EUROJUST

Overview Report

Challenges and best practices from Eurojust's casework in the area of cybercrime

November 2020

Criminal justice across borders

Contents

Executive summary

There are several factors that make tackling cybercrime unique and challenging. Cybercrime by its nature is borderless and swiftly evolving, sometimes faster than national authorities can react. Adding an additional layer of complexity is the horizontal nature of cybercrime: almost any type of crime can nowadays occur over the internet. Electronic evidence of such crimes may be difficult to collect, owing to the volatility of data, and may require specific expertise. Judicial cooperation is essential to ensure timely preservation of electronic evidence, which ensures its admissibility in judicial proceedings. International judicial cooperation may be hampered by significant differences in domestic legal frameworks (e.g. regarding criminalisation of conduct or data retention legislation) and conflicts of jurisdiction. The whole phenomenon of cybercriminality is reshaping the traditional legal concept of the territoriality principle as a result of the supranational nature of the evidence required to ensure the successful prosecution of cybercriminals.

Therefore, an effective national response to cybercrime often requires multilevel collaboration. Strengthened international cooperation is key, as cyberspace is international and cross-border in nature. 'Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace' focuses on creating a cyberspace that promotes access to the internet and ensures market growth, yet aims to achieve cyber-resilience and tackle cybercrime, striking the right balance between the fundamental rights of citizens and the rule of law ([1]). Furthermore, it promotes the use of international cooperation tools in the fight against cybercrime, as well as related police and judicial cooperation in third countries from which cybercriminal organisations operate ([2]).

The Council conclusions on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' ([3]) complement the EU cybersecurity strategy by emphasising the need to prevent, deter, detect and respond to malicious cyber-activities. They underline that public authorities need to be provided with the tools to detect, investigate and prosecute cybercrime.

Eurojust focuses on countering cybercrime with a view to strengthening judicial cooperation in this field, particularly by facilitating the swift handling of judicial requests – a crucial factor in addressing the issue of the volatility of data and filling gaps arising from the application of different domestic data retention rules – and the early involvement of the judiciary in cybercrime operations to ensure that data are collected in compliance with the applicable rules during the investigation phase and as a result may be tendered as admissible electronic evidence in subsequent judicial proceedings. In addition, Eurojust either produces or contributes significantly to the production of strategic products in the area of cybercrime, thus helping practitioners to further develop the necessary cyber-specific skills ([4]).

This report aims to give an overview of Eurojust's work in the area of cybercrime. The operational work performed by Eurojust offers an excellent insight into common challenges faced by practitioners, as well as best practices to overcome these challenges. Eurojust's casework is a useful source of information on specific obstacles in the context of judicial cooperation and how they can be overcome, feeding into the discussion on how best to address the phenomenon of cybercrime. Succeeding is a chapter giving case examples. Finally, Eurojust's corporate publications and projects of interest in the area of cybercrime are listed.

([1]) Council of the European Union, Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 22.7.2013 (12109/13)

([2]) Eurojust is committed to several capacity-building projects in the area of cybercrime, such as the Sirius project (http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx), the EuroMed Justice project (https://www.euromed-justice.eu/) and the GLACY+ project (https://www.coe.int/en/web/cybercrime/glacyplus).

([3]) Council of the European Union, Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 20.11.2017 (14435/17).

([4]) For more information, please refer to the section 'Eurojust's publications and projects in the area of cybercrime' in this document.

Eurojust's operational work in the area of cybercrime

Through Eurojust's casework in recent years, a number of challenges and best practices in investigations and prosecutions relating to cybercrime and cyber-enabled crime ([5]) have been identified. The majority of these challenges are of a general nature, relating either to national procedural and/or substantive legal requirements or matters of cross-border cooperation, or simply to difficulties in communication with foreign online service providers.

A minority of the challenges identified are essentially related to the horizontal nature of cybercriminality. Nevertheless, this does not mean that such cyber-specific challenges were not encountered at a greater scale at national level in these cases. It may be that Eurojust's assistance was not requested in that particular respect.

Furthermore, given that often the investigation of a crime precedes the involvement of the judiciary, and the fact that Eurojust is requested to support and facilitate cooperation between authorities in only a fraction of cybercrime cases, the account of challenges and best practices identified below is by no means exhaustive; however, it may serve as a good indicator of the problems faced by legal professionals working on cybercrime in their day-to-day activities.

Challenges

Prosecutors and investigative judges are confronted with certain challenges when handling cybercrime cases. Typically, these challenges are linked to the fact that cybercrime investigations tend to be dependent on electronic evidence, which can be freely moved across national borders and easily taken out of an investigator's reach by being deleted, transferred to a new jurisdiction or encrypted.

