121 JITs have received financial support, 69 of which applied for the first time.

Lastly, the changes introduced in 2019, including the revised evaluation criteria and extension of action period, were presented to the participants.

A JITs tutorial video on reimbursement will be made available to practitioners on the Eurojust website in the coming weeks.

Annex: Overview of conclusions

As a result of the discussions held within the framework of the 15th JITs Annual Meeting, and from a practitioners' perspective, participants in the meting made the following suggestions:

JITs in cybercrime cases: specific challenges and possible solutions	
Challenges	***Possible Solutions***
Defining the scope of the JIT	
Large number of countries involved	▪ To use additional cooperation structures, e.g. the Joint Cybercrime Action Taskforce (J-CAT) hosted by the European Cybercrime Centre (EC3) at Europol.
Purpose of the JIT	• To include 'subsequent proceedings', and/or to consider from the beginning setting up follow-up JITs.
Time pressure during set-up phase	▪ To establish guidelines for cooperation in pre-JIT phase dealing with supplementary instruments, e.g. the spontaneous exchange of information according to Article 26 of the Convention on Cybercrime (the Budapest Convention).
JITs in cybercrime cases: How to trigger the establishment of JITs more proactively	
Challenges	***Possible Solutions***
Timely setting up of a JIT in cybercrime cases	▪ Use of the JIT model agreement (template) for cybercrime attacks; ▪ Negotiating JIT agreement in one common language; ▪ Signature of a version in common language (with translations to follow, if required); and ▪ Introduction of electronic signature.
Other challenges (number of countries attacked by cyber-criminality, different stages of criminal proceedings or the lack of investigation in a country targeted by a cyber-attack)	▪ Eurojust and Europol to further analyse these issues and assist with advising on best practice. ▪ Early identification of cross-matches between overlapping investigations.

Raising awareness and spreading knowledge on JITs in cybercrime	▪ Sharing knowledge and experience between practitioners on successful cybercrime JITs; ▪ Training/education on tools and methods when dealing with cybercrime; ▪ Update of the CEPOL JIT Online Training Module by including specific guidance on 'cyber' JITs; ▪ Further promotion of JITs Practical Guide, JIT Model Agreement and JITs Restricted Area; and ▪ Role of the JIT National Experts in raising awareness and promoting JITs and supporting tools in their countries.
Support by Eurojust, Europol and JITs Network Secretariat	▪ Development of a checklist for setting up JITs in cybercrime cases; ▪ A manual on best practice in cybercrime cases could be very helpful; ▪ Including dedicated experts from Europol in each cybercrime JIT; and ▪ Promotion of Europol's Platform for Experts (EPE): a secure and collaborative web platform for law enforcement specialists in cybercrime area.
Experience of Europol Analysis Projects in supporting JITs	
Challenges	***Possible Solutions***
Direct and secure exchange of information	▪ Use of the Virtual Command Post to be extended throughout the lifetime of a JIT. ▪ Further promotion of JIT funding possibilities, including loan of Eurojust equipment, such as laptops, mobile telephones with accounts allowing for secure exchange of information.

Management of information flow among the JIT parties	▪ JIT partners to discus and agree on the information flow prior to the setting up of a JIT, possibly by inclusion of specific clause in the JIT agreement. ▪ To explore further how the use of secure videoconferencing systems could be better utilised.
Effective communication and efficient allocation of resources	▪ As best practice, 'expectation management' was identified: parties should be clear on the support needed from Eurojust and Europol; as well as submitting information via SIENA to Europol for analysis. ▪ Upgrading the catalogue of services available at Europol and Eurojust to support JITs (e.g. the criteria that need to be fulfilled for a case to be prioritised at Europol; what is needed to identify a suspect as a High Value Target, etc.). Additionally, the organisation of awareness sessions for practitioners was recommended.