EUROPEAN JUDICIAL CYBERCRIME NETWORK
6TH PLENARY MEETING

EUROJUST, 4 – 5 APRIL 2019

OUTCOME REPORT

1. Introduction

The European Judicial Cybercrime Network (EJCN) held its 6th plenary meeting on 4/5 April 2019 at the premises of Eurojust in The Hague. The meeting was attended by members of the EJCN from 27 Member States, Representatives of Switzerland, Norway as Observer States as well as by Representatives from Serbia, Eurojust, Europol/EC3, the Presidency of the Council of the EU, the European Commission (DG Justice and DG Home), and the Secretariat of the European Judicial Network (EJN).

This report reflects

- the key outcome points of the three topical discussions (for the scope of each of the topical discussions see introductory papers) conducted during the meeting (below Nr. 2),
- ideas for activities to be conducted in the EJCN sub-groups on data retention, e-evidence, case-building, training and virtual currencies as discussed within separate subgroup meetings (below Nr. 3) and
- key administrative action points for the EJCN requiring follow up in the near future (below Nr. 4).

2. Topical Discussions

2.1. Direct transborder access to digital evidence (incl. cloud data)

- Investigative measures aiming at direct access to data stored outside of the territory of the investigating state are each day more relevant tools to gather electronic evidence. Other than the cross-border cooperation with service providers such measures generally allow to secure data immediately. Also the scope of (unencrypted) data, which can be secured via direct access measures is different from the one available via the

cooperation with service providers. On this the SIRIUS project has the potential to provide for more clarity.

- A significant number of Member States already have domestic legislation in place and/or jurisprudence, which allows for the immediate access to data stored outside the national territory. This also includes situations beyond those where Art 32 Budapest Convention applies and/or where the location of the data is not known. Member States´ domestic laws combine these powers with various safeguards (like the exigence of a judicial decision) and limitations (e.g. excluding the permission for alteration or deletion of data).

- Some Member States´ legislation does not provide any legal basis going beyond Art 32 Budapest Convention. Also in view of their different concepts for the admissibility of electronic evidence these Member States are more or less able to still make use of investigative measures aiming at direct cross-border access to data.

- Helpful arguments and concepts to make the best possible use of the investigative tools available can be found in national court decisions. The EJCN will ensure their further dissemination and also work on a more detailed analysis of the situation within its subgroup on e-evidence (see below Nr. 3.2.).

2.2. Takedown of domains used for criminal purposes

- Procedural measures which aim at the takedown of domains are of increasing importance for the efficient investigation and disruption of the processes which criminal activities in cyberspace are relying on. Whereas criminals can easily replace a server within their infrastructure the takedown of domains has a more sustainable impact and has proven to be a best practice in combating many forms of cybercrime and cyber-enabled crime.

- Not all Member States' criminal procedure law includes a legal basis, which can be used for the takedown of domains. In some Member States the rules for seizure of tangible objects are applied. Other Member States use the concept of a seizure of the legal position of a registrant in relation to a particular domain. The limits of national law have been especially apparent in relation to seizures of unborn domains which in the context of the Avalanche case (presented at previous EJCN plenary meetings) were essential to prevent the criminal infrastructure from shifting to constantly changing domains.

- This situation gives a crucial role to the voluntary cooperation of registrars and registries, especially when they are based in Third States with limited basis for formal cooperation between competent authorities.

- The experience presented by Registrar of Last Resort illustrated the potential and flexibility of this kind of cooperation, which can adjust to the specific needs of competent authorities but also has to take special care of the applicable data protection framework, ICANN rules and issues linked to confidentiality.

- Nevertheless further work needs to be done to streamline and simplify working procedures for domain-takedowns. The EJCN will continue to look for possibilities to do so.

2.3. Dark web investigations and virtual currencies

Dark web investigations

- Strategies to identify TOR exit nodes and servers hosting hidden services have various technical and legal limitations. A significant role is therefore played by undercover investigations.

- Important legal and practical tools in the context of undercover investigations include dedicated legal regimes enabling an easier deployment of undercover agents in an online context or databases of (hashed) identifiers used by undercover agents on the dark web.

- Especially from the perspective of Europol/EC3 a reoccurring phenomenon preventing the deployment of undercover agents are obstacles to the initiation of investigations by the competent authorities of Member States concerned by certain criminal activities on the dark web. These obstacles could be linked to jurisdictional questions, to other procedural limits in national law or simply to a lack of available resources.

- In this situation early cooperation is required to take into account all of these factors in order to identify which Member State is in the best position to lead on a certain investigation.

Handling of Crypto Currencies

- Competent authorities mostly apply general provisions of their criminal procedure codes to conduct seizures of crypto currencies. This can involve analogies to the seizure of tangible or intangible objects or of rights to certain property.

- Practical problems to be solved include the creation of the technical infrastructure incl. wallets administered by the competent authorities in charge of keeping seized crypto currencies or the need to expeditiously exchange seized crypto currencies into fiat money.

- Some services related to crypto currencies, such as mixing or tumbling services give rise to the question, of whether their activities constitute a money laundry offence. The question of criminal intent is of special relevance in this context. Lists of indicators for such intent can help handling this phenomenon.

- The EJCN will further collect and disseminate existing guidelines to the issues mentioned above in relation to the handling of crypto-currencies. In its subgroup on

virtual currencies the EJCN will work towards an overview with a focus on the legal approaches in the Member States (see below Nr. 3.5.).

