Combating Cryptomarkets: Cross-Border Cooperation and Investigation

THEMIS Competition 2018

Semi-Final A: International Cooperation in Criminal Matters

Team Czech Republic:

Petra Hodysová
Miroslav Kaštyl
Sarah Kubaričová

Tutor:

Petr Kolban

Contents

Introduction

Modern life without new means of communication and information technology (IT), including the Internet and computers, is something beyond imagination. We live in the „*digital or information age*“, which creates loads of possibilities, opportunities and advantages in many fields, but as always, the bright side has its dark side too. Nearly unlimited possibilities of information technologies facilitate committing criminal activity on a new level without any border restrictions, in cyberspace. This term was firstly used by William Gibson in his cyberpunk book called Neuromancer published in 1984. Nowadays, it is closely associated with the phenomenon of the Internet and many related definitions exist. Czech legal definition states that cyberspace is *a digital environment enabling the creation, process and exchange of information, formed by information systems, electronic communication services and networks.*[1]

Cyberspace can be divided into 3 parts: the Surface web,[2] Deep web and Dark web. Deep and dark webs are often termed as Darknets. Darknets contain more than 90% of the information on the Internet, but it's not accessible by "the surface web viewers (surfers)". Dark web is a part of the Deep web accessible only through certain browsers designed to ensure anonymity through TOR ("The Onion Router"), I2P ("Invisible Internet Project") and other networks.[3] Dark web can be used for many purposes including private communication, political protests in places where freedom of speech is not fully guaranteed, but also for spreading illegal goods and information through so-called cryptomarkets - hidden market places.

These dark web sites often offer illegal goods for sale such as drugs, weapons, pornography content, stolen data or even illegal services like hacking for hire etc. Some of these cryptomarkets are even publicly known, such as Silk Road, which used to be called "the ebay of illegal goods".[4] Beside the illegal trade, they provide anonymity to their users, transactions carried out by cryptocurrencies protecting both vendors and buyers, and offer a huge financial turnover affecting not only the dark economies across the world. To be fair, cryptocurrencies can be also used for legal trade.

Cryptocurrencies are virtual digital currencies such as Bitcoin, Litecoin, Ethereum etc. The most well-known is Bitcoin, which is decentralized digital currency ("digital cash") that can

[1]See Section 2 under the Act No. 181/2014 Coll., on Cyber Security

[2]Sometimes also called the Visible Web, Clearnet or Indexed Web. It includes web sites such as Google, Facebook and Youtube.

[3]Kolouch Jan. *CyberCrime*. 1. vydání, Praha: CZ.NIC, z.s.p.o., 2016, p. 47-48.

[4]https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/

be sent or received through the internet without involving the bank or "middleman" for the transaction. It is controlled only by the owner of the bitcoin, it can be obtained by different ways and stored in always accessible „bitcoin wallet"- no matter the time. Network is always working and it is made of millions of individual users.[5]

The existence of cryptomarkets involves highly complex cybercrimes, an evolving form of transnational global crime carried out in the border-less cyberspace that cannot be adequately dealt with by single jurisdiction approaches to policing and investigation – combating cryptomarkets requires multilevel international cooperation. Also every model of cooperation offers different advantages as well as its own drawbacks; therefore it represents a unique opportunity to explore it, which is why we have chosen this topic.

In our paper, we shall describe the term cybercrime, focus on the legal framework of international cooperation with accent on the Convention on Cybercrime and European law, introduce European context of police and judicial coordination while combating cryptomarkets and finally outline the scope of cooperation with a private sector.

To summarize, the aim of the paper is to present the legal basis of the international cooperation within the context of the cybercrime and cryptomarkets, and to find out, what seems to be the appropriate approach for successful suppression of the cryptomarkets and what are the loopholes of current situation.

1. Cybercrime and legal framework

1.1. Cybercrime

Traditional crime often possesses strict definition in national legal provisions. On the other hand, commonly used definition of cybercrime still does not exist. It used to be called computer crime but due to the fast development in IT, it could be also committed via other electronic device and mean of the communication. For purposes of this paper, we concluded, that cybercrime is illegal and harmful activity carried out in the cyberspace, with the use of internet, computer network or other network technologies, to gain any profit out of the action, and to some extent it symbolises online dangers and risks. Main characteristics of cybercrime include technical complexity with ambivalent feelings, fast progress in the increase of the vulnerability as well as in the possibilities of breaching the rights and cryptography as a mean

[5] https://academy.bitcoin.com/#/what-is-bitcoin/.

of protection and obstacle to detect the offenders.[6] With respect to our previous explanation what cryptomarkets are, we must point out that not all cybercriminal activities include involvement of cryptomarkets.

