Council of the
European Union

Brussels, 25 April 2017
(OR. en)

8482/17

CYBER 62
COPEN 116
EUROJUST 55
JAI 369
CATS 32
ENFOPOL 199
COSI 83

COVER NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	European Judicial Cybercrime Network Kick-off Meeting 24 November 2016 - Outcome Report

Delegations will find attached the Outcome Report of the kick-off meeting of the European Judicial Cybercrime Network of 24 November 2016, as approved in the following plenary meeting of 6-7 April 2017.

1. Introduction

On 24 November 2016, the first meeting of the European Judicial Cybercrime Network (EJCN or the Network), since its establishment by Council Conclusion of June 2016, took place at Eurojust. Appointed members of the Network and observers from Switzerland, Norway, EC3, the Council of the EU and the European Commission, as well as the Secretary of the European Judicial Network, attended the meeting.
The first part of the meeting dealt with technical and legal challenges in relation to encryption, and legal obstacles to online undercover investigations. During the second part of the meeting, Eurojust presented its activities in support of the Network, and a discussion took place among the Network's members on its functioning.

The meeting was opened by the President of Eurojust and by the National Member of Romania, as Chair of the Eurojust Task Force on Cybercrime.

2. Session I – Technical and Legal Challenges in Relation to Encryption

The first session was chaired by the Network member representing the current Presidency of the Council of the EU, Slovakia.

A representative from EC3 provided an overview of practical challenges encountered by law enforcement authorities in encryption and possible solutions thereto. Encryption is an essential part of cyber security, which is also crucial for business purposes, and its abuse by criminals should be the real target for law enforcement and judicial authorities. Proper solutions should be identified, without necessarily reverting to front/back door tools; a combination of classic investigative techniques and technical solutions should be pursued.

A brief overview was presented of the activities of the Slovak Presidency with regard to the issue of encryption and its impact on the effectiveness of criminal investigations and prosecutions in the Member States.

The main outcome of an encryption mapping exercise, built around replies from the Member States to a questionnaire launched by the Slovak Presidency, was then presented. Some respondents reported that encryption is almost always encountered by national authorities in the context of criminal investigations and prosecutions; many respondents also pointed to a general lack of sufficient technical capacity to deal with encryption at national level, in addition to a lack of human and financial resources. A strong need to identify practical solutions in this respect was highlighted. Some Member States foresee obligations on Internet Service Providers (ISPs) to provide some type of decryption tool (e.g. passwords, keys), while only a few provide in their legislation for obligations of the suspects or accused or third parties to do so. Even if such obligations exist, the effectiveness and enforceability of such obligations need to be verified. An analysis of the jurisprudence should be considered.

Furthermore, reference was made to the possibility to distinguish between online and offline encryption, and to challenges regarding the gathering of electronic evidence peculiar to the two different scenarios. Eurojust commented that, in this respect, such distinction may be useful in view of assessing the type of investigative measure that might be most effective to employ.

The Network members engaged in a discussion of challenges and possible solutions to overcome limitations posed by encryption.

The Slovak Presidency suggested that the Network could look into the possibility of collecting case law and national legislation on this subject. Moreover, questions were raised regarding the availability of minimum standards in all Member States, as well as whether procedural matters available in domestic cases could also be applied in international cooperation.

Network members agreed that distinguishing between online and offline encryption is useful. In addition, participants observed that:

- EC3 can assist practitioners in this field.
- Training possibilities should become available for all practitioners, so that all can become at least aware of the meaning of encryption and the possibilities to deal with it. ERA, CEPOL and the EJTN should be considered in this respect.
- Offline encryption was perceived as easier to deal with than online encryption.
- Practitioners should be aware that decrypted information might be needed as evidence in another jurisdiction. Admissibility of such information as evidence in another jurisdiction is a topic for further exploration.
- A need to balance the protection of citizens from crime and the right to avoid self-incrimination was expressed, also in connection with possibilities to use biometrics of suspects or accused persons; some case law on this topic is being developed in a number of Member States, and should be shared with the Network members. Discussion also took place regarding whether encryption can be considered an absolute right, so that law enforcement cannot perform investigations in a useful manner.
- The use of back doors and whether law enforcement authorities are obliged to disclose their use to suspects should be mapped out in the Member States. Legal possibilities to use certain technologies and measures for evidence-gathering purposes were also discussed.
- Cooperation with ISPs is crucial: some participants reported some reluctance of ISPs to cooperate with law enforcement. Reference to the Yahoo! case was made and new case law on this matter should be shared with the Network as soon as available. EU institutions were invited to take good note of the Yahoo! precedent. In this respect, reference was also made to the ongoing discussions in the Council of Europe on the Guidance regarding Article 18.1b of the Budapest Convention.
- Costs for encryption, including offline encryption, are extremely high, and solutions to pool efforts should be found quickly; in addition, technical capabilities of law enforcement are not as sophisticated as those of criminals.

