EUROPEAN JUDICIAL CYBERCRIME NETWORK

11TH PLENARY MEETING

HYBRID MEETING, 2 – 3 DECEMBER 2021

OUTCOME REPORT SUMMARY

1. Introduction

On the 2th of December, the Head of Operations Department Mr. Vincent Jamin, on behalf of the President of Eurojust, welcomed the participants to the 11th Plenary Meeting of the EJCN, held in hybrid format 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 one room some EJCN Contact Points, the Chair of the Cybercrime Team and representatives from the Private Sector.

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, and European Cybercrime Training and Education Group (ECTEG) and EUROMED Project, 84 attendees in total.

During this Plenary meeting, participants were engaged in two workshops on the topic of Ransomware, both restricted to judicial and law enforcement authorities, as a more interactive way for participants to learn from each other's experiences and bring forward ideas that can benefit the judiciary of the countries that integrate the Network.

The first day of the Plenary was dedicated, during the morning, to the Workshops. The first one focused on Ransomware in the Health Care Industry and the second one focused on the results of the EJCN mapping of Ransomware in the EU, Norway and Switzerland.

During the afternoon of the 2nd December, the Network discussed its achievements in 2020/2021 and its plans for 2022.

On the 3rd of December, two topical discussions were held, one on the use of blockchain technology to ensure chain of custody in criminal cases, with LOCARD Project and another on cooperation with the private sector, with the presence of representatives from Microsoft and Kaspersky.

- **This report reflects** :

1. the description and key outcome points of the workshops;
2. Topical discussions conducted during the meeting and conclusions taken from them;
3. The achievements of the EJCN in 2020/2021 and its plans for 2022;

2. Workshop on Ransomware in the Health Care Industry

In the first workshop, three presentations were given related to Ransomware attacks in Ireland, Czech Republic and Germany. The cases are as follows:

In March 2020, as the COVID-19 Pandemic hit Europe for the first time, Brno hospital was hit by a ransomware attack. The hospital was forced to shut down its entire IT network, doctors were unable to access patients' data and had to write and transfer their notes manually. Some data was irreversibly lost. The hospital had to postpone urgent surgical interventions and reroute patients to other nearby facilities.

In September 2020, a ransomware attack affected a Düsseldorf hospital, encrypting about 30 of the hospital's servers. Due to this attack, the hospital was unable to receive a 78-year-old patient, who had to be redirected to another hospital. This patient subsequently died.

In May 2021 an unprecedented ransomware attack occurred, affecting almost every part of the Irish healthcare system, already worn down by the Pandemic. This attack had an impact on the treatment of serious health conditions, as health care workers had to revert to a paper system and the number of appointments in some areas dropped severally, in the days following the attack.

In these cases, no ransom was paid and decryption keys were offered by the attackers. However, the damages were severe and patients suffered an impact on available resources.

All three attacks had a huge impact on the functioning of the affected health care facilities. As an example, in one hospital, the information system was shut down, the E-archive, which is the electronic patient record, was no longer accessible and only 5 out of the 30 surgery rooms were still working.

The specificity of this type of Ransomware attacks on the healthcare sector has a double focus that public authorities need to pursue. On one hand, all necessary measures need to be taken to safeguard the core business of a health care facility and on the other hand, the investigation needs to be started as soon as possible.

Both go hand in hand and therefore it is of utmost important that all "actors" are involved from an early stage and working together in one "task force". The possible actors involved could be: the hospital Crisis Management Board, the internal IT department, the police and the police specialized cybercrime investigators (local and national), the prosecution office, the national security center and the private companies involved in mitigating the cybersecurity aspects of the attack.

Each one of these actors has its own interests and their priorities differ. However, from the perspective of criminal investigation and prosecution, cooperation and coordination among all of them is crucial from an early stage to secure evidence and avoid that it may be destroyed due to an action of one of the actors.

2.1 Conclusions

a) Communication between Stakeholders – including the private sector, from an early stage is crucial when facing an attack;

b) Information sharing needs to be improved, a possible solution would be the creation of a permanent point of contact among Stakeholders, with regular meetings among them to discuss relevant issues;

c) Common trainings among Stakeholders can be a good way to create professional connections and find a common working language, we need to forget the idea of who is best or does best, abilities need to be integrated;

d) In the investigation of an attack, it can be relevant to identify the "Ransomware Family" to pinpoint the Organized Criminal Group behind the attack and its usual *modus operandi*, not only to gather evidence for a possible conviction or asset recovery but also to support victim remediation, ex : "Is this a group that usually attacks health care? Or does it usually focus on other type of targets?";

e) Dark Web and TOR tracing is possible but it should be very fast using proper expertise, in this environment everything changes and disappears in an instant;

