The Regulation of Crimes Against Information Systems in Hungary*

Dr. Kitti Mezei
Junior Research Fellow
Hungarian Academy of Sciences, Centre for Social Sciences
Institute for Legal Studies
Ph.D. student
University of Pécs, Faculty of Law
Department of Criminal Law

Abstract

The aim of this study to present the legislation of the Hungarian criminal law in relation to cybercrime in the light of the European Union's effect on it. Since cybercrime has a transnational nature it presents a great challenge for legislators and law enforcement as well as on an international and on a national level like in Hungary too. The paper also deals with the most current and dangerous cyber challenges such as DDoS attacks and ransomware through demonstrating how these committed cyber-attacks are considered to be punished in accordance with the Hungarian Criminal Code's provisions. Introducing the following crimes: breach of information system and data, compromising or defrauding the integrity of the computer protection system or device and information system fraud.

Key words: *system, cyber challenges, fraud, crimes, computer protection system, device, information system.*

1. Introduction

Developments in information and communication technology (ICT) and digital computing devices have dramatically changed the ways in which people live and communicate, making their life more convenient with the offered advantages. However the developments also provide new opportunities for cybercriminals to exploit. Firstly, new offenses targeting computer and data have become increasingly common thank to the advancement of mobile devices and technology – so-called Internet of Things – that makes possible to connect all type of devices such as computers, smartphones and other smart household appliances and so on. Secondly, traditional offences are also stimulated by the new opportunities. Since cybercrime has a transnational nature it presents a great challenge for legislators and law enforcement as well as on an international and on a national level like in Hungary too.[1]

* SUPPORTED BY THE ÚNKP-17-3-I NEW NATIONAL EXCELLENCE PROGRAM OF THE MINISTRY OF HUMAN CAPACITIES.

[1] WANG, Qianyun: A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. 2016. p. 1.

2. The European Union's effect on the Hungarian criminal law legislation in cybercrime

The European integration has reached several fields of criminal law in the last decades and cybercrime is one of them.[2] The European Union's regulation affects the Hungarian legislation greatly and the author highlights the most relevant agreements related to the cybercrime.

In 2001, Hungary joined to sign the European Council's Convention on Cybercrime, which is the most influential international legal instrument in cybercrime. The Convention is open to signature and ratification for states who are not member of the European Council.[3] It was the first document which contained the substantive and procedure criminal law in regard to cybercrime. As a consequence of enactment of the Cybercrime Convention into the Hungarian legislation, the legislators altered the Hungarian Act IV of 1978 on the Criminal Code and refreshed the regulation of the computer crimes too. The old Criminal Code introduced the 'criminal conduct for breaching computer systems and computer data' in Section 300/C. and 'compromising or defrauding the integrity of the computer protection system or device' in Section 300/E. The legislators always must play an active role to make new regulations in this constant changing cyber environment.[4]

In 2013, the new Directive 2013/40/EU of the European Parliament and of the Council on the attacks against information systems came into effect and replaced the earlier EU regulation, the Council Framework Decision 2005/222/JHA. Both the EU Directive and the Council Framework are determinative to the Hungarian legislation.[5] The new EU Directive established minimum rules concerning the definition of criminal offenses and the relevant sanctions and to improve cooperation between competent authorities. It also draws attention to information systems[6] which are a key element of political, social and economic interaction in the EU, while introducing a new term which is more accurate to the ICT developments rather than using the old 'computer' term. The EU 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 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. According to the Directive (Article 3 – 9), the following crimes must be punishable in Member States: illegal access to information system, illegal system interference, illegal data interference, illegal interception, tools used for committing offences. In accordance with the Directive, the new Hungarian Act C

[2] GÁL, István László – TÓTH, Mihály: Az uniós jog és a magyar jogrendszer viszonya – büntető anyagi jogi jogharmonizáció. In: Tilk Péter (editor): Uniós jog és a magyar jogrendszer viszonya. Pécs, 2016. pp. 463 - 465.

[3] The European Council accepted the Convention on Cybercrime in Budapest, on 24 November 2001.