The majority of the challenges in cybercrime cases relate to the execution of mutual legal assistance (MLA) requests: slow execution of MLA requests due to a lack of coordination between jurisdictions affected by the criminality, or refusal of execution because of conflicting national interests and/or pending criminal proceedings at national level. The current MLA process is perceived as a slow and cumbersome method of gathering and sharing volatile electronic data, for example due to the reasons relating to lack of coordination between different jurisdictions affected by the criminality. Moreover, the issuance and execution of an MLA request can take longer than the legally established data retention period of the country requested.

The joint investigation team (JIT), as an alternative and complementary instrument of judicial cross-border cooperation, has brought its own specific challenges. Timing has been identified as one of the main challenges in setting up a JIT agreement in cybercrime cases, and it is not uncommon for delays to be caused by the need for information to enable a decision to be taken at national level on the initiation of joint investigations. It may be decided not to establish a JIT if the participants come to realise that they are at different investigative stages. If the parties are dissuaded from forming a JIT agreement because of the need for more time to build a case at national level, parallel national investigations may be required as a consequence.

Parallel investigations that lack the proper coordination at regional level hinder effective cooperation and increase the risks associated with conflicts of jurisdiction and/or occurrence of *ne bis in idem* situations, not to mention the waste of resources resulting from the duplication of work. Owing to the greater potential for problematic situations, a judicial response can be hindered and there may be difficulties in asserting criminal jurisdiction. Uncoordinated investigations may result in different law enforcement authorities investigating the same targets and one investigation may cause negative consequences for the other. International cooperation can solve these problems by de-conflicting the targets of the parallel investigations, with the result that the judiciary will be more inclined to pursue cooperation as well.

([5]) 'Cyber-enabled crime' refers to crime that does not fall into the traditional definition of 'cybercrime' but is committed online or with the use of computers, thus requiring very similar investigative actions to cybercrime (e.g. cyberbullying, online piracy, online stalking, organising a crime / communicating about a crime via social media).

Conflicts of jurisdiction are a greater risk in cybercrime cases because of the phenomena of loss of data and loss of location. Cloud computing, anonymisation tools and the dark web have led to loss of location issues, where authorities cannot reasonably establish the physical location of the perpetrator, the criminal infrastructure or the electronic evidence. In these situations, it is often unclear which country has jurisdiction and what legal framework regulates the collection of evidence or the use of special investigative powers. In relation to cloud computing, not even the industry knows where its data are stored at any given moment, as the jurisdiction in question can change instantly as a result of the automatic load balancing of internet-based services.

Another challenge stems from the fact that a growing number of electronic service providers implement default encryption of their services, and already the large majority of investigations involve the use of some form of encryption by the perpetrators. The gains in terms of privacy and confidentiality for citizens from encryption of services come at a price: traditional investigative techniques are becoming less efficient owing to the exploitation of modern technology by criminals.

Cryptocurrencies are an example of technology that anonymises financial transactions and the use of which is increasing. They entail increased use of 'tumbler'/'mixer' ([6])services, which effectively prevent law enforcement from 'following the money' and significantly complicate asset recovery and the prevention of fraudulent transactions.

Additional uncertainty about the availability of electronic evidence results from the absence of any streamlined legal framework for data retention (this issue is not exclusive to cybercrime investigations; the same problem can be detected in relation to phone communication data, as telecommunications service providers have no uniform legislation in place establishing minimum standards for data retention).

A rapid rise in low-threshold, high-impact cyberattacks, for example as part of an extortion scenario (e.g. using ransomware), brings completely new types of problems. Owing to the scale of such criminality – a massive number of victims located in several jurisdictions – it can be extremely difficult to identify and/or properly involve the victims in criminal proceedings, especially given that certain types of victims are not inclined to report these kind of attacks, as their reputation would suffer, with economic consequences (e.g. accounting companies and banks do not like to discuss the loss of partners' sensitive data).

The complexity of the organised criminal groups (OCGs) that are the subject of cybercrime investigations is a relatively common feature in Eurojust's casework. These groups – horizontal in nature, divided into specialised sub-cells and providing cybercrime as a service ([7]) – present new kinds of challenges, and national prosecuting authorities struggle, again, with conflicts of jurisdiction and/or *ne bis in idem* situations, as the same suspect(s)/victim(s) may be the subject of various proceedings in different jurisdictions.

The challenges mentioned above bring with them problems relating to prioritisation and resource management at national level, which have an impact on international cooperation. Resource constraints on national investigations and JITs are compounded by the excessive workloads of forensic experts.

Large datasets and the need to analyse vast amounts of files lengthen the overall duration of criminal proceedings and the intervals between investigative actions, which can result in the loss of data.

There may be insufficient expertise for a thorough examination and cross-examination of the intricacies of electronic evidence. Similarly, expertise is required within law enforcement authorities to capture and handle such evidence in a forensically sound fashion. Currently, however, there is no internationally agreed forensic standard for the collection of electronic evidence for the purpose of criminal investigations and prosecutions.