The Network made the following conclusions:

- Practitioners should try, to the extent possible, to distinguish between online and offline encryption when devising their prosecutorial strategy. A distinction between technical and legal issues should also be made.

- Online decryption seems to pose more problems than offline decryption, one of the reasons being that it is more dependent on third parties' cooperation.

- When faced with offline encryption, practitioners should keep in mind that other means of evidence might assist in decrypting or gathering information, as well as in securing other types of evidence.

- Many measures are available for offline encryption, which as a best practice should be shared within the Network.

- The need for immediate measures in online encryption was highlighted, as well as the need to identify the most difficult issues in investigations and prosecutions.

- Regardless of the approach that is chosen, effective criminal investigations, protection of fundamental rights and cyber security should always be in balance.

- Expertise among judicial authorities, especially in connection with their function of safeguarding the rights of suspects or accused persons, is needed.

- Investigative measures need to be effective and timely on technical and investigative levels.

- Creative application of existing legislation is encouraged, including the use of more traditional investigative means that can support an effective investigation.

3. Session II – Legal Obstacles to Undercover Investigations Online

The second session was chaired by the Network representative from the Netherlands. Two Network members from the UK introduced the topic of covert online investigations, and also presented the practical challenges associated with it in the UK. Overall, while covert online investigations offer enormous opportunities for proactive investigations, they also pose a few challenges that are linked to the peculiarities of the online world (e.g. specific online-related language).

A common issue faced in many countries is that, at the moment, undercover officers are not experts in the online environment, and are often located in different departments (one dealing with online investigations; another with undercover operations).

Another issue is the thin line between online undercover operations and entrapment. Some participants pointed to the fact that undercover investigations can only be authorised within the territory of a given Member State, which requirement cannot be easily satisfied in the online environment. Participants also discussed the definition of 'undercover operations', which relates to different legal instruments, and is interpreted in different ways in the Member States.

The seizing of registration credentials was highlighted as a practical solution, as the credentials can be used by the online undercover agent in the investigation.

The Network made the following conclusions:

- In relation to the thin line between online undercover investigations and entrapment, one should keep always in mind the European Court of Human Rights *Teixeira de Castro v. Portugal* case.

- As the majority of Member States are not yet fully familiar with online undercover investigations, experience with practical, legal and ethical challenges brought by the UK members of the Network should be further shared with the Network. Particular reference is made to existing case law.

- Creating a log of registration details of apprehended suspects could be a best practice, although in many countries legislative constraints may prevent such a log. Best practice should be shared within the Network.

- The need for training in this field was emphasized.

- New legislation on this matter, like that in Belgium concerning 'infiltration light', the objective of which is to identify the individual concerned, should be shared with the Network.

- If, during the carrying out of an undercover online investigation, the location of the suspect becomes known and points to a different State, the competent authority of this State should be informed immediately.

- In relation to the previous point, any risk of interference with another undercover investigation should be avoided. A common procedure to determine the level of risk would be welcome.

4. Session III – Eurojust support to the EJCN

This session, chaired by Eurojust, provided a description of ongoing activities carried out by Eurojust in support of the Network. Since 2014, Eurojust has held two meetings per year on cybercrime.

In June 2016, Eurojust published the first issue of the *Cybercrime Judicial Monitor* (CJM).The second issue of the CJM, which is released once per year, was presented to the Network.

The restricted website of the Network has been set up. Latest developments on the usability and content of the website were presented. Documents on substantive and procedural law and other strategic documents, such as the CJM, country *fiches* and national guidelines relevant to cybercrime have been published on the website.

Eurojust has also participated in working level meetings with the European Commission, and relations between the Network and the European Judicial Network have been maintained.

The Slovak Presidency presented a proposal for an EJCN database with information on ISPs. In preparation for this presentation, the Presidency launched a survey to gather the Network members' opinions on the collection of certain information on ISPs.

During the meeting, the European Commission representative referred to the Council Conclusions of 9 June 2016 on improving criminal justice in cyberspace, where reference to this possibility is also made. Deliverables are expected to be produced in June 2017. The European Commission representative indicated that the Network will be a very useful group to test some ideas that should be of benefit to practitioners.

