The organised criminal phenomenon on the Internet[1]

DR. HABIL. Zoltán András NAGY
Associate professor
University of Pécs, Faculty of Law
Department of Criminal Law

DR. Kitti Mezei
Ph.D. student
University of Pécs, Faculty of Law
Department of Criminal Law

Abstract

The use of Internet offers wide range of available features for cybercriminals which are exploited by them such as anonymization, encryption and virtual currencies, creating constant challenges for law enforcement. Cybercrime is getting more sophisticated and increasing in scale and impact. Cybercrime has also become a big profit-driven illegal and service-based industry and created the Crime-as-a-Service business model. It lured even the traditional mafia-style criminal organizations into the cyberspace since they are able to expand and transfer their offline activities.
The present paper analyses the followings:
- *the organised criminal characteristics with general aspects*
- *criminal communication and networking*
- *DoS, DoSS – attack with extortion*
- *unlawful gambling operations*
- *child pornography as a business opportunity*
- *online money laundering.*

Keywords: *organised crime, cybercrime, DoSS attack, unlawful gambling operations, child pornography, online money laundering.*

1. The organised criminal characteristics with general aspects

The disadvantage of the technology development is that the criminals may exploit and take advantage of the modern technology for their own criminal acts.[2]

First of all, the present paper examines criminal networks in cyberspace. Cybercrime has become a big profit-driven illegal and service-based industry. It has developed the Crime-as-a-Service business model which provides a wide range of services such as rental botnets, denial-of-service attacks, malware development. It has

[1] The present paper is part of a project, namely the program for raising the quality of legal education and research, supported by the Hungarian Ministry of Justice. [Jelen tanulmány az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programjai keretében valósult meg.]

[2] Papp, P., Hi-tech bűnözés napjainkban [High tech crime in our days]. Belügyi Szemle 52. 2001/11-12. p. 5.

also lured traditional organised crime groups into cybercrime areas since it offers high financial gain with low risk. Cybercriminal groups lack the structure and hierarchy of a traditional organised crime group.[3] "The most common view on the structure of organised criminal groups is that they represent flexible network formed by high-skillet, multi-faceted cybercriminals."[4] They plan, organize and commit numerous cybercrimes and set up online criminal networks which operate on a "stand alone" basis. Their members rarely meet or keep physical contact in person with one another, only meeting online. The organization is run by its core members.[5]

Cybercriminals started to adapt legitimate business models and imitate the operations of big companies such as eBay, Yahoo, Google and Amazon. They provide the most value for their consumers, who are not the victims, but the criminals using the tools to commit different crimes.[6]

McGuire has suggested a typology of cybercrime groups, which has six types of group structure with three main groups.[7] The first group operates fundamentally online and assessed via reputation in their online activities. It can be divided into two types firstly, there are the swarms, which are large collectives, disorganised organizations without leadership, typically consisting of ephemeral clusters of individuals, active in ideologically driven online activities such as hate crimes and political resistance (e.g. Anonymous has a swarm). Secondly, there are the so-called hubs, which are more organised with a clear, central command structure and diverse online activities from botnets to online sexual offences. The second type of group is called "hybrid" since it combines both online and offline activities. There are also two types within the hybrid one: the clustered hybrid, which operates as a small group and focuses on specific activities or methods and the extended hybrid, which is similar, but a lot less centralized. The third type of group operates mainly offline but take advantage of technology development to improve their offline activities. It can be subdivided into hierarchies, which are the traditional criminal groups, mafia crime families who continue their activities online such as pornography, online gambling, extortion and aggregates, which are loosely organised, temporary groups without a clear purpose sometimes, their operation is ad hoc.[8]

We chose the title carefully, since the paper analyses the problem more widely rather than only focusing on the Hungarian Criminal Code's concept of criminal organization.[9] We also deal with organised crime related acts which have some organised criminal characteristics.[10] Complex illicit operations, cybercrime infrastructure, the level of

[3] EUROPOL – Internet Organised Crime Threat Assesment (IOCTA) 2014. p 9.

[4] Tropina, T., The evolving structure of online criminality: how cybercrime is getting organised. eucrim 4/2012 p. 162.

[5] http://www.unicri.it/special_topics/securing_cyberspace/cyber_threats/explanations/ (accessed: 12.11.2016)

[6] Tropina, T., op. cit. p. 158.