3. Meetings of Subgroups

Meetings of the following sub-groups took place as detailed below. The other sub-groups remain active but did not meet on this occasion.

3.1. Subgroup on data retention

The concept behind the planned activity of the subgroup is to update national authorities concerning the legislative developments and new national case law evolved in the light of *Digital Rights Ireland (C-293/12)* and *TELE2 (C-203/15)* and *Watson (C-698/15)*. The latest report available is from 2017 and produced by Eurojust with support from the EJCN. The main objective of the exercise is to facilitate judicial cooperation between national authorities by clarifying differences and similarities in each other's law and jurisprudence in the field of data retention. The subgroup agreed to collect information via the EJCN members and by a questionnaire with specific attention to the following:

- legislative developments concerning judiciary and the intelligence services ;
- legislative developments from the aspects of retaining data and of accessing to data;
- legislative developments with the attention to retention period, types of data (if specified) and admissibility of evidence;
- national case law particularly when difficulties arose due to the judgements of the CJEU.

The subgroup aims to have both the legislative and the national case law update available for the next EJCN meeting in late 2019.

3.2. Subgroup on e-evidence

The focus of the subgroup activities will be twofold: on the one hand, the follow-up and involvement of the EJCN in the process related to the proposed legal instruments on e-evidence and on the other hand, in a broader sense, taking a closer look at the topic of cross-border access to e-evidence.

The subgroup agreed on the actions and work to be done as follows:

(1) **EJCN involvement in the process of the new legal instruments:**

- assistance/input with types of data to be included in EPOC(-PR)/orders; and
- gathering of obstacles/best practices detected in e-evidence collection.

The future role of the EJCN will be assessed along the way.

(2) **Direct transborder access to data**

- analyse the topic further on the basis of a short questionnaire, with the purpose of obtaining a more structured and clear information on the current situation of the

Member States regarding legal transborder access, as mentioned above in section 2.1., 2nd and 3rd points.

(3) **Initiate collection of judgments related to e-evidence gathering**

- overview of judgments to be compiled on the EJCN website.

3.3. Subgroup on case-building

The conceptual idea of the subgroup is to assist national authorities in developing cross-border investigations by making use of support from Eurojust and Europol/EC3, especially where the investigations are related to the mandate and the topical focus of the EJCN.

The subgroup intends to start its work with a first case as soon as possible. For this the following four steps are envisaged:

- EJCN members of MSs, which would possibly be involved in the concrete case discuss strategy for its development
- EJCN member of Lead-MS assists competent authorities in bringing case to Eurojust and in making use of support from Europol/EC3
- Eurojust coordinates (the initiation of investigations) between MSs involved (where possible with the assistance of the respective EJCN members)
- EJCN members extract lessons learned and report back to EJCN plenary

3.4. Subgroup on training

The subgroup intends to focus on the following items with the aim to take the indicated actions as soon as possible depending on the availability of the members of the subgroup and the support from the EJCN support team:

- Discussion of the Training Competency Framework on Cybercrime coordinated by CEPOL
  Action: Continue to follow up on the discussion and fully engage in the project
- Explore possibilities of training for the EJCN members with ERA-EJTN-CEPOL-COM
  Action: Subgroup will approach ERA-EJTN-CEPOL-COM on the current trainings
- Contribution to GLOBAL CYBERCRIME CERTIFICATION initiative
  Action: Subgroup will continue following up on this initiative
- Contact ECTEG to apply for a grant to organise training for the judiciary
  Action: approach ECTEG
- Formulate an EJCN training programme with one of the training partners 2019-2020

3.5. Subgroup on virtual currencies

The focus of the subgroup activities will be geared towards developing expertise and knowledge related to the topic of virtual currencies, with the aim of creating comprehensive guidelines for judicial authorities on the virtual currencies.

Following activities are envisaged for the creation of the knowledge product:

- Initiation of a mapping exercise with the aim of collecting relevant documents/manuals/guidelines related to the topic of virtual currencies

- Analysis of existing and collected data and development of a questionnaire with a list of questions/points of interest to be disseminated among the EJCN members

- On the basis of the data collected, development of guidelines on virtual currencies covering the definitions and legal concepts, legal standards for the investigation, seizure and asset recovery etc.

4. Administrative action points

- The EJCN support team will assist the topical subgroups of the EJCN to work on the projects mentioned above under Nr. 3

- The Board of the EJCN will further promote the role of the EJCN during the ongoing assessment of the EJCN by the Council. The goal of these efforts is the allocation of additional resources to Eurojust for its 2020 budget, which would allow Eurojust to set up a dedicated secretariat of the EJCN

- The members of the EJCN will continue to submit information on relevant national case law to the EJCN support team for dissemination among the network via the restricted website and as contribution to Eurojust projects (such as the Cyber Judicial Monitor or the Encryption Observatory)

- The EJCN support team will gather contributions from the members of the EJCN on concrete cases illustrating
    - characteristic obstacles encountered in the cooperation with US-based service providers. The input from the EJCN will be used during consultations with US-based service providers in the course of a study visit to the USA in the context of the SIRIUS project
    - consequences of the reduced access to ICANN WHOIS data. The input will be used involving Europol/EC3 to further promote the law enforcement perspective at ICANN policy discussions

- Based on the input received during the current plenary meeting the EJCN will until the next plenary meeting define a framework for its further cooperation with Serbia