EUROPEAN JUDICIAL CYBERCRIME NETWORK

10TH PLENARY MEETING

VIRTUAL MEETING, 17 - 18 JUNE 2021

OUTCOME REPORT SUMMARY

On the 17th of June, the President of Eurojust Mr. Ladislav Hamran, welcomed the participants to the 10th Plenary Meeting of the EJCN, held virtually due to the restrictions of the COVID-19 pandemic.

With the implementation of safety measures, namely COVID-19 Rapid Tests, it was possible to have in the Plenary the physical presence of the President of Eurojust, the EJCN Support Team Members and two Dutch Prosecutors (current and former EJCN Contact Points for The Netherlands).

The meeting of the **EJCN Contact Points from the European Member States, Norway, Serbia and Switzerland**, counted with the participation of representatives **from Eurojust, European Judicial Network (EJN), Europol-EC3, the Council of the European Union, the European Commission, CEPOL, European Institute for Gender Equality (EIGE) and European Cybercrime Training and Education Group (ECTE)**.

At the Plenary Opening, the President of Eurojust, Mr. Ladislav Hamran, praised the support of the EJCN to Eurojust, highlighting the fact that being cybercrime the fastest growing type of crime, **EJCN should benefit from an equal status to the other Networks at Eurojust becoming a Secretariat,** as it deserves to carry on and improve its very relevant work.

The Plenary of the EJCN started with the discussion on "**New Trends on Cybercrime and Cybercrime Investigations**", in which the Dutch and German EJCN Contact Points proposed a new strategic and a multidisciplinary approach to the present challenges in the criminal justice response to cybercrime. This new strategy should allow for a better distribution of resources, with an evidence-based approach to cybercrime: adaptable, robust, future-proof and done in cooperation with the private sector.

A relevant part of this strategy is the idea of a "**Book of Cybercrime**".

The **"Book of Cybercrime"** should be a living document, containing insight into the unique chain of actors and facilitators that add value to that particular crime script, such as ransomware. It should also contain an overview of interventions, which cause the greatest disruption of the criminal business model, as well as an overview of committed public and private stakeholders.

The Network proceeded with the discussion of "**Cybercrime as a Service – EMOTET and Victim Remediation**". Speakers from countries involved in the EMOTET investigation (DE, NL, USA) shared their perspectives on international cooperation and victim remediation from their side of the investigation.

From the speaker's interventions and input from the EJCN Plenary, it was concluded that:

- international judicial cooperation is paramount to successfully disable a global type of malware offered by an organized criminal group;
- early stage careful consideration of the legal instruments to be used as tools of international cooperation in lawful access is necessary;
- options for victim remediation may vary among the partners of international cooperation and should consider the points of: credibility of messages directed to victims, possible cooperation with the private sector, proportionality of the intervention necessary to remove the infection versus privacy and property of the victim.

The presentation to the Network of the **EU CyberNet Project** finalized the first day of discussions. The EU CyberNet Project focuses on the support to cyber capacity building activities in the EU and with 3rd countries. This presentation gave the opportunity to build a working relation between CyberNet and the EJCN and allow national Contact Points to join the project as Experts. The participation of EJCN in the CyberNet Project as a Stakeholder was well received by the Plenary.

On the second day of the Plenary, discussions followed on the topic of "**Social Engineering and Online Fraud**". Former EJCN Contact Point for the Netherlands and EJCN Contact Point for Slovakia, described the phenomenon of the IT Support Fraud, how it was addressed by authorities in their respective countries and shared possibilities on how to tackle the phenomenon.

It was concluded that:

- the phenomenon is very much underreported to authorities;
- cooperation with the private sector, software companies, banks and Fintechs, is essential to prevent and investigate the phenomenon;

- it is necessary to addressed this issue from the prevention side with awareness campaigns and from the financial side, avoiding that perpetrators are able to collect the profits they obtained from victims;

Also on the second day of the Plenary, the Subgroups of the EJCN presented their activities and plans.

The Subgroup Chairs presented to the Plenary their current and future deliverables to be made available in the EJCN Restricted Area: **Virtual Currency Guide** for Judicial Authorities, **WHOIS** Access Chart, **Direct Cross Border Access** to Digital Evidence Study, **Training Needs** Survey and refocus of the Case Building Subgroup on the topic of **Ransomware**.

Input from Stakeholders, Eurojust, Europol, EJN, the European Commission and the Council of the European Union finalized the Plenary. The Chair of the Cybercrime Team at Eurojust, greeted the Network for its relevant contributions and seconded the opening the words of the President, **concluding it is time to give to the Network necessary support to develop its potential with the creation of a Secretariat**.

The Plenary of the EJCN strongly welcomed the idea for a creation of a Secretariat, as it would allow EJCN to achieve its full potential as a relevant actor in the strategic support to practitioners, in the field of cybercrime and cyber enabled crime.