[7] McGuire, M., Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security.

[8] Broadhurst R. – Grabosky P. - Alazab M. – Chon S., Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology. Vol 8 Issue 1 January - June 2014. p. 5-7.

[9] According to the Hungarian Act C of 2012 on the Criminal Code: 'criminal organization' shall mean when a group of three or more persons collaborate in the long term to deliberately engage in an organised fashion in criminal acts, which are punishable with five years of imprisonment or more.

[10] Korinek, L., Kriminológia II [Criminology II]. Budapest, 2009. p. 338-339.

specialization through division of labour show the characteristics of organised cybercriminal activities in order to gain financial or other material benefits.[11] The following characteristics can be recognized in the online environment:

a) Committing a single crime is not a lucrative investment:

- Legitimate and relatively bureaucratic actions are required: domain name requisition, web hosting rental, later on establishment of foundation for money laundering, application for different permits which allow them to do legal, but cover activities such as online gambling.

- It also requires financial investments: the expense of Internet access and web hosting rental, the fee for making the website, the price of the programme for website mirroring or covering their TC/IP number.

b) Division of labour[12] is also necessary as it appears typically in case of crimes committed by criminal groups. The division of labour between its members and their activity in criminal organization generally is aimed to maximize profit.[13] In case of organised cybercriminal organizations, the increasing specialization of perpetrators is typical and the tasks are divided amongst its members.[14] The knowledge of information technology is manifold so as the expertise and designated role of the cybercriminal group members, though some tasks might be outsourced:

- Coders or programmers write the malware, other software tools and design or upload a website to commit the cybercrime. As regard designing a website, there are many websites which make available templates free of charge or for money. These templates are simple and meet basic requirements, although specialized technical knowledge is needed to create more complex ones. The legitimate business associations may also design or upload websites, even provide web hosting services. If the cover-up activities are legal (foundation, online gambling, sale of used belongings etc.) then they can make and upload the websites without consequences. Although they must be aware of that if these activities or contents (pornography, pedophilia, drug distribution, illegal gambling etc.) are considered to be illicit then they may become perpetrator or accomplice by uploading the website. The criminals generally do these for themselves.

- Distributors or vendors trade and sell stolen data or illicit goods.

- Technicians maintain the infrastructure and technologies such as serves, ISPs and encryption. The server provider for the Internet access and the contracting party with the web hosting service provider who rents it are two different people generally. The Internet access: through legitimate service provider or through web hosting service. After this they might use tricks to hide the subscriber or his/her computer (server): For example, when the server crosses the Hungarian border (or overseas). It raises some jurisdiction related questions. It is possible that the server is in Hungary, but its content

---

[11] Nato, J., Cybercrime, Organized Crime and Societal Responses. Emilio C. Viano (editor). p. 186.

[12] The developed division of labour can be recognized in case of other crimes. See: Réka Gyaraki, Az on-line elkövetett szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye. [Online infringement of copyright and certain right related to copyright]. Infokommunikáció és jog. 41. 2010/6. p. 220.

[13] Balogh, Á., The definition of criminal organization and consequences of committing crime in the framework of a criminal organization under Hungarian criminal law. Law Series of the Annals of the West University of Timisoara 2015. p. 17.

[14] Tropina, T., op. cip., p. 158.

http://www.unicri.it/special_topics/securing_cyberspace/cyber_threats/explanations/ (accessed: 12.11.2016)

is mirrored to another country's website. Mirroring is not a complex activity, though it requires some practice.[15]

Anonim or public proxy servers can be used to hide the real servers. These „pirate servers" could play a role in some activities and they are not able to provide continuous cover. In particular, there is the distorting proxy which can be tricky since it shows a fake IP address for the host server.

Proxy chaining, proxy to proxy, for examples makes possible for us to appear in one of the Caribbean Islands. Its efficiency can be deadened by the decrease of bandwidth but it can offer a continuous website availability.

- Cashers control drop accounts and provide those names and accounts to other criminals for a fee also they manage "money mules". Money mules are used to transport and launder stolen money or merchandise. Tellers assist in transferring and laundering money through digital currency services and between different national currencies.