5. Session IV – The functioning of the Network

The final session, chaired by Eurojust, presented the Network functionalities and collected suggestions for the work programme for the first two years of activities of the Network. To foster discussion, a discussion paper had been disseminated in preparation for this session. The participants discussed possible differences between members and observers, the Network's representation, the chairing and running of the Network meetings and choice of topics for discussion, etc.

Many participants stressed the need to ensure that this Network will be for the benefit of (judicial) authorities in the Member States, be as autonomous as possible, and be supported by Eurojust.

Some participants expressed their feeling that creating a distinction between members and observers was artificial, as the objective of the Network is to share expertise and best practice cross-border, and, as such, its members should not be confined to the Member States. . However, the Network was set up by Council Conclusion, clearly specifying that representatives should be appointed by the Member States. A distinction between members and observers was also discussed in relation to different levels of access to the Network's website.

Suggestions on which groups should be given observer status included EU institutions, Norway and Switzerland (but all with full access to the website), and also private sector companies. For the latter, however, participants underlined that they should be invited to attend meetings on an *ad hoc* basis, i.e. only if relevant. The possibility to meet in closed sessions was also supported by a number of participants.

Many saw a role for the Presidency's representative in steering the Network's activities, and a more limited role for Eurojust, and others also did not exclude a role based on voluntary contributions by the Network's members. The possibility to establish an informal Board consisting of the trio Presidencies and one Eurojust representative was also discussed and was supported by many. The Board, however, should also be joined by members who could make a contribution based on expertise and availability. External representation should be decided first among the informal Board members, and consideration should also be given to members specialised in a certain field. Regarding the Network's activities, many suggested organising members and observers in working groups, depending on the topic.

Participants also stressed the need to keep close contact with the main actors involved in the fight against cybercrime, to share knowledge to the maximum extent and to avoid duplication of efforts. Reference was made *in primis* to Eurojust, particularly in consideration of its operational know-how and close links with EJN, EUIPO, etc. The Secretary of the EJN suggested that a practical way to create synergies between the Network and the EJN could be for the Network's members representing a particular Member State to be informed of the identities of the EJN Contact Points in that Member State so as to establish a connection and mutually exchange expertise in judicial cooperation in criminal matters and cybercrime.

The majority of participants indicated that members of the informal Board, particularly the representative of the current Presidency or Eurojust, could represent the Network at external meetings. Costs for such representation, however, should be borne by Eurojust. Flexibility is required by all to avoid burdening Eurojust with unnecessary costs, particularly because at the moment no extra funding has been allocated to Eurojust to support the Network.

Eurojust also indicated that currently at least one meeting per year could be funded, and that resources from its Administration will continuously be deployed to provide support to the Network (e.g. for the development of the website, the analysis of legislation and case law for the CJM, and the organisation of meetings). A suggestion was made to organise meetings lasting one and one-half days, starting after lunch on the first day and continuing until late afternoon on the following day.

Following discussion, the meeting participants concluded that the EJCN:

- is an autonomous network of the Member States;
- consists of full members representing the Member States, third State observers, and other observers (EU institutions and private entities); representatives from Switzerland and Norway will have unrestricted access to the EJCN website;
- will be steered by an informal Board, consisting of representatives of the Trio Presidencies of the Council of the EU, supported by one representative from Eurojust;
- could carry out certain activities by means of (virtual) working groups;
- will be represented externally by members of the informal Board (*in primis* the chair) and by other Network members, based on required expertise and availability;
- will meet twice per year at Eurojust; and
- should avail itself of the possibility to meet in closed sessions.

Possible activities to be carried out during the next two years were discussed. Reference was made to the website, which should be enhanced to include a forum for the direct exchange of expertise and ideas and quick access to relevant information. The website and the forum should be able to support the exchange of information in a secured manner. The website should also list all relevant training possibilities available, at a minimum within Europe. Reference was made to the Council Conclusions on improving criminal justice in cyberspace. The EJTN and the EJCN will also play a role..

The following suggestions were also made:

- establishing contacts with service providers, particularly regarding encryption;
- working further on the matter of encryption, continuing the discussion held in the morning session, in partnership with the European Commission;
- reflecting by the JHA Council in December on encryption and the potential contribution of the EJCN and Eurojust, to be followed up to identify the deliverables that could be foreseen in the next two years; and
- exploring the role of the European Investigation Order for the gathering and admissibility of e-evidence.

The informal Board should prepare a first draft of a work programme with the support of Eurojust, and the draft should then be circulated for consultation to the main stakeholders as identified in the Council Conclusions setting up the Network. The work programme should be finalised within the first quarter of 2017.

The website was suggested as a platform to share ideas on the content of the work programme, and for consultation purposes. For the first round, however, open consultation will be via e-mail.

_____