([6]) A 'tumbler' or 'mixer' is an online service that attempts to sever the links between the perpetrator's cryptocurrency wallet address and a new address by sending funds from the ??":
to other people and funds from them to the perpetrator. It also randomises transaction amounts and sometimes adds time delays to the transactions. The aim is to mix potentially 'tainted' cryptocurrency funds with others, so as to obscure the trail back to the funds' original source. Tumblers were developed to further anonymise cryptocurrency transactions.

([7]) This involves the provision of tools and services for criminal purposes with a financial incentive in mind. For examples, please refer to the section 'Case examples' in this document.

The new tools available to criminals also bring challenges that national criminal proceedings laws are not tackling, for example with regard to the seizure, confiscation and conversion to fiat currency of cryptocurrency. National criminal laws do not usually answer questions regarding the legal nature of cryptocurrencies (e.g. are they to be treated as 'normal' money or bonds?).

Best practices

First, the referral of cases to Eurojust for support and facilitation of cooperation and coordination of investigations and prosecutions is in itself a best practice.

Coordination meetings, coordination centres and JITs are the main judicial cooperation tools at Eurojust.

Eurojust is a key facilitator of early information exchange. It is instrumental in detecting links between national investigations, thus enabling the dismantlement of cross-border criminal infrastructures. It facilitates agreement on prosecutorial strategies, which contributes to unveiling previously undetected activities of the perpetrators and minimises the risk of conflict of jurisdiction.

At an operational level, the early involvement of judicial authorities in cybercrime cases is desirable, as it helps to safeguard the admissibility of evidence gathered at a later stage. Therefore, the early involvement of Eurojust in cybercrime cases is also beneficial, as it is in a unique position to facilitate multilateral judicial cooperation, coordination and exchange of information.

Eurojust served on a number of occasions as a forum for aligning prosecutorial strategies. Such agreements are based on a mutual understanding that one Member State may be in a better position to undertake an investigation or to prosecute specific acts than another. Eurojust is in the unique position of being able to issue non-binding joint recommendations to national prosecution services, thus reinforcing such agreements. To date, no joint recommendation has been challenged by the affected national authorities.

Eurojust also facilitates the execution of MLA requests by clarifying (legal) requirements for their execution, advising on content and ensuring the transmission of documents. In addition, it helps in exploring alternatives to MLA. For the purpose of collecting non-content data, the establishment of a public–private partnership through direct interaction with service providers can be such an alternative.

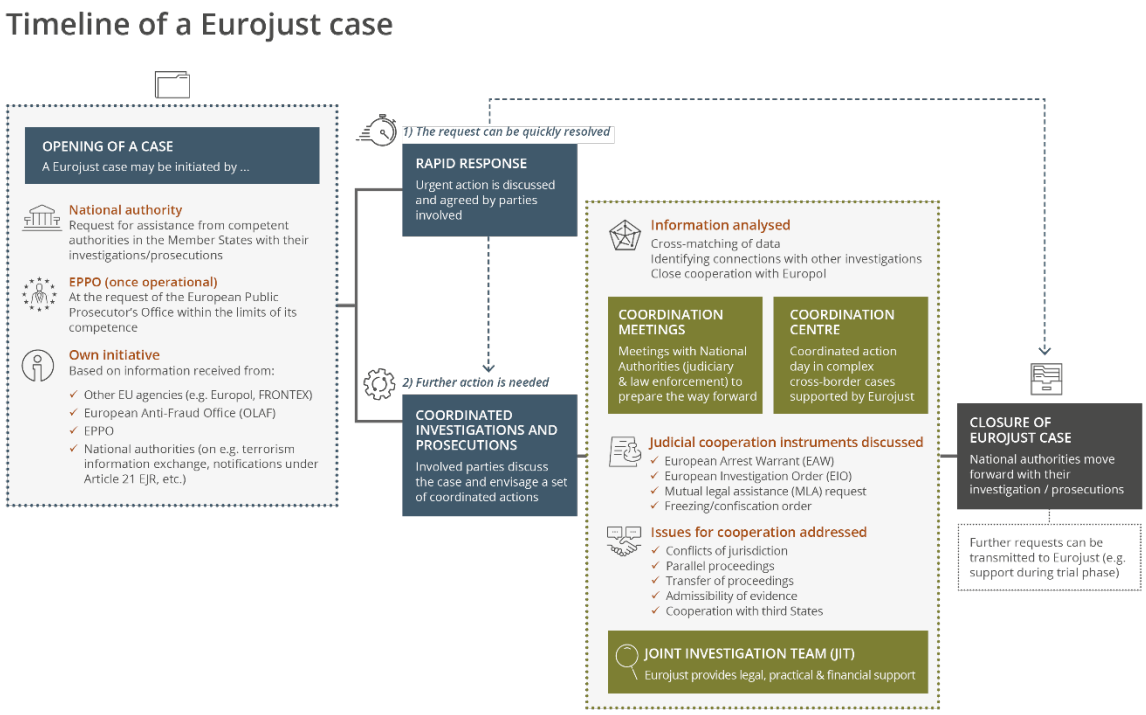
Close coordination between Eurojust and Europol facilitates the cross-checking of information and the verification of further connections between national investigations and prosecutions at an early stage of the investigation. Europol provides support through secure information exchange, participation in JITs, organising operational meetings and the de-confliction of targets, and deploying a mobile office on action days. Europol is also instrumental in performing real-time analysis and cross-checks against its databases, and it functions as a bridge between the public and private sectors.