f) Crypto tracing is essential, not just of the concrete attack but also of the group and its previous known attacks, we may not be able to arrest the perpetrators but we can go after their cryptocurrencies;

g) Criminals are operating worldwide and have the possibility to set up their IT infrastructure all over the globe while the judicial system is limited to national legislation; MLA procedures are slow or ineffective even when executed. Due to the data retentions limits the data often is not available at the time of a request;

h) Good cooperation with the victim is crucial. Build trust, the victim can be afraid to be exposed and remain uncooperative, the victim needs to understand the value of the presence of judicial authorities to prevent future attacks (not to save them or solve the current problem);

i) Critical infrastructure facilities should be asked at the national level to regularly check and control their internal IT infrastructure for security breaches;

j) Most health facilities are not prepared for the event of a Ransomware attack, the creation of a checklist at the national level to be followed when such an attack occurs would be a useful tool;

k) This type of check list can be useful for all critical infrastructure to improve resilience to a cyber-attack;

3. Workshop on EJCN Map of Ransomware

During the 10th Plenary Meeting of the EJCN, the Case Building Subgroup decided to change the approach to its purpose, in order provide the EJCN, in the benefit of the judiciary in the Member States and at Eurojust, a structured, step-by-set tool to tackle the persistent growth of the Ransomware attacks affecting several jurisdictions. In order to follow this approach, a questionnaire was sent to the Members of the EJCN on the topic of Ransomware from a judicial perspective.

Ransomware groups are increasingly more sophisticated, act strategically to maximize profits and reduce risks, are using multilayers of extortion methods to pressure victims and cooperate with other malware criminal groups in a “cybercrime as a service approach”[1].

The global perspective from the Network, taken from the questionnaire, is that dark figures are very high, there is a consistent perception incidents are underreported. Some jurisdictions created online reporting platforms that can also serve statistical purposes (EE, FR), reporting

[1] For instance, Internet Organized Crime Threat Assessment IOCTA , p. 19-22.

obligations (CZ) , single points of contact (LU), reporting templates (BE) and connections with the private sector (CZ, NL) to improve their perception of ransomware attacks and act swiftly.

These findings were discussed during the Plenary in an effort for Judicial Authorities to be ready for the next wave of Cyber Attacks in line with the EU Strategy to Strengthening the EU resilience to Cyber Attacks[2].

During the second workshop, the Network analysed the above mentioned current state of play on the topic of Ransomware in the EU, Switzerland and Norway, touching upon best practices on reporting of ransomware, communication with the victims and evidence gathering, as well as the most relevant challenges encountered by judicial authorities when investigating ransomware.

The Network discussed a working model, which can be used when futures attacks takes place. As mentioned in the first workshop, there are different interests by all the possible actors involved. A balance has to be found between "rescuing" the company from the attack that is taking place and the judicial investigation with the aim the safeguard the evidence.

Another point discussed, is the lack of reporting of Ransomware cases. There is a dark number and underreporting of the incidents, which cause the problem to be underestimated. In addition, when Ransomware is reported, the reporting made to authorities lacks a lot of relevant information. A possible solution to address this issue is to create a reporting template for Ransomware, as done by Belgian authorities.

It was highlighted that in some cases, the victims have no idea of what happened, how it happened and the extension of the damages. The attack can have a high financial impact, not only regarding the ransom to be paid but also due to the efforts needed to reconstruct the IT infrastructure, which are themselves time consuming and costly.

3.1 Conclusions

a) There is no single approach, formal/informal to tackle Ransomware;
b) A complete new minimum EU standard is needed to tackle and investigate Ransomware cases, a kind of blue print taking into account all possible factors, involving all actors in order to bring the criminal ransomware investigation to the right level and place;

[2] As mentioned in relation to the future Directive aimed at reducing the vulnerabilities and strengthen the resilience of critical entities.

c) The EJCN, in its Subgroup Structure, can develop this new model to share it with the Member and Observer States Judiciary;

d) Ransomware attacks to critical infrastructures, which have a huge impact on security, society and the economy require specific attention from public authorities;

e) Formal judicial cooperation is often ineffective to address cybercrime in general and Ransomware in particular, other possibilities need to be explored: police to police cooperation, use of 24/7 Network, Eurojust, Europol, existing Networks such as the EJCN, voluntary cooperation;

f) Cooperation at all levels is needed: at the level of prevention, investigation and prosecution (in particular to obtain e-evidence for Ransomware investigations). An European approach with the involvement of the private sector is a key point for success;

g) Better and easier reporting of Ransomware attacks by victims is needed to clearly map the phenomenon, its extension and support swifter criminal investigation. The use of an European template can be a useful tool to address this problem;

h) The EJCN can help establish a permanent judicial connection with the private sector, functioning as a judicial point of contact (SPOC[3]) with the Private Sector for cooperation in cybercrime;

i) The following steps could be integrated in mapping the different phases of a Ransomware attack for a more coordinated approach to Ransomware:

➢ **The Pre-phase**

- Private companies such as possible OSPs or and cybersecurity companies play an important role. They can detect the pre-indications such as high traffic and increase in creation of domain names;
- At LEA level, new attacks can be detected when monitoring Dark Web forums;

➢ **The Attack itself**

- It is important to understand the type of the attack in order to respond appropriately. It should be possible to list the possible indicators to assess the impact of the Ransomware;
- Based on the ransom asked, it could be possible to understand the weight of the attack. If no or very low ransom is asked or the communication channels with the

[3] Single Point of Contact at EU level, expanding but not replacing other possibilities of judicial authorities to connect with the private sector.

attackers are disabled, this could flag a State backed attack or an attack with political motivations;

- Another useful indicator is to identify as soon as possible the Ransomware "family". Some "families" are used by specific groups, others can be bought on certain forums. This could give an indication how the criminals have set up the attack[4].

➢ First steps to be taken during an attack

- It is crucial to understand the impact of the attack as soon as possible. Therefore, the reporting of a Ransomware attack should be done immediately after detection. On one hand, there is the company who wants to rescue its activities and on the other hand, there is the judicial investigation. Both need to understand each other and agree to cooperate;
- Creation of "Task Force", all actors involved need to cooperate and not only at National level. The involvement of the private companies in this "Task Force" is needed. The Task force could prioritise all actions to be taken into account in the interests of its members, such as the interest of the attacked company, the protection of direct and indirect victims, police and prosecution investigatory needs;
- The involvement of authorities (police/judicial) in the above mentioned points is based on their respective roles and powers, in accordance to their respective MS legal system.

j) In the preparation of a EU approach to Ransomware attacks, the following actions can be taken:

- Identify critical infrastructures susceptible to attacks;
- Prevention campaign targeted at critical infrastructure (IT systems);
- Creation of a stable connection to the Private Sector at the Judicial Level, in which the EJCN could act as SPOC;
- Creation of a common reporting template to appropriately map attacks.

[4] SOCTA 2021.

4. Achievements and Future of the EJCN

During the afternoon of the 2nd December the EJCN discussed its achievements during 2020/2021 and plans to develop its activities in 2022.

As a very important general achievement, the Network considers that it has managed to maintain its work during the difficult times of the Pandemic, in which personal contacts were very limited. The Subgroups maintained their work, twice per year Plenaries were held, input to Stakeholders was given and deliverables were produced.

The EJCN offered input to the Encryption Observatory Report, Digital Evidence Situation Report, Cybercrime Judicial Monitor and Working Groups of Eurojust's Cybercrime Team. New deliverables were produced such as : EJCN European Map of Ransomware, Declaration on the Digital Evidence Package, Mapping of EU+Observers in relation to direct digital access to digital evidence plus access to WHOIS data, Quarterly Newsletter and Virtual Currencies Guide for Judicial Authorities.

During the Pandemic, the synergies with EJN and Sirius Project were maintained and strengthened, with the participation in the Digital Evidence Workshop organized by the EJN and with the promotion of the SIRIUS Project. In order to support the later, an EJCN leaflet was created in EN, ES, FR, IT, PT, SK and disseminated by the Contact Points.

The EJCN participated in several Training Activities of its Stakeholders, such as ERA, EJTN, EU CyberNet and ECTEG, aimed at the EU Judiciary.

In general, the outreach of the EJCN was extended, in the online and offline environment, with a presence in several activities by the Contact Points or Support Team Members.

An outreach to the Private sector for strategic knowledge exchange was started during 2021 as another tool to gain efficiency in the fight against cybercrime.

The Network maintains as crucial the creation of a Secretariat to support its activities, in similarity to the other Networks supported by Eurojust. This would also give more relevance to Eurojust in the fight against cybercrime and would allow the EJCN to offer more to support the judiciary in the Member States during investigation and trial phases of cybercrime cases.

During the discussion about the future of the Network, it was highlighted the importance of the connection with the Private Sector, a point the Network considers it should be developed. This point was seen as crucial in the future fight against cybercrime and during 2022 the EJCN will discuss the appropriate framework to establish a stable connection with the Private Sector, in the benefit of the EU and Observer States Judiciary. In this regard, the EJCN can be an intermediary for dialogue and play a relevant role as a Point of Contact with the Private Sector.

The Network develops its work in the benefit of the European Judiciary and it aims to build its visibility with it to offer more support. In conclusion, the work of the EJCN should be made available to the Judiciary by developing synergies with other Networks and Projects, disseminate its deliverables in a public website and offer trainings to judicial authorities.