The problem with definition results in many cybercrime classifications outlining what is understood by related criminal behaviour. For purposes of this paper, we shall describe two of them. Cybercrimes according to the Convention on Cybercrime (see below) are offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences, offences related to infringements of copyright and related rights. Additional protocol defines other cybercrimes related to racist and xenophobic issues. Another classification of the cybercrimes concentrate on the role of the personal computer; whether it is a target of the attack or the instrument of the attack, and on the type of the act; whether it is traditional illegal acts such as forgery of a bank notes or new illegal acts such as phishing, ransomware, DDoS.[7]

Because cybercrimes are committed in a cyberspace, they are not limited by any borders, which of course the perpetrators take advantage of. To be able to respond to new criminal phenomena, properly investigate the suspicious conducts and prosecute the offenders, the need for international cooperation arises.

1.2. International law: Convention on Cybercrime

On global scale, police and judicial cooperation are governed by bilateral and multilateral treaties and implemented directly by individual states. Prevailing principle is principle of mutual legal assistance, such as in the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters[8] and its additional protocols.[9] In general, principle of dual criminality often applies, therefore harmonisation of national legislation is desirable.

The most important outcome of international cooperation related to suppression of cybercrime is the Convention is the Convention on Cybercrime (ETS No. 185),[10] which is the first international treaty on crimes committed via the Internet and other computer networks. This

[6]GŘIVNA, Tomáš and POLČÁK, Radim ed. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. p. 34-35
[7]Kolouch Jan. *CyberCrime*. 1. vydání, Praha : CZ.NIC, z.s.p.o., 2016, p. 38.
[8] Council of Europe Convention on Mutual Assistance in Criminal Matters was ratified by 47 Council of Europe member states and also by Chile, Israel and Republic of Korea.
[9]Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (1978) and Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (2001).
[10]Full text of the Convention on Cybercrime available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

most important legal document about combating cybercrime was introduced by the Council of Europe to protect societies from the related threats worldwide. The convention was opened for signatures on 23/11/2001 in Budapest (therefore also referred to as "the Budapest Convention"), and came in force on 1/7/2004. It is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.[11]

According to the preamble of the Convention, it was introduced having in mind changes brought by the digitalisation, convergence and ongoing globalisation of computer networks and due to the believes that increased, rapid and well-functioning international cooperation in criminal matters, common criminal policy and appropriate legislation on domestic and international levels would lead to effective fight against cybercrime and protection of the legitimate interests in the use and development of IT. Therefore, the main objective of the Convention is to establish common minimal standards for purposes of the harmonization of the national legislation of the substantive law, procedural law and as a framework for international cooperation while combating the cybercrime.

The Convention is divided into preamble and four chapters containing 48 articles. The most important used terms (computer system, computer data, service provider and traffic data) are defined in Chapter I. Chapter II. outlines what measures have to be carried out by the contracting party at the national level. This chapter is divided into three sections: substantive criminal law, procedural law and jurisdiction. In the articles about substantive criminal law, there is description of the cyber offences[12] with the result of new cybercrime classification as mentioned above, followed by ancillary liability (such as aiding, abetting and corporate liability) and sanctions. In the second part of Chapter II. (procedural law), the specific investigative methods and competences are stated. They are essential for the detection of computer crimes and are evincible by high instability of electronically saved data because of the easiness of their transfer, change or destruction. Coherent articles incorporate provisions about expedited preservation of stored computer data (including traffic data), production order, search and seizure of stored computer data either saved in computer system or memory storage media, real-time collection of computer data.

[11]Until today, 60 states signed the Convention and 56 ratified it. For more details see https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Lswq5GgK.

[12]Illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights.

Chapter III. provides legal framework for international cooperation and is divided into two parts called general principles and specific principles, where the section about general principles includes provisions about extradition and mutual assistance. This is the main part of the Convention with the regard to our topic, we dedicate it separate sub-chapter. Last Chapter IV. covers final provisions such as signatures, entry into force, accession to the convention, effects of the convention and so on.

1.2.1. International cooperation under the Convention on Cybercrime[13]

International cooperation under the Convention is designed to be complementary to the existing instruments. It should be commonly used in the context of the application of the international treaties on mutual assistance or extradition or in the accordance with domestic law. This statement arises from the Article 23, which establishes general principles related to international cooperation as follows. International cooperation shall be provided among parties of the Convention to the widest possible extent in accordance with the provisions included in the Chapter III, through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws. Cooperation is for the purposes of investigations or proceedings of cybercriminal offences as well as for the collection of evidence in electronic form („digital evidence“) related to any criminal offence.