Coordination meetings facilitate the exchange of information (with the convenience of simultaneous interpretation) among national competent authorities, support the expedited execution of legal assistance requests, coordinate ongoing investigations and prosecutions, and detect, prevent and overcome judicial cooperation obstacles, such as conflicts of jurisdiction.

Coordination centres provide a unique opportunity for real-time exchange of information and centralised coordination of the simultaneous execution of, inter alia, arrest warrants and searches and seizures in different states. Coordination centres expedite the timely transmission of the additional information that is urgently needed to execute such measures and newly issued MLA requests, and they provide a final overview of the results of the coordinated action, which is shared with all participants.

The casework highlights that the JIT is seen by practitioners as an important judicial tool for closer cooperation and more direct cross-border exchange of evidence, particularly since a specific cybercrime JIT template has been made available to make joint investigations as easy as possible. JITs facilitate accurate and speedy exchange of information in cases in which information is often scattered, and JITs can also apply for

funding to have the evidence gathered translated into the language of the investigating country. Signing a JIT agreement has a direct effect on the admissibility of evidence before a court of law. Evidence lawfully collected in one country that is party to the agreement has to be recognised by the judiciary of the other, so, in short, forming a JIT ensures the mutual admissibility of evidence. This makes it easier for countries with different legal systems to work together effectively.



In addition to coordinating the efforts of judicial authorities in the EU, Eurojust has established a network of more than 50 contact points all around the world. Enhanced operational cooperation is provided for through cooperation agreements with third countries. There are 12 such agreements in place; in 8 of them, specific arrangements are made for the secondment of liaison prosecutors to Eurojust. Through the provision of contacts in and immediate operational support in relation to third countries, Eurojust is able to expedite judicial cooperation outside the EU and address challenges characteristic of cybercrime, such as loss of data.


Liaison Prosecutors
stationed at Eurojust
Norway
Switzerland
Ukraine
USA
Montenegro
North Macedonia
Serbia
Georgia
Cooperation agreements
USA
Iceland
Liechtenstein
Norway
Switzerland
North Macedonia
Moldova
Montenegro
Albania
Ukraine
Georgia
Serbia
EUROJUST
Contact Points
More than 50 third countries comprise Eurojust's judicial Contact Point network

Case examples

In addition to the emblematic cases that have been analysed for this report and which are presented as case examples below, Eurojust has previously published independent casework analyses related to the investigation and prosecution of cybercrime.

Operation *Avalanche* – A closer look (April 2017)

Operation *BlackShades* – An evaluation (April 2015)

Operation Emma 95/Lemont

Case summary

This was a French and Dutch investigation into EncroChat, an encrypted communications service provider (developed in Spain with technical infrastructure located in France and Canada) that sold encrypted phones at a cost of around EUR 1 000 worldwide and offered subscription services with 24/7 support at a cost of EUR 1 500 for a 6-month period.

In addition to secure communications services, EncroChat provided users with hardware that was untraceable (no association with the device or SIM card) and physically modified to ensure a higher level of security (removal of the camera, microphone and USB port, disabled GPS module). These phones used dual operating systems, with the encrypted system interface being hidden from the naked eye and made less easily detectable. Some features of the software developed included various ways of deleting data: erasure of the content of the device by the user or support service from a distance, 'alternative' access credentials for the devices that, instead of providing access to the device, erased all the content on it, etc. Therefore, the services themselves and all the surrounding aspects of them (including the hardware and software) were designed with providing almost full anonymity to users in mind.

EncroChat devices were found in the investigations concerning OCGs. It became evident that there were EncroChat user hotspots in source and destination countries for cocaine and cannabis, as well as in money laundering centres.

Issues encountered

An inherent issue in cases of cybercrime facilitation – be it, as in this case, the abuse of encrypted communications services or something else – is the level of proof needed to establish the criminal character of the facilitation activities. This is relevant with regard to meeting the criteria of double criminality within a request for international judicial cooperation and/or to begin a criminal investigation in another jurisdiction for the purposes of coordinated parallel investigations.