[4] DORNFELD, László: A kiberbűnözés elleni küzdelem kihívásai. [The challenges of fight against cybercrime] Diskurzus: Batthány Lajos Szakkolégium Tudományos Folyóirata 5. p. 1.

[5] SINKU, Pál: A vagyon elleni bűncselekmények. [Offenses against property] In: Busch Béla (editor): Büntetőjog II., HVG-Orac Lap- és Könyvkiadó. Budapest, 2012. p. 623.

[6] According to the Directive 2013/40/EU: 'information system means a device or group of interconnected 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.'

of 2012 on the Criminal Code introduced the new information system term and an individual chapter (Chapter XLIII – 'illicit access to data and crimes against information systems') for the attacks against information systems. The new Criminal Code includes the following by name and content changed crimes: 'breach of information system or data' in Section 423, 'compromising or defrauding the integrity of the computer protection system or device' in Section 424.

It also introduced a new crime, the 'information system fraud' in the chapter of offenses against property (Chapter XXXVI). According to the justification of the Criminal Code, the information system fraud is an act of causing damage fraud, which first of all violates financial interest, furthermore these fraud like conducts are absent of the classical fraud's conditions, which are the use of deceit, deception or trickery, *i.e.* explains why it is appeared as a sui generis crime in the new Criminal Code. The current regulation differs from the former ones: firstly, this crime was handled as fraud,[7] but later in our previous Criminal Code (due to the amendment of 1994) it was regarded as computer fraud. There was also an amendment in 2001 when this crime found its place among the economic crimes as the criminal conduct for breaching computer systems and computer data, also as the cash-substitute payment instrument fraud.

3. The effective regulation of cybercrime in Hungary

3.1. Breach of Information System or Data

Section 423

(1) Any person who gains unauthorized entry to an information system by compromising or defrauding the integrity of the technical means designed to protect the information system, or overrides or infringes his user privileges is guilty of a misdemeanor punishable by imprisonment not exceeding two years.

(2) Any person who:

a) disrupts the use of the information system unlawfully or by way of breaching his user privileges; or

b) alters or deletes, or renders inaccessible without permission, or by way of breaching his user privileges, data in the information system;

is guilty of a felony punishable by imprisonment not exceeding three years.

(3) The penalty shall be imprisonment between one to five years for a felony if the acts defined in Subsection (2) involve a substantial number of information systems.

(4) The penalty shall be imprisonment between two to eight years if the criminal offense is committed against works of public concern.

There are more *protected legal objects* of this crime: firstly, in the Subsection (1), it is the integrity and security of the information systems. Secondly, it is more specific in the a) and b) points of the Subsection (2), which is the safe operation of the information systems without interruption and complemented with the interest of the integrity, stability and authenticity of the electronic data in the b) point.

The *subjects of the crime* are the followings: information system and data in the information system. In accordance with the closing provisions, 'information system'

[7] PALLAGI, Anikó: A vagyon elleni bűncselekmények. [Offenses against property] In: Blaskó – Hautzinger – Madai – Pallagi – Polt – Schubauer, Büntetőjog – Különös Rész II.; Rejtjel Kiadó. Budapest - Debrecen, 2013. p. 200.

shall mean equipment intended for the automatic processing, handling, storage and transmission of data or a collection of such devices that are interfaced. According to the Subsection (5), in the application of this Section 'data' shall mean facts, information or datum stored, controlled, processed and transmitted in information systems in all forms which allows them to be processed in information systems, including those programs designed to execute certain functions by the information systems.[8]