Provisions about extradition including coherent general principles as well as possible application of “extradite or prosecute” principle are covered in Article 24. Article 25 about mutual assistance firstly repeats some of the general principles introduced in Article 23. Parties have to establish national legal basis to carry out the specific measures adapted in the Convention as written below. This article aims at speeding up the process of obtaining a response to a coherent request by different secured means of communication. It also sets principle that mutual assistance is subject to the conditions of applicable mutual assistance treaties and domestic laws and provides definition of dual criminality. Article 26 allows contracting party authority to spontaneously provide obtained information to another party without requesting it to help with the initiating or carrying out cybercrime investigations or proceedings or which could eventually lead to a request for cooperation by that party. Next

[13] Article about international cooperation under the Convention on Cybercrime published by Council of Europe is available athttps://rm.coe.int/1680304352.

article includes loads of basic provisions in case of absence of applicable international agreements on mutual legal assistance, which was mainly adopted because of non-European countries-parties. Also according to this article parties have to designate a central authority responsible for sending and answering requests for mutual assistance.[14]Article 28 is concerned about confidentiality and using limitation of provided information if no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation exists between the requesting and the requested parties.

Second part of Chapter III includes specific provisions about application of modern procedural measures with provisional or investigative nature, which are very important to carry out concrete operative actions while combating cybercrime. The expedited preservation of stored computer data (adapted in the Article 29) can take place in the order to carry out very quick action to save the data, if the requesting party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. Next article deals with expedited disclosure of preserved data, due to the fact, that data often transit several countries and servers. Therefore, a service provides must disclose sufficient amount of the data to be able to identify the path through which a communication was transmitted. Article 31 is about the request to search or access, seize or secure and disclose data stored on a computer system located in foreign territory. Article 32 states that party may trans-border access publicly available stored computer data even without consent and through computer system in its territory it can also access or receive stored computer data located in another's land if the person authorized to handle such data agree. Articles 33 and 34 deal with interception of data. First one covers the real-time collection of traffic data. Second one is about interception of content data, which represent high level of intrusion; therefore restrictions in mutual assistance apply.

Last part of specific provisions within international cooperation is concerned about 24/7 Network under Article 35. This network of contact points available on 24 hours, 7 day-a-week basis was introduced in the order to ensure the immediate urgent action for the purpose of cybercrime investigation or proceedings or for collection of its electronic evidence in another country. Contact points should have the capacity to carry out communications with each other on an expedited basis, be able to coordinate on expedited basis with authorities responsible for

[14] In the Czech Republic, the authorities responsible for submitting and handling requests for mutual assistance, the execution of such requests or their transmission to the authorities responsible for their implementation, are the Supreme Prosecutor's Office (when the case is not yet before the court) and the Ministry of Justice (after the case has been handed over to the court).

international mutual assistance or extradition and to ensure trained and equipped personnel to facilitate the network operation. The idea of 24/7 contact points was born from the "G8 Hi-Tech Crime Subgroup" created in 1996 - real and effective contact points network among G8 states (8 major industrial nations) was established in 1998.[15]

As we introduced the main international legal instrument against cybercrimes, we move on to the European Union.

1.3. EU law

Police and judicial cooperation in the European Union is one of the three pillars of the EU and as such is enshrined in Article 67 paragraph 3 of the Treaty on the Functioning of the European Union (TFEU).[16] According to Article 82 and 83 of the TFEU, judicial cooperation in criminal matters in the EU shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations. The European Parliament and the Council shall adopt measures to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension. Based on these provisions, several directives concerning police and judicial cooperation in criminal matters were adopted.[17] The most used tool is probably the European Arrest Warrant (EAW),[18] which is operational since 2004. Its aim is to arrest and surrender requested person in one Member State, for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order in another Member State.[19] It was followed by the European Evidence Warrant (EEW) and it has to be stressed that both of these instruments made cooperation between EU member states much easier. However, it turned out that the EEW has some flaws and can be used only when there is certainty about whereabouts of the evidence, which resulted in the

[15] For more details see discussion paper prepared by Pedro Verdelho: *The effectiveness of international cooperation against cybercrime: examples of good practice*, available at https://rm.coe.int/16802f69c3.
[16] Art. 67 par. 3 of the Treaty on European Union and the Treaty on the Functioning of the European Union (2012/C 326/01) reads as follows: The Union shall endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws.
[17] For example Council Framework Decision 2008/909/JHA, Council Framework Decision 2008/947/JHA, Council Framework Decision 2009/829/JHA.
[18] Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States.
[19] Art. 1 par. 1 of the Council Framework Decision 2002/584/JHA.

establishment of the European Investigation Order (EIO).[20] Last but not least, there are Council Decisions concerning freezing and confiscation orders and European Supervision Order.[21] All of these tools are vital for combating all kinds of criminality, including cybercrime. It needs to be emphasised, that there are no special procedural provisions or tools concerning specifically cybercrime.