- Executives select the potential victims and recruit members also assign members to the above tasks, they are charge of the management of the organization.[16]

c) The cybercrimes are deemed to be committed on a commercial scale since the cybercriminals are engaged in criminal activities of the same or similar character to generate profits on a regular basis. The profit might be gained by selling illegal contents or services, or using extortion with DoS or DDoS attack. Cybercrime industry intends to meet forbidden needs for.[17] As Mihály Tóth stated about the notion of criminal organization is "continuous, business-like criminal conspiracy"[18] which is also suitable for the modern cybercrime industry.

The following topics are discussed in detail: criminal communication and networking, DoS and DDoS attacks – extortion, unlawful gambling operations, child pornography and online money laundering.

2. Criminal communication and networking

The organised criminal groups might use networks for communication. The hacker legend Kevin Mitnick[19] presents a case in his book: when an unknown person persuaded a boaster young man to get the student database of the Chinese engineering university, then obtain the description of the Boeings' safety technology systems from Lockheed Martin, which means basically he made him to hack these information systems for these documents and after the assignment the principal has become unavailable. The young hacker has realized what he has done after only he heard about the Indian hijacked Boeing. The police of the United States of America found the connection between the

[15] The most popular mirroring applications are the followings: Teleport Pro, Wget, WebWhacker or Webcopier. The cybercriminals prefer the registry free ones.

[16] Broadhurst R. – Grabosky P. - Alazab A. – Chon S., op. cit. p. 7.

[17] Tóth D. – Gál I. – Kőhalmi L. – Organized crime in Hungary. Journal of Eastern-European Criminal Law. 2015. p. 43.

[18] Tóth, M., A bűnszervezet környéke. [The environs of the criminal organization] Jogtudományi Közlöny 1997,12., p. 507.

[19] Mitnick, K. (1963-) spent 5 years in prison due to different committed cybercrimes. He hacked the most well-known and protected IT networks and gained thousand of clients' data. Today he has his own IT security venture with significant references. He published two books: „The art of deception" (Perfect, 2003) and „The art of intrusion" (Perfekt, 2006).

hijacking and the hacker's activity so they caught him.[20] This method is suitable for recruitment of people with specialized expertise. Web-based chatrooms and open forums or forums within the deep web or Darknet are ideal places for the communication. The most popular English speaking criminal forum the Darkode was taken down by law enforcement in 2015 and there is no any notable replacement so far. Two type of communications can be distinguished in relation to criminal communications: criminal-to-criminal (C2C) and criminal-to-victim (C2V). For C2C communication is the key the security and anonymisation while for C2V communications is accessibility, the ability to contact more easily the potential or targeted victims for example in this case e-mail is the simplest way and beyond that applications are widely used such as Skype, Facebook Messenger, WhatsApp and Viber which can be used for sending spam, social engineering, phishing etc.[21]

3. DoS, DDos – attack with extortion

The organised crime use capable opportunities for destructive attacks.[22] Instead of viruses, malwares which might cause serious damages in databases and software or a website defacement, firstly we focus on a modern crime, the extortion on the information technology networks. It is not a new phenomenon because in the early '90s Lewis Popp already sent infected discs with virus about the medical development of curing AIDS and it activated itself after 90 days unless the unsuspecting user bought an antivirus disc for money.[23] An increasingly popular motivation for DDoS attack is extortion, by which a cybercriminal demands money in exchange for stopping or not carrying out the attack.

During troubleshooting they send some short packets (ping) to check the connection for the host computer which has to respond to it. They use this technical solution in case of so-called denial of service or distributed denial of service attacks (DoS or DDoS). The attacked system receives a larger volume of data packet and it cannot respond to them, which means generally sending packets as fast as possible without waiting for replies. The server is overloaded and waits for the client computer's confirmative respond in vain. The differences between DoS and DDoS are substantive. In a DoS attack, a perpetrator uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests. The aim of the assault typically is to exhaust server resources (e.g., RAM and CPU). On the other hand, DDoS attacks are different since it is launched from multiple connected devices that are distributed across the Internet. These connected devices are the so-called zombie computers activated by a software to send packets. Users usually don't know that their computers are infected with a malicious software and serve criminal networks. Perpetrators use software tools

---

[20] Mitnick K. – Simon W., A behatolás művészete [The art of intrusion]. Perfekt kiadó. Budapest, 2006. p. 27-59.