There are three different basic cases with different *criminal conducts* in Subsection (1) and (2). First of all, *gaining unauthorized entry* to an information system, id est hacking, is a punishable act in Subsection (1). "The mere unauthorised intrusion, *i.e.* 'hacking', 'cracking' or 'computer trespass' should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery."[9] In the firs scenario, unauthorized entry is when the hacker pretends to be the entitled user and uses the information system which is owned or used by the legitimate user. It means basically logging on without permission. At the more sophisticated level it may involves using networks to gain remote access via information systems in several jurisdictions. Such hacks may be 'user level', where the hacker has the same access to the system as an ordinary user of the system, or 'root level' or 'god' access, where the hacker has the same rights as the system administrator and can view or modify data at will. The hackers are seeking the 'bugs' in different software to exploit them. There are essentially three motivations to entry a system: access to information (*e.g.* confidential commercial or government information such as trade secrets, intellectual property or personal information like medical records, credit card, social security numbers), modification of data (*e.g.* delete or modify accounts, databases etc.) or use of a computer (*e.g.* obtain valuable services for free, 'wardriving' which means using a wireless network without authorisation and gives rise to a number of potentially criminal scenarios).[10]

It is significant to be emphasised that the information system *must be protected by technical-security means* such as passwords or programs and it must be active, otherwise the entry is not considered to be unauthorized. It is regarded to be culpable if the perpetrator compromises or defrauds the technical protection, but it is irrelevant how the criminal acquired it like by using social engineering techniques, using force or intimidation, capturing the information thank to the negligence of the target user, using decoder or spyware program.[11] Generally the weakest link in security chain is the human element that's why attackers prefer social engineering techniques (such as phishing) rather than using technical solutions. According to Kevin Mitnick – the world's most famous hacker – social engineering bypasess all the technologies, including

---

[8] NAGY, Zoltán András: XLIII. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. [Illicit acces to data and crimes against information systems] In: Tóth Mihály – Nagy Zoltán (editors.): Magyar Büntetőjog – Különös Rész. Osiris Kiadó, Budapest 2014. p. 594.

[9] The Explanatory Report to the Convention on Cybercrime. Budapest, 2001. p. 9.

[10] NAGY, Zoltán András: Számítógépes környezetben elkövetett bűncselekmények. Ad Librum Kft. Budapest, 2009. pp. 271-272.

[11] NAGY (2014a) Op. cit. pp. 594-595.

firewalls by using manipulation, influence and deception to get a person, a trusted insider within an organization, to a comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker.[12] Unfortunately in case of cybercrime, most of the time users contribute to become the victim of these type of crimes like by sharing too much personal information, falling for phishing easily and so on.[13]

In the second scenario of this Subsection, unauthorized entry shall happen when the authorized user overrides or infringes his privileges, which means that he logs in with his own name and password but he does such operations which he has no right like the system administrator of an institution or a company starts collecting the data of the system's users.

According to Subsection (2) point a), *the unlawful disruption of the use of the information system* is punishable. It might happen by installing, activating malicious software (malware)[14] offline like inserted directly via pendrive, CD or DVD or online via Internet or other computer network via executable files (e.g. downloading infected e-mail attachments or files from Peer-to-Peer networks), which are able to affect the operation of the information system differently.[15] Launching a distributed denial of service (DDoS) attack is a good example of disruption without entering the system. It is a cybercrime in which the primary goal is to deny users of computers or other types of electronic devices access to an information system or its resources (such as making unavailable online services like e-banking or webshop of businesses etc.). DDoS attacks often involve flooding a computer network with massive amounts of data in a short period of time so that servers cannot keep up with the amount of data being transmitted.[16] In point a), besides the criminal conduct, the *consequence* is also stated, requiring the realized and unlawful disruption, which includes the case when the system does not work at all, but also it covers when it does not work properly by any aspects or it does not operate properly for its intended purpose[17]. For example in 2016, the Hungarian government's websites were under a wave of DDoS attacks, which caused information system partially breakdown for few hours.[18] It is worth to mention that there is a new tendency when cybercriminals use an extortion scheme with DDoS attacks against specified website owners (*e.g.* the targets are like from the energy,

[12] MITNICK, Kevin D. – SIMON, William L.: A legendás hacker – A megtévesztés művészete. Perfect Kiadó Budapest, 2003.

[13] PARTI, Katalin – KISS, Tibor: Informatikai bűnözés. [Cybercime] In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia 2. Wolter Kluwer, Budapest, 2016. pp. 505-506.