Another challenge was ensuring legal compliance when putting a technical solution in place to circumvent the encryption techniques and access users' communications in the different jurisdictions.

As intercepted communications revealed criminals' interactions on planning serious criminal acts, certain measures needed to be put in place to ensure proactive responses to life-threatening situations.

There was also a need to protect the source of the information in relation to spin-off investigations based on the interception and analysis of communications.

Given that there is no exclusive jurisdiction to prosecute the facilitation of criminality and associated offences, there was a need for a strategic approach to de-confliction of investigations and a mutual understanding on prosecuting jurisdictions.

Another issue encountered was the impossibility of simultaneously dismantling the encrypted communications services and addressing all the underlying criminality.

Eurojust's involvement

Eurojust ensured close cooperation and coordination among the prosecuting and investigating authorities. Six coordination meetings were organised, where decisions were taken to facilitate the execution of coordinated actions to make simultaneous arrests and searches, prevent conflicts of jurisdiction, and continue with parallel investigations and exchange of information.

To facilitate the demanding investigation run at international level, the French and Dutch judicial authorities established a JIT, which was set up and funded with the assistance of Eurojust.

The interception of EncroChat messages came to an end on 13 June 2020, when the company realised that a public authority had penetrated the platform. EncroChat then sent a warning to all its users advising them to immediately destroy the phones.

While the activities on EncroChat have been stopped, this complex operation shows the global scope of serious and organised crime and the connectivity of criminal networks that use advanced technologies to cooperate at national and international levels. The effects of the operation will continue to echo in criminal circles for many years to come, as information obtained from it has been provided to hundreds of ongoing investigations and has also triggered a very large number of new investigations of organised crime across Europe and beyond.

Operation Cepheus

Case summary

Operation Cepheus was an investigation by the Australian authorities into a computer hijacking tool, the Remote Access Trojan (RAT), that was of significance because of its features, ease of use and low cost. Sold for USD 25, it took full remote control of victims' computers, stealing data and passwords and watching the victims via their webcams. The hackers were able to disable antivirus and anti-malware software, carry out commands such as recording keystrokes, and steal data and login credentials.

The spyware was sold to more than 14 000 buyers in EU Member States and third countries, and it was subsequently deployed by users in 124 countries.

Issues encountered

Initial problems encountered were a massive number of victims – estimated to be in the tens of thousands – and large datasets of stolen personal details, passwords, private photographs, video footage and other electronic data that needed to be analysed for intelligence and evidence-gathering purposes.

An addition layer of problems related to an inherent issue in cases of cybercrime facilitation – be it, as in this case, the abuse of remote access tools or something else, such as the provision of encrypted communications services – namely the level of proof needed to establish the criminal character of the facilitation activities. This is relevant with regard to meeting the criteria of double criminality for a request for international judicial cooperation and/or to begin a criminal investigation in another jurisdiction for the purposes of coordinated parallel investigations.

Finally, there were issues relating to gaining legal authorisation for the direct cross-border application of tailor-made software as part of covert operations to retrieve specific data from suspects' computers in various jurisdictions and the evidential value of the data collected in this way.

Eurojust's involvement

With perpetrators and victims located worldwide, Eurojust supported and coordinated the activities of the judicial authorities of Australia, Belgium, Colombia, Czechia, the Netherlands, Poland, Spain, Sweden and the United Kingdom. This was done in close liaison with Europol's European Cybercrime Centre and Joint Cybercrime Action Taskforce and the European Judicial Cybercrime Network, which is hosted by Eurojust.

Given the legal implications, Eurojust supported discussions in relation to the legal restrictions and requirements of various jurisdictions concerning the criminal character of the remote access tool, as well with regard to legally penetrating the servers used by the perpetrators and using the data retrieved as admissible evidence in courts.

Thanks to the coordinated approach taken, the spyware's infrastructure has been taken down, RAT can no longer be used by those who bought it and no further harm is being perpetrated.

Operation Bruno

Case summary

This was an investigation by the Romanian and Italian authorities into a multinational OCG that used spear-phishing emails impersonating the tax authorities to collect the online banking credentials of the victims targeted. The stolen banking credentials were used for consecutive transfers of money from the victims' accounts into accounts under the control of the OCG. As a final step, money was withdrawn from ATMs located in Romania.

Issues encountered

The highly organised OCG pursued its criminal activity using encrypted chat applications. It established its power by applying intimidating and punitive methods to affiliates and competitors. Members of the OCG were also suspected of money laundering, drug and human trafficking, prostitution and participation in a criminal organisation.