In case of crypto markets, the cooperation focuses mainly on a seizure of illicit goods (such as drugs) obtained through crypto markets, a seizure of crypto market´s hardware (such as servers), a seizure of cryptocurrencies and arrests of persons who created or help to maintain the crypto market running. Hence it is mixture of traditional legal measures supplemented by measures relevant for cyberspace, especially where electronic communication data and cryptocurrencies are involved. In this regard, recently we have seen several attempts to minimize discrepancies and unify the legal standards within EU. Some of them were more successful than others.

Thus in 2006 the Directive on the retention of data was adopted to retain telecommunications data for investigation and prosecution of serious crimes.[22] However, in its ruling of 8 April 2014 the European Court of Justice overturned (invalidated) the Data Retention Directive due to wide-ranging collection of data which particularly violated right of privacy.[23] Consequently, the ruling disturbed capability of public authorities to obtain data from private sector (such as internet service providers) for criminal investigations. In December 2016 the Court delivered another judgment concerning implementation of the Directive in two member States and its violation of EU law. In 2017 the future of data retention was still debated within EU analysing the implications of the judgements potential impact on international judicial cooperation in criminal matters indicating that the data retention should be still available on a limited scale based on a judicial warrant.[24] In this regard, Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in

[20] Directive (EU) 2014/42 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union 2014/41/EU.

[21] Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence, OJ L 196 of 2/8/2003; Council Framework Decision 2003/577/JHA on the application of the principle of mutual recognition to confiscation orders, OJ L 328 of 24/11/2006.

[22] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. It required providers of electronic communications services or public communications networks to retain traffic and location data, for example Internet protocol addresses, the numbers dialled, call transfer records. These were supposed to be stored for at least six months.

[23] For more details see Judgment of The Court (Grand Chamber), Digital Rights Ireland Ltd. (C–293/12) v. Minister for Communications, Marine and Natural Resources. Basically, general and indiscriminate retention obligation for crime prevention and other security reasons is not in accordance with fundamental rights.

[24] See Council of the EU, Working Party on General Matters, February 9, 2017, Available at:http://data.consilium.europa.eu/doc/document/ST-6159-2017-INIT/en/pdf.

criminal matters should be mentioned.[25] Its aim was to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy when their personal data are transmitted or made available for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[26] It was later replaced by the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing.

While combating cryptomarkets the expanding use of cryptocurrencies represents another challenge as suspicious anonymous transactions are usually not sufficiently monitored by public authorities in order to link them to specific persons. Thus the issue of monetization through cryptocurrencies is impairing the efforts of public authorities.[27] Yet for a long time the cryptocurrencies have not deserved adequate attention within EU. In 2016 first proposals for amendment of existing legal framework related to money laundering emerged to control an access to virtual currencies.[28] The still ongoing debate for cryptocurrencies regulation is currently planning to disclose identities of private traders and the platforms for trading (exchanging) currencies should meet the standard of due diligence and report suspicious transaction. However, as a connection between cybercrime and especially crypto markets and cryptocurrencies is more apparent nowadays, more legal obligations will probably follow in the future.

As already stated, cybercrime is rising phenomenon and therefore number of legal instruments concerning cybersecurity and related issues have been adopted. However, due to limited extent of this paper, we cannot dwell on it any further.

[25]Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
[26] Article 1 para 2 of the Framework Decision 2008/977/JHA.
[27] See Council of the EU, Report from Eurojust / Europol Delegations. *Common challenges in combating cybercrime,* Brussels, March 13, 2017, Available at:http://data.consilium.europa.eu/doc/document/ST-7021-2017-INIT/en/pdf.
[28] See for example Proposal for a Directive amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC.

2. Institutional Level

Moving from legal framework to institutional level, police and judicial cooperation in criminal matters predominantly takes place between national police and judicial authorities. Nevertheless, substantive support and in some cases even the main role of transnational agencies cannot be omitted. We shall focus on Europol and Eurojust as the two main agencies in the EU, although we are well aware that for instance part of Interpol´s agenda are also initiatives related to cybercrime such as operational and investigative support, cyber intelligence and analysis, digital forensics, etc. Finally, we shall introduce so-called Joint investigation teams as a typical example of multilevel cooperation.