[21] EUROPOL – Internet Organised Crime Threat Assesment (IOCTA) 2016. p. 45-46.

[22] Mezei, N., Digitalizált bűnözés – digitalizált védelem. [Digitized crime – digitized protection]. Rendészeti Szemle, 57. 2009. p. 40-45.

Sebők, J. A harmadik világháború (Mítosz vagy realitás) [The third World War (Myth or reality)]. Budapest, Népszabadság könyvek, 2007. p. 88-93

[23] Nagy, Z., Bűncselekmények számítógépes környezetben [Crimes in the IT envrionment]. Budapest, Ad-Librum, 2009. p. 257.

for automate attacks[24], which can be preinstalled or downloaded, unpacked (games, other programmes from websites, torrents etc.) by users. Unlike single-source DoS attacks, DDoS assaults tend to target the network infrastructure in an attempt to overwhelm it with huge volumes of traffic. Secondly, DDoS attacks also differ in the manner of their execution. DoS attacks are launched using homebrewed scripts or DoS tools (e.g., Low Orbit Ion Canon), while DDoS attacks are launched from botnets, large clusters of connected devices (e.g., cellphones, PCs or routers) infected with malware that allows remote control by an attacker. The botnet makes possible to launch large-scale attacks on the less protected private (with easily obtainable personal data or sensitive information) or corporate systems with high-levelled protection by sending spam or disseminating malware.[25] This botmaster controls the botnet remotely, often through intermediate devices known as the command and control (C&C;, or C2) servers. To communicate with a server, the botmaster uses various hidden channels, including IRC and HTTP websites, as well as popular social networks like Twitter, Facebook and even Reddit. Botnet servers are able to communicate and cooperate with other botnet servers, effectively creating a P2P network controlled by a single or multiple botmasters. Botnets-for-hire are widely available, they are often being auctioned and traded among attackers in the underground economy using online marketplaces which are hard to be tracked down. Botnets can be rented and used for DDoS or other attacks. These platforms, often hiding behind the ambiguous service definition of stressers, or booters, sell DDoS-as-a-service. They provide their clients with a toolkit, as well as a distribution network, so as to execute their attacks on call.[26]

The European Union has realized the fact that botnets pose a higher level of threat to the Member States in the public and private sector too. The Directive 2013/40/EU on attacks against information systems[27] has come force in 2013. It aims to introduce criminal penalties for the creation of botnets and also encourages the Member States to use more severe penalties and make available as aggravating circumstances where an attack against an information system is committed by a criminal organisation or conducted against a critical infrastructure of the Member States. It also sets up measures against identity theft and other identity-related crimes. The above mentioned elements from the Directive are missing for example from the Hungarian Criminal Code.

There are an increasing number of cases when DDoS attacks are designed to keep a business competitor from participating in a significant event (e.g., Cyber Monday), while others are used for shutting down business websites for a long time. The target is well considered and chosen. The offenders often choose websites whose operation demand continuous and undisturbed conditions (e.g. online casino websites). For example, Europol arrested of key members of the extortionist DD4BC hacking group that blackmailed multiple European companies (e.g. an online gambling company, PokerStars was confirmed as a victim) with DDoS attacks in exchange for Bitcoin payments. The group launched small DDoS attacks against companies and then asked for a ransom in Bitcoin to prevent further assaults. If the victim declined to pay, the

[24] Gercke, M., Understanding cybercrime: phenome, challenges and legal response. ITU 2012. p. 17.

[25] Tropina, T., op. cit. p. 161.

[26] https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html (accessed: 18.11.2016)

[27] According to the Directive 2013/40/EU: 'information system' means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.

group would then launch more powerful attacks in the following days. The extortion scheme has become a regular practice these days and there are many copycat groups who follow this lead.[28] The conventional crimes against property – such as extortion - can be committed with the help of modern technology solutions too.

