EUROPEAN JUDICIAL CYBERCRIME NETWORK
INTERMEDIARY PLENARY MEETING

11 JUNE 2020

OUTCOME REPORT

1. Introduction

The European Judicial Cybercrime Network (EJCN) held an intermediary plenary meeting on 11 June 2020. Due to Covid-19 related restrictions on events and travelling the meeting was held via video conference and focussed solely on topical discussions. Subgroup workshops will be organised through separate virtual meetings and stakeholder updates will again be included in the next regular plenary meeting of the EJCN. The meeting was attended by members of the EJCN from 14 Member States, Representatives of Switzerland, Norway and Serbia as Observer States as well as by Representatives from Eurojust, Europol/EC3, the European Commission (DG Home and DG Justice), the General Secretariat of the Council of the EU 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 supporting documents distributed to the participants prior to the meeting) and is **intended for dissemination only to members of the EJCN and other participants of the intermediary plenary meeting.**

2. Topical discussions

2.1. Remote cross-border Victim Remediation

Based on the presentation of two investigations (Retadup and Bredolab botnets) different strategies of remote cross-border victim remediation were described. These included the authorisation by the investigating authority of direct remote cross-border access to victims' computers to either cause malware to self-destruct or to notify victims of the botnet take-down including instructions on how to clean their computers.

Among others the presentation and following discussion indicated that following:

- there currently is no national or international legal framework which would provide practitioners with guidance on the possibilities and limits for remote cross-border victim remediation,

- open questions which practitioners are confronted with include

    - the technical design of a particular remediation measure and the estimation of the risks connected to it,
    - the definition of the competent (judicial) authority to authorise a remote cross-border victim remediation measure,
    - the criteria used for deciding to approve or not to approve such a measure,
    - the technical and legal need to involve foreign authorities and/or private partners (incl. internet access providers) and
    - the legal and tactical aspects of a notification of the victims,

- the topic of remote cross-border victim remediation is linked to several priorities of the current EU strategy on victim rights.

The practical handling of the questions mentioned above could be facilitated through the creation of an EJCN case-repository reflecting the solutions which have so far been applied in practice. The two cases presented at the meeting could form the start of such a repository which could be enriched by further contributions from network members and/or partners.

2.2. Challenges for lawful interception related to the introduction of 5G technology

The presentations introducing the topic to the network indicated

- the persisting potential of the ongoing technical developments and their international standardisation to create significant obstacles for the future use of investigative tools like e.g. lawful interception or IMSI catchers in the environment of 5G mobile networks,

- that this potential can be addressed through national legislation providing for "front doors", as transparent requirements for service providers to cooperate with law enforcement/judicial authorities e.g. by ensuring the availability of complete unencrypted surveillance copies and

- that within the EU the efforts of promoting the perspective of law enforcement of these developments have so far not been without success and will continue including within the framework of a law enforcement working group coordinated by Europol/EC3.

Aspects which could be addressed from the point of view of judicial authorities include

- The risk of impunity but also of an increase in the application of more intrusive investigative measures (e,g. the deployment of undercover agents or covert surveillance

measures incl. covert application of software on target devices) where investigations can no longer rely on lawful interception,

- A need for training in understanding and interpreting electronic evidence generated in the new 5G environment.

The board of the EJCN is going to present to the network a proposal on how the EJCN could contribute to raising awareness of the perspective of law enforcement and judicial authorities.

2.3. Operation Cepheus – cross-border application of new Australian legislation on covert investigative measures to access e-evidence

In their presentation of operation Cepheus the Australian Federal Police (AFP) and several prosecutors involved in the operation on the European side gave an overview of the issues which had to be solved, when a tailor-made software (the "technical resolution") had been applied across borders in a covert operation to retrieve specific data from suspects' computers in various European countries (the "target countries").

These issues and their possible solution vary greatly depending on the national law of the target country. Examples mentioned include the following:

- Norway: national law does only allow for covertly taking a single image of data held on a suspect's computer. In contrast the technical resolution included a repeated imaging of data over a specific period of time. As a result there was no way to authorise the application of the technical resolution to suspects in Norway.

- Belgium: the technical resolution was authorised by a Belgian investigative judge under Belgian law in the framework of an own investigation against suspects on Belgian territory. The Belgian interpretation was, that in conducting the technical resolution on computers of suspects on Belgian territory the AFP was providing technical assistance to this Belgian investigation.

- Netherlands: Similar to the Belgian solution the technical resolution was authorised on the basis of an own Dutch investigation. Subsequently the Dutch authorities asked the AFP through an MLA request to support this investigation by applying the technical resolution to computers of suspects on Dutch territory.

- Both the Belgian and Dutch solutions had to solve an additional problem resulting from the fact that the technical resolution directly provided data retrieved from suspects' computers to the AFP. Based on a requirement of Australian law the data could be provided to Belgium and Netherlands only on the basis of another MLA request.

The EJCN could compile an overview of the perspectives of all target countries on the main legal issues raised during operation Cepheus. Apart from the possibilty of authorising the technical resolution and its direct cross-border application by the AFP this compilation could also include additional aspects like the level of proof of the criminal character of the use of the remote access tool (RAT), which is required to initiate an investigation against its users.