2.1. Europol

Europol (The European Union Agency for Law Enforcement Cooperation) was established in 1999 by the Europol Convention.[29] Its objective is to improve the effectiveness and cooperation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international crime where there are factual indications that an organized criminal structure is involved and two or more Member States are affected by the forms of crime in question in such a way as to require a common approach by the Member States owing to the scale, significance and consequences of the offences concerned.[30]

Its main tasks is to facilitate the exchange of information between the Member States, to obtain, collate and analyse information and intelligence, to aid investigations in the Member States and to maintain a computerized system of collected information.[31] Competences of Europol were recently updated[32] in order to strengthen its role in supporting cooperation among law enforcement authorities in the EU. Updated powers should enable Europol to step up efforts to fight cybercrime and other serious modern threats.[33]

Each Member State is represented by national unit, which serves as the only liaison body between Europol and the competent national authorities and carries out tasks listed in the Europol Convention.[34] Agreements on operational and strategic cooperation are adopted in

[29]Council Act 95/C 316/01 of 26 July 1995 on the establishment of a European Police. Its adoption was based on the Article K.3 TEU (Maastricht Treaty).
[30]Article 2 par. 1 of the Europol Convention.
[31]Article 3 of the Europol Convention.
[32]By the Regulation (EU) 2016/794 of the European Parliament and of the Council.
[33] https://www.europol.europa.eu/newsroom/news/europols-new-regulation.
[34]Article 4 of the Europol Convention.

order to establish cooperative relations and develop framework for operative collaboration between Europol and non-EU states.[35]

Concerning cybercrime, the Europol among others established in 2013 the European Cybercrime Centre (EC3). Its task is to strengthen the law enforcement response to cybercrime.[36]It serves as the European cybercrime information focal point, pools European cybercrime expertise to support Members States in capacity building, provides operational support to Member States' cybercrime investigations (for example by encouraging the establishment of cybercrime Joint Investigations Teams and the exchange of operational information in on-going investigation and by providing high-level forensic assistance and encryption expertise for cybercrime investigations).[37]

2.2. Eurojust

The European Union's Judicial Cooperation Unit basically stimulates judicial coordination and cooperation between national judicial authorities to combat cross border and serious organised crime affecting more than one EU country. The emphasis of cooperation is underlined in relation to Europol and European Judicial Network.[38]

The agency generally helps with difficulties concerning mutual legal assistance in criminal matters, extradition requests and addresses the question of jurisdiction to prosecute in cross-border cases. It further improves the coordination of investigations and prosecutions between responsible authorities and at the request; it might also help with the cooperation between member and non-member states. However, originally, it has not been designed for operational

[35] For the list of agreements see https://www.europol.europa.eu/partners-agreements/operational-agreements.

[36] These activities are also supported by the Cyber Intelligence Team (CIT), whose analysts collect and process cybercrime-related information from public, private and open sources and identify emerging threats and patterns. Working alongside EC3 is the Joint Cybercrime Action Taskforce (J-CAT), which works on the most important international cybercrime cases that affect EU Member States and their citizens.
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[37] Communication from the Commission to the Council and the European Parliament: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012DC0140&from=CS.

[38] See Council Decision, No. 2002/187/JHA, setting up Eurojust with a view to reinforcing the fight against serious crime. The European Judicial Network represents a network of national contact points for the facilitation of judicial cooperation. It assists with establishing direct contacts between competent authorities and by providing legal and practical information necessary to prepare a request for judicial cooperation. More information available at:https://www.ejn-crimjust.europa.eu/ejn/EJN_Home.aspx.

actions.[39] Yet, the need for operational effectiveness emerged over the time to provide assistance in urgent cases.[40]

The competence of the agency included fight against "computer crime" from the very beginning (Article 4 of the 2002 Council Decision) although by that time it was mainly connected with computer fraud (Annual Report 2002).[41] Nevertheless, very soon the agency encompassed in its structure a team responsible for cybercrime activities (Annual Report 2004). With cyberspace vast malignant opportunities on the rise, especially the sale of illicit goods over the Internet the legal difficulties caught the agency's attention, mainly in the field of relevant national legislation and different methods of combating cybercrime. As cybercrime has become more and more regular and sophisticated quickly spreading to other areas, affecting EU citizens non-discriminately, the agency focused on increasing the awareness of this criminality and continued to deal with the legal aspects of mutual assistance; the exchange of information, evidence gathering, coordination of joint actions in specific cases (Annual Report 2007, 2008).

Thus the agency has expanded its scope to face this challenge and when the era of crypto markets and cryptocurrencies has arrived within this decade, the agency already had an operational basis for initiating and developing cooperation with national authorities.[42] The agency's activities should facilitate legal assistance in order to become more effective to suppress cybercrime focusing primarily on faster exchange of information and enhancement of operational measures for the purpose of investigation and prosecution.[43] However, as the evaluation of the agency's activities going on, even more proactive steps might be coming to increase its operational attitude. On the other hand, as both EU agencies, Eurojust and Europol, continue to provide the assistance in coordination of investigations, their role in this field might be blurred over the time.