4. Unlawful gambling operations

Unauthorized gambling activities are typically planned to run in the long term. The organised groups earn tax-free revenues. It has always attracted those who want to avoid their taxation and other obligations.[29]

The different kind of gambling games (poker, slot-games, blackjack, baccarat, craps and other games) and betting websites has become widespread and fastest-growing areas in the Internet. The poker has become popular thank to the broadcasted tournaments by sport channels, poker websites and online casinos' advertisements. The online casinos are widely available and hosted in countries with liberal laws or no regulations on online gambling. Their popularity can be explained by the higher odds and tax-free prizes (no game tax or income tax). Most of the them just as well legitimate or illegal ones offer free demo games which help the users to get acquainted with the casino. They can open accounts, transfer money and play games of chance. Although the players must be aware of that the payment might be uncertain in case of unlawful operations. Online casinos can be used in money laundering and activities financing terrorism. There are players who are supposed to be insiders and they play to lose and pay in only. Online role playing games are also used to launder money, especially massively multiplayer online role playing games (such as Second Life and World of Warcraft) provide an easy way since these games use credits that players can exchange for real money.[30]

Gambling operations are considered to be unlawful due to the fact that the organizer has no right to run the operation. Gambling activities generally belong to the state monopoly. It can be transferred to others with a concession agreement, though the authorized cannot assign to other people. According to the Hungarian Criminal Code unlawful gambling operation can be determined if it is orientated to gain profit on a regular basis id est several or indefinite number of games in advance and the elapsed time is rather short between the games. In the case of Internet gambling's key factor is the regularity owing to the refunded investments and financial enrichment. Organizing the game, maintaining the website, handling or accepting the stakes, paying out the prizes are all considered to be perpetrator's conduct. It is also unlawful operation when the authorized person is entitled to organize the legal gambling but he/she would exceed his/her authority. It is indifferent whether it gives financial benefit as a result in the end. Offering the server is determined as an accomplice's behaviour and it is irrelevant whether it is free or it is for a valuable consideration.

---

[28] https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629 (accessed: 21.11.2016)

http://news.softpedia.com/news/members-of-dd4bc-the-group-that-blackmailed-companies-with-ddos-attacks-arrested-by-europol-498797.shtml (accessed: 21.11.2016)

[29] Farkas I. – Jávorszky J., Az illegális pénznyerő-automaták felderítése [The investigation of illegal gambling machines]. Rendészeti Szemle, XXXI. évfolyam 1993.5. p. 58-59.

[30] Jean-Loup Richet, Laundering money online: a review of cybercriminals methods. p. 12.

5. Child pornography as a business opportunity

Organised criminal networks play a significant role in child sexual exploitation, including commercial and online sexual activity. The users thank to the anonymization and encryption are able to follow their dark sexual desires on the Internet. Pedophiles have a deviant sexual tendency and their sexual urges are not accepted by the public, thus they do their culpable activities in secret. We examine child pornography thoroughly in this paper. Child pornography is "any material that visually depicts a child engaged in real or simulated sexually explicit conduct; any depiction of the sexual organs of a child for primarily sexual purposes; any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes".[31]

Since Internet has become widespread it has a substantial damaging drawback: it is used as a platform for child sex offenders to communicate, store and exchange child sexual exploitation material (CSEM) and made easily for them to hunt for new victims. There are two types of sexual coercion and extortion online: content driven, for sexual purposes, and financially driven, for commercial purposes. It means typically grooming[32] the child or impersonating another in order to gain their trust. The sexual predators use different platforms such as social networks, online games, forums and chats where the sexting begins which is part of the grooming process.[33] This activity can lead to the sexual extortion of children by asking self-generated photo or video of a sexual nature and involves a process whereby they are coerced into continuing to produce sexual materials or told to perform sexual acts under threat of disclose or send to others like directly to family, friends etc. There are an increasing number of more extreme, sadistic, and degrading demands by the perpetrators.[34] The self-generated images might give further challenge since in some jurisdictions it is considered that the minor who generated and distributed it is guilty of producing and disseminating CSEM.

The most common method to exchange child abuse material (CAM) is still Peer-to-Peer (P2P) platforms, but they started to use more sophisticated ones for distribution, such as the Darknet. The use of Darknet is getting more popular among perpetrators using hidden services on platforms like TOR. These platforms facilitate untraceable CSEM by allowing sharing of images anonymously through websites, private messages and email. The another growing area is the live streaming of child sexual abuse which poses a particular challenge for law enforcement. It also supports the so-called hands-on

---

[31] According to Article 2 (c) of the Directive 2011/92/EU of the European Parliament and the Council on combating the sexual abuse and sexual exploitation of children and child pornography

[32] According to the Interagency Working Group on Sexual Exploitation of Children: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Adopted by the Interagency Working Group in Luxembourg, 28 January 2016) p. 51. „In the context of child sexual exploitation and sexual abuse, "grooming" is the short name for the solicitation of children for sexual purposes. "Grooming/online grooming" refers to the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person."