Eurojust's involvement

Eurojust ensured close cooperation and coordination among the prosecuting and investigating authorities. Two coordination meetings were organised, where decisions were taken to facilitate the execution of coordinated actions to make simultaneous arrests and searches, prevent a conflict of jurisdiction (a *ne bis in idem* issue), continue with parallel investigations and exchange of information, and organise a coordinated action day. A coordination centre was set up at Eurojust, facilitating exchange of information between the countries involved and providing a final overview of the results.

To facilitate the demanding investigation run at international level, the Romanian and Italian judicial authorities established a JIT, which was set up and funded with the assistance of Eurojust. The JIT enabled efficient cooperation and coordination, including the continued exchange of information and evidence between Italy and Romania.

A 2-year-long cybercrime investigation by the Romanian Directorate for Investigating Organised Crime and Terrorism, the Romanian National Police, the Prosecution Office of Milan and the Italian National Police, with the support of Eurojust, Europol and Europol's Joint Cybercrime Action Taskforce, led to the arrest of 20 suspects in a series of coordinated raids. Nine individuals were detained in Romania and 11 were arrested in Italy for banking fraud that netted EUR 1 million from hundreds of customers of two major banking institutions. The Romanian authorities conducted 15 house searches involving 120 Romanian police officers, while the Italian authorities carried out 9 home and computer searches involving more than 100 Italian police officers. Documents, IT devices, drugs and other materials were seized in Romania and Italy.

In April 2019, the Italian authorities sentenced the accused to serve between 2 and 5 years in prison and to pay a combined fine of almost EUR 9 000. Various assets with a total value of almost EUR 138 000 were also confiscated. In addition, the defendants were sentenced to pay damages to the victims.

Operation against GozNym criminal network

Case summary

This case involved an investigation by the United States authorities into a complex, globally operating and organised cybercrime network, which used GozNym malware to steal an estimated USD 100 million from more than 41 000 victims, primarily businesses and financial institutions.

GozNym malware was designed to capture victims' online banking login credentials. Once the credentials were obtained, the perpetrators gained access to victims' online bank accounts and stole the money by making transfers to bank accounts under their control.

'Bulletproof' hosting services were provided to the GozNym criminal network by an administrator of the service known as the Avalanche network. The Avalanche network provided hosting services to more than 200 cybercriminals and hosted more than 20 malware campaigns ([8]).

Issues encountered

The OCG exemplified the concept of cybercrime as a service, providing various criminal services such as cyberattacks, bulletproof hosting, money mule networks, 'crypters' (encryption of malware to avoid detection by antivirus tools and protective software), spamming (mass distribution of the malware through phishing emails), coding, organisation and technical support.

Eurojust's involvement

Eurojust, with all the actors involved at the levels of law enforcement and the judiciary, played a critical role in supporting this coordinated operation, by holding coordinating meetings, helping with exchange of information, evidence and judicial best practices, and providing financial support and interpretation services.

The German and Bulgarian national desks at Eurojust made major contributions, and the successful result of the operation was also due to the active roles taken by the liaison prosecutors from the United States and Ukraine and Eurojust's contact points in Georgia and Moldova. Specific experience and expertise was also provided by the European Judicial Cybercrime Network.

Operation Warenagent

Case summary

The Lithuanian and German authorities conducted a successful 6-year investigation, Operation Warenagent, into organised cyberfraud. The lengthy and extensive investigations revealed that, since 2012, more than 35 000 items of high-quality merchandise, such as smartphones, computers, navigation devices, TVs, vacuum cleaners and branded clothing, had been illegally obtained by the OCG, which maintained a strict hierarchy and distribution of roles. Various shippers ordered the merchandise through a network of agents recruited in Germany, using fraudulently obtained credit card information. The agents acted as recipients of the merchandise and transferred the shipments to addresses located abroad. The merchandise was then forwarded to other accomplices to conceal their own as well as the final recipients' identities. The illegal merchandise was reportedly sold mainly in eastern Europe, namely in Russia, Ukraine and the Baltic states.

Issues encountered

Difficulties encountered in the investigations related to the high level of conspiracy through technological means: offenders were active online using only codenames and encrypted/anonymised access to the network (Tor, virtual private networks, proxy servers, etc.), all payments were made using cryptocurrencies,

([8]) For more information on the dismantling of the Avalanche network, please refer to Eurojust's publication *Operation Avalanche – A closer look*, April 2017 (available at https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2017-04_Avalanche-Case_EN.pdf).

and the OCG members communicated online using sophisticated databases regularly updated with illegal activity reports.

In addition, the OCG was very agile in coordinating its activities across borders; goods were usually ordered from mid-European service providers and sold in eastern Europe. Investigations into this type of criminality need timely coordination in several countries in parallel. The same issues were encountered at the level of the judiciary at a later stage, as coordination was necessary to decide where members of the OCG should be prosecuted.