---

[39] Stefano Ruggeri: *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings.* Springer. 2013, p. 218-221. Solange Ghernaouti-Helie: *Cyber Power: Crime, Conflict and Security in Cyberspace*, EPFL Press. 2013, p. 283.

[40] For developments see Council Decision, No. 2009/426/JHA, on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime.

[41] As mentioned previously in Chapter 2, the European Arrest Warrant was adopted approximately at the same time and it also included computer-related crimes (see Article 2).

[42] One of the early examples of this successful cooperation includes operation Onymous (TOR Network) in 2014 directed at illegal cryptomarkets with Eurojust supporting public authorities throughout the action day. Seehttp://www.eurojust.europa.eu/press/PressReleases/pages/2014/2014-11-07.aspx.

[43] This corresponds with the European Agenda on Security, issued by the European Commission in 2015, COM(2015) 185 final. The priorities include terrorism, organised crime and cybercrime as interlinked areas with a strong cross-border dimension, specifically referring to the abuse of anonymisation techniques and anonymous payment mechanisms for illicit online trade. Seehttps://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

The agency has also set-up a Task Force on Cybercrime to enhance sharing of experience and expertise related to investigation and prosecution of cybercrime with its aim to cover the judicial dimension. It also supports the European Judicial Cybercrime Network, a group of specialised practitioners (such as prosecutors and judges). Its role is countering the challenges posed by cybercrime, following investigations and prosecutions, as well as the obstacles to effectively securing and gathering e-evidence.[44] It should enable the exchange of expertise and best practices related to the investigation and prosecution of cybercrime.

As for the tools available to the agency to achieve its goals, the agency may hold so-called coordination meetings to exchange information related to a specific investigation, to agree on a common strategy or plan joint activities. These meetings also provide platform for legal debates and they soon proved to be essential in the context of fight against cybercrime,[45] considering that the perpetrators and computer servers are usually situated in different countries. Therefore, the parallel investigations and prosecutions required common approach in order to clarify details and decide how to deal with specific ongoing cases including collection and preservation of (electronic) evidence and exchange of information (Annual Report 2009). To facilitate cooperation among involved states even further, joint investigation teams, so-called JITs, and coordination centres might be established (see below).

With these tools available, the Eurojust has been able to adapt to the era of cybercrime. In fact, it might be exactly this phenomena with electronic evidence difficult to collect, differences in national legislation related to criminalisation of certain cyberspace conduct, data retention, admissibility of evidence etc. that shows the agency's potential in its best. So far it has served as a successful platform for interstate cooperation and coordination to prevent legal discrepancies and operational difficulties hamper the real-time work of investigators and prosecutors especially in the field of evidence gathering and execution of simultaneous measures. On the other hand, the complexity of some cases and especially number of States involved may stretch the agency´s tools to the limits. In view of these developments, the potential of existing tools might be exhausted.

[44]Briere, Weyembergh*:* op. cit**.**
[45]ChloéBriere, Anne Weyembergh*: The Need Balances in EU Criminal Law: Past, Present and Future.* Hart Publishing. 2018, p. 346 - 350.

2.3. Joint Investigation Teams

Idea of close cooperation and shared cross-border investigation in criminal cases is expressed by a so-called "JIT" (Joint Investigation Team). The JIT focuses on operational cooperation in parallel investigations. It may be set up on ad hoc basis depending on the suitability of the individual case and it comprises of judicial and police representatives drafting agreement for a specific purpose (evidence-gathering, sharing of information, identification of suspects and confiscation of the criminal assets) leading to a common action day. This makes JITs a suitable tool for cooperation related to cybercrime vested with certain powers but without unnecessary prolonged procedures connected with bilateral legal assistance. For example according to the Czech law, under the Section 72 of the Act no. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters, evidence gathered by the JIT might be used for the purposes of criminal proceedings provided that the evidence is obtained in accordance with law.

Within the EU, JITs are commonly used by Eurojust in cases when for example differences in criminal procedure appear between states; authorities provide documentation to satisfy individual national evidentiary requirements. Eurojust may also provide JITs with logistical equipment, operational analysis etc.[46] What is more important, Europol and Eurojust may participate together in the establishment of such teams at the request of a Member State.[47] JITs may also be set up with Third States, on a judicial basis such as the 2001 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of the CoE or the 2009 Agreement on mutual legal assistance between the EU and the US (see Catelan, Cimamonti and Perrier (dir.), 2014). JITs might be viewed as an act of trying to standardize the cooperation.