[33] IOCTA 2016. op. cit. p. 24.

[34] Interagency Working Group on Sexual Exploitation of Children p. 51.

offending which means after the live stream the soliciting offender travels to the place for purpose of child exploitation. The Internet and new technologies revives online and offline child sex tourism, it can be arranged easily with low risks and offers profitable services overseas. It is an attractive proposition to earn easy money with the crime of abuse via live streaming. These are paid services and the payment is generally made through international money transfer and, less frequently, via local money transfers.[35] The organised crime represents itself on the cyberspace in the followings:

- commercial sexual exploitation of children online;
- obtaining credit card information and get money with them;
- blackmailing clients with their "sex adventure" in order to gain financial benefits.

In our troubled world it is typical that individuals turn to perversions and the information systems offer a suitable platform for this. The organised crime is based on this demand. The tolerance against extreme contents drives the supply to serve the interested potential clients with more marginal contents.[36]

The most endangered injured parties are children who are under the age of 18 years and entitled to special protection, whether they are acting in the online environment or offline.[37]

In the EU the online content regulation related issues are part of the Member States' jurisdiction (e.g. Germany, the UK and Hungary adapted Internet blocking), except child pornography.[38] There are some well-meaning, binding international documents with clear contents[39] in this field, though there is a tendency for further dynamic spread of child pornography due to new technology developments. The virtual reality (VR) devices make a good example by their consumer release in 2016. It is possible that such devices could be used to simulate abuse on a virtual child or view CSEM since VR pornography industry is already established in Asia which means this development could be adopted easily for this disturbing purpose as well.[40] Cloud computing is also challenging since files are stored in a shared pool of computer resources on the Internet, it makes them accessible from any computer and the storage is maintained by the cloud server without a need for installing anything. The cloud system makes possible for the users to share their access and files with other designating users. It has been already recognized that perpetrators use cloud for possession and distribution of CSEM.[41]

---

[35] IOCTA 2014. op. cit. p. 28-34.

[36] Parti, K., Gyermekpornográfia az interneten [Child ponography ont he Internet]. Bíbor Kiadó, Miskolc, 2009. p. 48.

[37] Interagency Working Group on Sexual Exploitation of Children p. 11.

[38] Dornfeld, L., A virtuális tér geopolitikája. In: Dornfeld L. – Keleti A. – Barsy M. – Kilin J. – Berki G. – Pintér I. 2016/1. szám p. 63.

[39] International conventions:

- United Nation Convention on the Rights of the Child
- Optional Protocol of the Convention on the rights of the child
- Cybercrime convention
- Lanzarote convention
- Framework Decision 2004/68/JHA
- European Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography

[40] IOCTA 2016. op. cit. p. 27.

[41] Rogers, A., From peer-to-peer networks to cloud computing: how technology is redefining child pornography laws p. 22.

The Hungarian Criminal Code under Section 204 subjects to punishment obtaining or having in possession, producing, offering, supplying or making available, distributing, dealing with or making pornographic images of an under aged person or persons.

6. Online money laundering

Eventually the aim is to monetise the obtained, crime-related assets in the legitimate economy. Money laundering is not tied solely to organised crime, but it is an essential part, providing the organised operations, economic background and making the offenders wealthy. Laundering the illegally gained money has industrial scale nowadays.[42] It is a global phenomenon and Internet contributes to offer a wide range of different money laundering methods.

The phases of money laundering in real world can be recognized in the virtual space too. Anonimity is enough for some service requisitions which means a fake name and address is able to hide the real user. Furthermore, most of the financial transactions can be carried out anywhere and anytime. It is supported by the bank sector's interest, on the one hand, the banks help the cash flow with flexible regulations, technical background, client friendly ways, on the other hand, the banks charge the clients with different fees during the transactions which make them interested.