Eurojust's involvement

Eurojust provided support to the national authorities throughout the investigations. As a result of the judicial cooperation between the German and Lithuanian authorities, five coordination meetings were held at Eurojust.

The two countries entered into a JIT agreement with the support of Eurojust. The JIT helped simplify and accelerate the exchange of case-related information between the national authorities concerned. In total, national authorities from eight European countries were finally involved in the investigation.

Eurojust contributed to the successful outcome of the operation by coordinating the pre-trial investigation with national prosecutors and police officers, as well as by facilitating and supporting international judicial cooperation.

In October 2017, Lithuanian and German police officers conducted 11 searches in various Lithuanian cities, leading to the arrest of 5 suspects. In the period from 12 to 15 June 2018, a cross-border operation was carried out in various countries across Europe: 31 private residences and business premises were searched in Cyprus, Finland, Estonia, Germany, Latvia, Lithuania, Switzerland, Ukraine and the United Kingdom, 6 arrests were made in Germany, Lithuania and Switzerland, and the organiser of the OCG was arrested in Cyprus. Two further actions, with 4 arrests and 10 searches, took place in Lithuania between 26 and 29 June 2018.

Operation Triangle

Case summary

A large-scale OCG, consisting of members mainly from Nigeria and Cameroon, was responsible for carrying out phishing fraud totalling EUR 6 million. This criminal network used the 'man in the middle' method, diverting funds from legitimate to illegitimate destinations by accessing passwords and personal data to acquire ownership of victims' email inboxes and illegitimately obtain money from them and/or from their customers.

Issues encountered

The case involved numerous countries, with perpetrators and victims identified in at least 16 jurisdictions worldwide.

Parallel proceedings taking place in Italy and Spain revealed that individuals under investigation were part of hierarchically structured cells with fluid and flexible interactions between the networks. In view of these close connections, challenges to the domestic prosecuting authorities were identified in relation to potential *ne bis in idem* issues. A possible overlap of targets was highlighted, meaning that the same suspects could be the subject of multiple criminal proceedings instituted in different jurisdictions.

Eurojust's involvement

The national authorities in Italy, Poland and Spain referred their cases to Eurojust for judicial coordination. Several coordination meetings were held to clarify the details of existing domestic investigations and exchange information.

With a view to undertaking simultaneous coercive measures, the parties agreed on a suitable time for the joint action day, which was supported by a Eurojust coordination centre. While the Spanish authorities could have taken action quite quickly, early intervention in Spain might have jeopardised the less advanced but broader Italian investigation.

Dialogue on the legal requirements in the different jurisdictions was necessary to understand the restrictions on the proceedings in the various countries and to determine the most favourable schedule for joint action. Owing to the information exchanged during the meeting, a compromise regarding the date of the action day was achieved. It took place in June 2015 and was led by Italian, Polish and Spanish judicial and police authorities, with the support of Belgium, Georgia and the United Kingdom . A total of 49 suspects were arrested and 58 searches carried out. Facilitated by the coordination centre, the joint action yielded excellent operational results in the fight against cybercrime and fraud, and sent a strong deterrent message to cybercriminals, proving that through close judicial cooperation and coordination between countries, prosecutions in cybercrime cases can take place in any jurisdiction.

Operation Mickey Mouse

Case summary

The Romanian national authorities, in close cooperation with the Dutch national authorities and with the active support of Eurojust, dismantled an OCG involved in cybercrime, fraud and organised property crime that caused damages estimated at EUR 2 million during the period from 2017 to 2019.

The members of the OCG 'spoofed' emails from cargo companies (modified and disguising the emails so that they appeared to have been sent from a known/trusted source), pretending to be the companies' representatives. They then received offers for cargo services from various victims, signed the counterfeit contracts, and scheduled the date and place of the cargo delivery. Once they received the cargo, the members of the OCG appropriated the prepayment for the cargo service and the cargo itself, using forged documents and vehicles with fake licence plates. The stolen cargo, which was later resold within the European Union at a considerably lower than market price, consisted of a variety of goods, including solar panels, aluminium bars and clothing.

Eurojust's involvement

Eurojust provided for smooth and effective cooperation by organising two coordination meetings and by facilitating the drafting, transmission and execution of several European Investigation Orders and MLA requests issued by Romania to Belgium, Czechia, Germany, Hungary, Luxembourg, the Netherlands and Poland.

During the joint action day, a coordination centre was set up at Eurojust, which enabled real-time exchange of information between the authorities.

Overall, 46 houses and several trucks were searched, 6 suspects were identified and presented before the Romanian prosecutor, 14 witnesses were heard, and telephones, laptops, forged ID documents and licence plates, as well as stolen goods, were seized.