For making simultaneous decisions especially at the last minute the coordination centres provide real-time exchange of information, the joint execution of judicial measures (such as seizures, arrests, witness interviews, freezing orders etc.) in order to ensure that measures are made in a timely and arranged fashion and implemented as soon as possible. The goal is not to jeopardize less advanced investigation in one country while taking measures in the other

[46]See Joint Investigation Teams Practical Guide prepared by the JITs Network. 2017, available at:http://www.eurojust.europa.eu/doclibrary/JITs/JITs%20framework/JITs%20Practical%20Guide/JIT-GUIDE-2017-EN.pdf. The support during coordinated actions is usually provided in close cooperation with Europol, focusing on on-the-spot support and working with a team of investigators.

[47]Article 6 of the 2009 Agreement between Europol and Eurojust and art.6 of the consolidated Eurojust Council Decision.

with its investigation ready for a rapid action. In other words, to plan, monitor and provide national authorities with a successful action day schedule.

3. Cooperation and private sector

As described in previous chapters, combating crypto markets requires effective interstate and institutional cooperation that facilitates criminal investigation conducted by public authorities. However, due to sophisticated nature of cybercrime, this cooperation cannot be limited to public sector only.[48] Public authorities usually do not have access to private data or into the private networks founded and operated by private sector. On the other hand, the aim of private sector is not to suppress cybercrime, nor eliminate the existence of crypto markets. Furthermore, the private sector lacks access to intelligence information collected by public authorities and powers invested with them by law.

Thus while combating cybercrime and crypto markets mutual assistance with private sector cannot be omitted. It may provide both sides with useful tips or information, early warnings, best practices or even vital evidence.[49] All of these in order to eliminate crypto markets and prosecute those who create and administer them. However, as one of the essential problems with crypto markets is that once the market is down the users move to another, the cooperation should not be formed on an ad hoc basis but held on durable terms. Unfortunately, more arrests, takedowns and publicity increase awareness of investigative techniques at the same time.[50] Even though, from a strategic point of view, this cooperation and especially its outcome may be profitable for both sectors.

Yet, it should be also considered that the private sector and especially private companies are based on different principles and governed by different culture. Their goal is not to pursue public security but usually self-interest (for example a profit). They are responsible to their shareholders and concerned with mutual competition and privacy of their customers. Also, the reputational damage cannot be forgotten. In other words, the instinct of self-preservation and

[48] The call for the private sector involvement has been part of the agenda from the very beginning. See for example UN General Assembly Resolutions 55/63 and 56/121 *Combating the criminal misuse of information technologies* or the Convention on Cybercrime.
[49] Jody R. Westby: *International Guide to Combating Cybercrime*, ABA Publishing. 2003, p. 171.
[50] Lillian Ablon, Martin C. Libicky, Andrea A. Golay: *Markets for Cybercrime Tools and Stolen Data: Hackers´ Bazaar*, Rand Corporation. 2014, p. 17 accompanied with several examples.

lack of trust rather than that of cooperation may have the upper hand for private sector.[51] It may simply not be willing to yield to criminal investigation.

This leads to serious questions, what should be the foundation of this cooperation to minimize its negative impact? Should it be voluntary or legally imposed, informal or formal? Any effective cooperation will probably require all of these to maximize participation but at the same time respect interest and hidden agendas of both sectors. Thus fluctuation of personnel between public and private sectors (for example former law enforcement personnel working for private companies) may typically facilitate informal cooperation based on friendly or expert relations. This might be accompanied by the existence of hotlines, security expert meetings, educational programmes, conferences, etc.[52]At the same time, the development of comprehensive cybercrime policy supported by traditional as well as cybercrime oriented legislation is necessary.[53] Therefore, in some cases, private sector might be under a legal obligation to provide cooperation. With respect to the rule of law, formal and legally mandated procedures are especially required in the field of gathering and preservation of evidence. We may conclude that to strengthen and speed up the cooperation, unified legal framework is inevitable.

[51] Abraham D. Sofaer, Seymour E. Goodman: *Cyber Crime and Security. The Transnational Dimension* in The Transnational Dimension of Cyber Crime and Terrorism. Hoover Press. 2001.
[52] Westby, p. 176-177. Op cit. For specific forms of cooperation and examples see for example Tatiana Tropina, Cormac Callanan: *Self-and Co-operation in CyberCrime, Cybersecurity and National Security*, SpringerBrief. 2015.
[53] Marco Gercke: *Understanding cybercrime: phenomena, challenges and legal response*. ITU. 2012. p. 97. For the European Union cybercrime policy see for example *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 2013*, European Commission, Brussels, JOIN(2013) 1 final.

Conclusion

Since the beginning of the millennium the proliferation of cybercrime has highlighted the need for cooperation related to criminal matters. With the existence of crypto markets involving anonymous transactions and the use of cryptocurrencies the scope of this cooperation has to be moved even further.