As a global conclusion, the Network considers its most relevant action for the Judiciary is to provide a forum for specialized judicial authorities to connect and contact each other informally to gain speed and efficiency in cybercrime investigations.

5. Topical Discussions

.1 New Trends in Cybercrime and Cybercrime Investigations: Digital Evidence and Blockchain Technology

The knowledge of Blockchain technology can be of relevance to the judicial community as it has several other uses with implications in judicial proceedings besides cryptocurrencies.

This idea was brought forward to the Network by a representative from LOCARD Project, which aims to automate the collection of digital evidence in any electronic format and medium. Its goal is to provide a comprehensive management approach to handle digital evidence to be presented in a court of law, alleviating many issues of current art and practice.

The Network was informed about the possible applications of blockchain technology in criminal justice, namely its ability to increase trust in the handling and processing of digital evidence and the management of chain of custody, in a transparent, immutable way, accessible to all participants in the proceedings (accordingly to respective credentials).

The practical use of the platform designed by LOCARD Project for law enforcement and judicial authorities was shared by the Hellenic Police.

5.2 Cybercrime and Cooperation with the Private Sector

During the 10th Plenary Meeting of the EJCN, the Case Building Subgroup decided to change the approach to its purpose in order provide the EJCN, in the benefit of the judiciary in the Member States and at Eurojust, a structured, step-by-set tool to tackle the persistent growth of the Ransomware attacks affecting several jurisdictions.

This outcome, as discussed during the 10th Plenary, also comprises the conclusion that it is impossible for judicial authorities, to investigate cyber incidents and support victims without connecting with the private sector. It might as well be impossible for private companies, to obtain certain elements or results in the benefit of their clients in relation to cybercrime, without the powers of public authorities.

As a result, combining the competences of the private and the public sector, in a way that allows for a more efficient investigative approach, could provide better outcomes in cybercrime investigations.

Nevertheless, for both sides addressing cybercriminal actions, this is still quite a new cooperation in uncharted territory. In relation to cybercrime, public authorities and the private sector share the goal of preventing attacks and ensure swift victim remediation. However, they have different business needs in relation to that goal, as well as different rules to follow.

For the first time, the EJCN has invited representatives from the private sector to its Plenary, to share experiences with the objective of improving the public/private dialogue to fight cybercrime.

This topical discussion was initiated by the EJCN French Contact Point, who shared the experience and developments in France on the topic, concluding that it is essential for the prevention and remediation of cybercrime threats, to establish a permanent platform of information sharing with the private sector and to formalize cooperation, as it is already being done in France.

From the French experience, the topic of blockchain and cryptocurrency tracing is of great relevance, not only in the criminal investigations themselves but also as a topic of knowledge for the judiciary, as knowing how to present a case and understand the evidence gathered on these topics is essential for a successful trial in cybercrime related cases. These topics are considered to be a point of relevant connection to the private sector.

Another point of successful connection with the private sector from taken the French experience was the fight against Stalkerware. A cooperation done with Kaspersky's TinyCheck Project to support victims of domestic violence/cyber violence is being implemented to test the use of a small, cheap device, able to diagnose a Stalkerware infection in a victim's device at the local police level.

The cooperation with the private sector, namely cybersecurity and insurance companies can be very valuable for the protection of critical infrastructure, such as hospitals. The creation of a crisis plan, nationwide or European wide for ransomware or other type of cyber-attacks can be an invaluable tool and needs input from the private sector.

In this presentation, the Network was informed that the most relevant, time-consuming barrier to an efficient public/private sector cooperation is language, related to the detailed description of what is requested, on one hand, and what private companies need to know, from a legal perspective to comply with requests, on the other.

Judicial authorities should be as specific as possible; the public/private sectors need to speak the same language and the EJCN/Eurojust can have a role in closing this language gap to enhance information sharing for the efficiency of cybercrime investigations.

The lack of a framework regulating the public/private cooperation in cybercrime should not be an obstacle to start and develop that type of cooperation, whenever the need arises and common interests align.

The correct reporting of incidents, namely with the use of a template, was mentioned as relevant and that the private sector should have proper feedback in relation to the actions it participates in. Cybersecurity companies can contribute with skills that are standard in their everyday work but not easily done by public authorities and public authorities can pursue developments in a way closed to private companies.

The presentations from the private sector were well received by the Network, which recognizes that it has the ability to help close the language gaps in the public/private sector dialogue. Most importantly, the Network considers it may have the ability to act as a Specialized Point of Contact in the public/private sector cooperation in cybercrime, a topic to be discussed and developed during its work in 2022.