Operation Dark Room

Case summary

The Norwegian national authorities began an investigation in relation to child sexual abuse. A suspect in Norway was taken into custody, but there was additional suspicion that a Romanian resident was involved in the online sexual abuse of her own child. Norwegian authorities sent an urgent MLA request on 10 August 2017 regarding the required investigative steps in Romania. Even though the Norwegian perpetrator had

been taken into the custody, there was a great risk that the Romanian perpetrator might be offering 'services' to others, and therefore a possibility that a child was being exposed to sexual abuse by their mother.

Issues encountered

The main aims were to ensure the safety of the child and to secure witness statements from the child victim. Norway has a unique model for hearings of children as victims/witnesses. The child is, with parents or guardians, invited to a safe facility (known as a 'Children's House'). A specially trained investigator takes evidence in a neutral and transparent manner, with only the investigator and the child present. The victim's lawyer and the defence lawyer are located in a separate room. The defence lawyer can address additional questions to the investigator during breaks, and the investigator can in turn ask the victim. The recorded video statement is then used as admissible evidence in court.

The next challenge was to secure/obtain evidence admissible in both countries, since the countries had decided to cooperate on coordinated parallel proceedings, with one trial, of the buyer of the services, taking place in Norway and another, of the seller of the services, in Romania.

Eurojust's involvement

Establishing direct contact with the executing authorities in Romania and formulating a detailed plan on the initial phase of the investigation were important first steps. Discussions revolved primarily around the prosecutorial strategy, avoiding the *ne bis in idem* situation, and the methods for the hearings of the suspects and witnesses, including those who were under age.

The swift and excellent cooperation between the Romanian and Norwegian desks at Eurojust was crucial, as the first coordination meeting was held within 3 weeks of the opening of the case at Eurojust. Norway presented its findings and the Romanian delegation declared that it was highly motivated to start its own investigation of the suspect, who was living in Romania. A second coordination meeting was organised in Romania and a JIT agreement was signed. The suspect was arrested the day after that, and the child was taken into care. This excellent result was achieved only 6 weeks after Eurojust received the first MLA request.

Eurojust's publications and projects in the area of cybercrime

Eurojust produces various products related to cybercrime and cyber-enabled crime, highlighting challenges and best practices based on the analysis of lessons learned not only from Eurojust casework but also from national experiences and court decisions shared with Eurojust, which may be of interest to practitioners in view of facilitating cross-border electronic evidence gathering.

Eurojust issues the ***Cybercrime Judicial Monitor*** (CJM) on a yearly basis. The CJM serves as a regular reporting tool to support practitioners in the investigation and prosecution of cybercrime cases. It aims to provide relevant authorities with useful information on legislative developments, court rulings, emerging trends and issues related to cybercrime.

Repository of issues of the CJM

Eurojust and Europol have published a jointly drafted paper, **'Common challenges in combating cybercrime'**, which looks at these challenges predominantly from law enforcement and prosecution perspectives. The document was first published in 2016 and was updated in 2017 and 2019. It identifies six main challenging areas: loss of data, loss of location, legal frameworks, public–private partnerships, international cooperation, and the rapidly developing threat landscape and resulting expertise gap. The paper serves as a starting point for further discussions with relevant stakeholders about possible approaches to address these challenges, including further alignment of legal and practical instruments concerning MLA and exchange of information and electronic evidence for the purpose of criminal investigations and prosecutions.

Latest version of 'Common challenges in combating cybercrime' (June 2019)

Eurojust and Europol draft a joint annual **report on encryption in relation to the encryption observatory function**, which is based on the measures proposed by the European Commission in its *11th progress report towards an effective and genuine Security Union*. The report examines the landscape, including new and emerging trends and developments, and highlights the challenges faced by law enforcement and judicial authorities with respect to encryption.

Latest report of the observatory function on encryption (January 2020)

Eurojust and Europol are co-partners in the **Sirius project**, which is a knowledge library for EU law enforcement and judicial authorities providing information on how to obtain electronic data from (mainly) US-based service providers. To help national judicial and law enforcement authorities gain access to electronic evidence, the project team has prepared guidelines, templates for data requests to service providers and other specialised products, which can be used in, inter alia, cybercrime investigations and prosecutions.

Further information on the SIRIUS Project.

Eurojust, Johan de Wittlaan 9, 2517 JR The Hague, The Netherlands
www.eurojust.europa.eu • info@eurojust.europa.eu • +31 70 412 5000
Twitter & LinkedIn: @Eurojust

Print: Catalogue number: QP-02-20-836-EN-C • ISBN: 978-92-9490-504-8 • DOI: 10.2812/177738
PDF: Catalogue number: QP-02-20-836-EN-N • ISBN: 978-92-9490-503-1 • DOI: 10.2812/691335