The legal basis of the current cooperation derives from various instruments with different impact. The most important international legal framework for combating cybercrime is covered by the Convention on Cybercrime as presented in Chapter 1.2., which represents assumption of responsibility on the international level. Even though it has supplementary role to already existing instruments, we believe that it has several benefits including the accent of the need to cooperate on the widest possible extent, enabling harmonization of the key cybercrimes, network of 24/7 contact points, easier gathering of evidence, providing legal information and locating suspects. The advantages of the Convention are also the involvement of states across continents in the debates about safe cyberspace, the pressure on states to amend their legal provisions related to cybercrimes, to improve technical cooperation on international level and to adopt new procedural institutes. However, more states would have to sign and ratify the Convention to fully reach its objectives. At the same time, some states found problematic, that the Convention was adopted on the grounds of the Council of Europe not the United Nations and that they were not participating in preparation of the coherent text.

The jurisdiction and legal discrepancies are still the main factors that challenge the law enforcement authorities to be able to successfully gather enough evidence and prosecute the perpetrator of a cybercrime. The patchwork of separate, territorially defined national jurisdictions causes difficulties in determining the applicable law in transnational interactions and gives rise to legal uncertainty, thereby preventing cooperation across borders, which is necessary to deal efficiently with cybercrime. Thus the considerable number of cybercrimes still remains unpunished. There is an ongoing need to develop shared procedural standards which can determine the territorial factors that provide grounds for the applicable law in cyberspace, and to define investigative measures which can be used regardless of geographic borders.[54] However, the improvement of international police and judicial cooperation and reduction of delays in cross-border requests would improve the number of resolved cases. In this regard, the work of agencies within the EU dealing with cooperation related to

[54]Report of the European Parliament of 26 July 2017 on the fight against cybercrime (2017/2068(INI)).

cybercrime on a regular basis and means they provide not only proves that the cooperation is possible on a horizontal (interstate) and vertical levels but also that this might be the way how to efficiently deal with complex cybercrimes including illicit trading enabled by crypto markets. Since cryptomarkets are global threat, the response must be also transnational. The typical example of this cooperation is the use of JITs overcoming obstacles related national legislature.

The cooperation between public and private sector and various forms of this cooperation represent another challenge. Yet the involvement of private sector seems to be inevitable. This includes not only informal ad hoc cooperation to eliminate single crypto markets but also legal obligations especially for strict regulation of crypto currencies and probably for retention of data. However, after initial steps, the shape of this regulation is still being debated within the EU, although recent law enforcement operations shown that crypto markets are still on the rise.

However, as there is no definite answer what is the appropriate way for successful suppression of the cryptomarkets at this moment, we may conclude that the use of all advantages of multilevel international cooperation through different instruments and institutions, and sharing best practices worldwide, should lead to effective fight against the cryptomarkets.

Sources

Lillian Ablon, Martin C. Libicky, Andrea A. Golay: *Markets for Cybercrime Tools and Stolen Data:Hackers´ Bazaar*, Rand Corporation. 2014. ISBN 978-0-83308-574-0

Chloé Briere, Anne Weyembergh*: The Need Balances in EU Criminal Law: Past, Present and Future*. Hart Publishing. 2018. ISBN 978-1-50991-700-6

Marco Gercke: *Understanding cybercrime: phenomena, challenges and legal response*. ITU. 2012

Solange Ghernaouti-Helie: *Cyber Power: Crime, Conflict and Security in Cyberspace*, EPFL Press. 2013. ISBN 978-1-4665-7304-8

Stefano Ruggeri: *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*. Springer. 2013. ISBN 978-3-642-32011-8

Tatiana Tropina, Cormac Callanan: *Self-and Co-operation in CyberCrime, Cybersecurity and National Security*, SpringerBrief. 2015. ISBN 978-3-319-16447-2

Abraham D. Sofaer, Seymour E. Goodman: *Cyber Crime and Security. The Transnational Dimension* in The Transnational Dimension of Cyber Crime and Terrorism. Hoover Press. 2001. ISBN: 0-8179-9982-5

Jody R. Westby: *International Guide to Combating Cybercrime*, ABA Publishing. 2003. ISBN 1-59031-195-7

Kolouch, Jan. *CyberCrime*. Praha:CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

GŘIVNA, Tomáš and POLČÁK, Radim ed. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-809-0378-674

https://rm.coe.int/16802f69c3 (The effectiveness of international cooperation against cybercrime: examples of good practice by Pedro Verdelho)

https://www.deepdotweb.com

https://academy.bitcoin.com

https://www.coe.int

https://data.consilium.europa.eu

https://europol.europa.eu

https://eur-lex.europa.eu

https://ejn.crimjust.europa.eu

https://eurojust.europa.eu

https://ec.europa.eu

Cover photo: https://www.ndtv.com