Money laundering involves three distinct stages which are recognizable in its cyber form too since criminals transfer and circulate funds within the digital economy.[43] The first phase is the so-called placement when cash moved from its source like in the following examples:

Onetime or frequent transactions to another individual, organization or foundation and the legal grounds of the transactions are indifferent and might be anything like based on charity, personal reasons or simple sympathy.

In case of legal or illegal gambling when the insider gamer loses all the time.

In the above mentioned cases the offenders may pay or transfer money also in a legal way, but then the money may go directly to terrorist groups or other organised criminal organizations. The legal literature calls this phenomenon as inverse money laundering.[44]

The fraudulent online auction activity is also serve as a suitable mean of money laundering. The auction is supposed to be fraudulent if:

- selling obtained goods which originate from crime commission (dealing in stolen goods), or

- after transferring the money there are no movement of the goods or service fulfilment. There is an opportunity to shorten the auction with accepting the pre-set highest automate bid.

The second stage is the layering. The primary purpose of this stage is to separate the illicit money from its source. The criminals use sophisticated layering of financial transactions that hide and make difficult to find the link between the money and the

---

[42] Bardócz, Cs., Pénzmosási technikák [Money laundering techniques]. Belügyi Szemle XXX. évfolyam, 1997. p. 74.

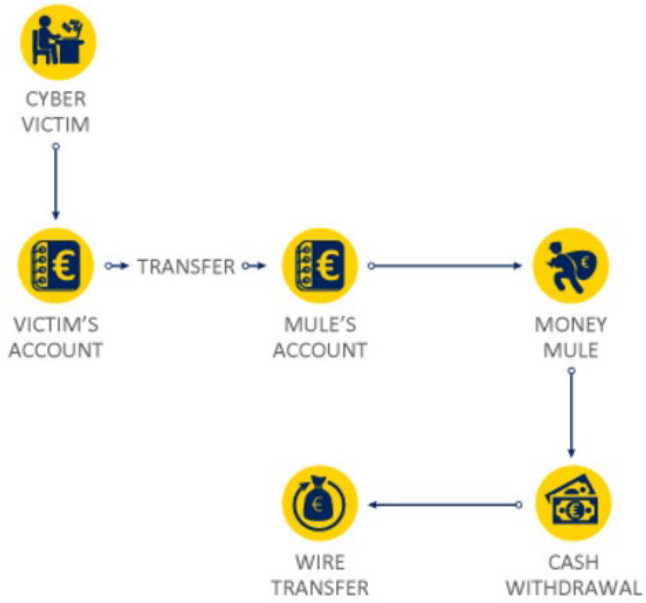
[43] IOCTA (2016), op. cit. p. 43.

[44] Gál, I. L., A pénzmosás és terrorizmus finanszírozása. [Money Laundering and financing terrorism] In: László Korinek – László Kőhalmi – Csongor Herke (editors). Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára. PTE ÁJK Pécs, 2004. p. 39.

original crime. Generally, the „dirty" money land in businesses, banks or it is placed in securities and finally the multiple transactions are untraceable for the law enforcement.

In the final third integration stage the money, which is layered through a number of financial transactions therefore it seems like resulting from a legitimate source, is fully integrated into the financial system and can be used for any purpose.

Most organised crime shares a common denominator which is the financial motive. Organised crime groups boost their assets and then inject them into the legal economy through different money laundering schemes.[45] The following figure shows an online money laundering scheme:



1. Figure: Example for an online money laundering scheme (source: EUROPOL)

Law enforcement traces the assets likewise the criminal networks. The investigation of money mule networks is a top priority both the law enforcement and the financial sector and in order to track them down they cooperate with each other (e.g. European Money Mule Actions). According to IOCTA „money mules are individuals recruited, often by criminal organisations, to receive and transfer illegally obtained money between bank accounts and/or countries. The recruited individuals may be willing participants, however some may, initially at least, be unaware that they are engaging in criminal activity and believe they are performing a legitimate service."[46]

Conclusion

The use of Internet, the widespread of innovative technology, the increasing number of Internet users, the fast-paced development of high-tech hardware and

[45] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering (accessed: 24.11.2016)

[46] IOCTA (2016), op. cit. p. 43.

software contribute to the expansion of cybercrime and organised crime in the cyber space and on the networks. It makes possible for criminals to meet each other in the online world without physical connection. Most of the users are not aware of the danger of the Internet, they can be deceived easily and become a victim of a cybercrime. Their computer or mobile devices might serve criminal networks without their knowledge. The cybercrime phenomenon intensifies the competition between the safety, security technology and the technical knowledge of the cybercriminals.

Bibliography

- Balogh, Á., The definition of criminal organization and consequences of committing crime in the framework of a criminal organization under Hungarian criminal law. Law Series of the Annals of the West University of Timisoara 2015.
- Bardócz, Cs., Pénzmosási technikák [Money laundering techniques]. Belügyi Szemle XXX. évfolyam, 1997.
- Broadhurst R. – Grabosky P. - Alazab M. – Chon S., Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology. Vol 8 Issue 1 January - June 2014.
- Directive 2013/40/EU on attacks against information systems
- Directive 2011/92/EU of the European Parliament and the Council on combating the sexual abuse and sexual exploitation of children and child pornography
- Dornfeld, L., A virtuális tér geopolitikája. In: Dornfeld L. – Keleti A. – Barsy M. – Kilin J. – Berki G. – Pintér I. 2016/1. szám
- EUROPOL – Internet Organised Crime Threat Assesment (IOCTA) 2014.
- EUROPOL – Internet Organised Crime Threat Assesment (IOCTA) 2016.
- Farkas I. – Jávorszky J., Az illegális pénznyerő-automaták felderítése [The investigation of illegal gambling machines]. Rendészeti Szemle, XXXI. évfolyam 1993.5.
- Gál, I. L., A pénzmosás és terrorizmus finanszírozása. [Money Laundering and financing terrorism] In: László Korinek – László Kőhalmi – Csongor Herke (editors). Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára. PTE ÁJK Pécs, 2004.
- Gercke, M., Understanding cybercrime: phenome, challenges and legal response. ITU 2012.
- Jean-Loup Richet, Laundering money online: a review of cybercriminals methods.
- Korinek, L., Kriminológia II [Criminology II]. Budapest, 2009.
- McGuire, M., Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security.
- Mezei, N., Digitalizált bűnözés – digitalizált védelem. [Digitized crime – digitized protection]. Rendészeti Szemle, 57. 2009.
- Mitnick K. – Simon W., A behatolás művészete [The art of intrusion]. Perfekt kiadó. Budapest, 2006.
- Nagy, Z., Bűncselekmények számítógépes környezetben [Crimes in the IT envrionment]. Budapest, Ad-Librum, 2009. p.
- Nato, J., Cybercrime, Organized Crime and Societal Responses. Emilio C. Viano (editor).
- Papp, P., Hi-tech bűnözés napjainkban [High tech crime in our days]. Belügyi Szemle 52. 2001/11-12.

- Parti, K., Gyermekpornográfia az interneten [Child ponography ont he Internet]. Bíbor Kiadó, Miskolc, 2009.
- Rogers, A., From peer-to-peer networks to cloud computing: how technology is redefining child pornography laws
- Sebők, J. A harmadik világháború (Mítosz vagy realitás) [The third World War (Myth or reality)]. Budapest, Népszabadság könyvek, 2007.
- The Interagency Working Group on Sexual Exploitation of Children: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Adopted by the Interagency Working Group in Luxembourg, 28 January 2016)
- Tóth, M., A bűnszervezet környéke. [The environs of the criminal organization] Jogtudományi Közlöny
1997,12.
- Tóth D. – Gál I. – Kőhalmi L. – Organized crime in Hungary. Journal of Eastern-European Criminal Law. 2015.
- Tropina, T., The evolving structure of online criminality: how cybercrime is getting organised. eucrim 4/2012.

Online sources

- http://www.unicri.it/special_topics/securing_cyberspace/cyber_threats/explanations/ (accessed: 12.11.2016)
- https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html (accessed: 18.11.2016)
- https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629 (accessed: 21.11.2016)
- http://news.softpedia.com/news/members-of-dd4bc-the-group-that-blackmailed-companies-with-ddos-attacks-arrested-by-europol-498797.shtml (accessed: 21.11.2016)
- https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering (accessed: 24.11.2016)