[14] For example the most common ones are viruses, worms, Trojans, bots and spyware. A virus infects another program. Worms are self-replicating without infecting other programs. Trojans are programs which appear to be innocent but contain a hidden function (like opening 'back door' access). A bot is a program which infects a targeted computer and allows it to be controlled remotely. The term'spyware' is a generic description for a range of programs that in some way monitor computer use.

[15] NAGY (2014a) Op. cit. pp. 594-595.

[16] MCQUADE, Samual C. III.: Encyclopedia of cybercrime. Greenwood Publishing Group 2009. p. 63.

[17] MOLNÁR, Gábor Miklós: XLIII. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. [Illicit acces to data and crimes against information systems] In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál (editors): Büntetőjog II. – Különöse Rész. HVG-Orac Lap és Könyvkiadó Kft. Budapest, 2016. november p. 948.

[18] http://www.kormany.hu/hu/belugyminiszterium/hirek/senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast Downloaded: 11.11.2017

financial sector or gambling websites), if they pay the ransom – cryptocurrencies like Bitcoin[19] – then they may regain control of their site without interruption.[20]

In point b), it subjects to punishment for altering or deleting, or rendering inaccessible data in the information system. It is important to note that software, programs are also regarded as data. *'Alteration'* means the modification of the content of existing data like make it misleading and/or worthless[21] by overwriting or deleting it partially etc. It is irrelevant whether it is stored in internal or external data medium (e.g. HDD, SSD or pendrive).[22] For example Supreme Court of Hungary established this crime when somebody entered the higher education's study system – so-called NEPTUN – and changed the grade of a not fulfilled exam. It may be used to obtain different advantage for example by increasing a line of credit.[23] The unlawful modification of the content of a website is the so-called 'website defacement', when the website's appearance is changed like different pictures and or/words are placed there. It is considered to be a virtual graffiti by most like hacktivist.[24] The targets are generally government organizations (*e.g.* the Constitutional Court of Hungary's website was defaced in 2012) and religious websites.[25] *Deleting* means the complete removal of data. For example there was a case handled by the Supreme Court of Hungary when the system administrator logged from his own workstation in his boss's computer and unlawfully deleted data files.[26] *Rendering inaccessible* do not need any comments, it may happen when data is hidden in a file or folder, which is protected by password or it becomes encrypted.[27] Ransomware continues be one of the most prominent malware threats in terms of the variety and range of its victims and the damage done by the criminal use of encryption. Ransomware encrypts certain file types on infected systems and forces victims to pay the ransom to get a decrypt key, because it is based on data encryption the attacker accomplishes the breach of data offence according to the Hungarian Criminal Code. This malware is popular among cybercriminals since beyond the initial infection, all the attacker has to do is collect the ransom payment, and by using pseudonymous currencies such as Bitcoin, then laundering and monetisation is considerably simple. Furthermore, the nature of the attack means that ransomware can attack a much more diverse range of targets. Victims are atypical from the usual financial targets, and include entities such as hospitals, law enforcement agencies, and government departments and services. While the public also continues to be targeted, small to

[19] Bitcoin, launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency based on blockchain technology. Transactions are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual. Therefore, Bitcoin is said to be "pseudoanonymous".

[20] NAGY, Zoltán András: A sértett szerepe néhány kibertérben elkövetett bűncselekményben – alkalmazott viktimológia. . [The role of the victim in commited crimes in the cyberspace - applied victimology] In: Finszter Géza – Kőhalmi László – Végh Zsuzsanna (editors) Egy jobb világot hátrahagyni… Tanulmányok Korinek László professzor tiszteletére. Pécs, 2016. p. 488.

[21] CLOUGH, Jonathan: Principles of cybercrime. Cambridge University Press, 2010. p. 29.

[22] NAGY (2014a) Op. cit. p. 598.

[23] CLOUGH Op. cit. p. 29.

[24] See more: SIMON, Béla: Hactivism and its status in Hungary. Magyar Rendészet. 2016. 16:(2) pp.161-174.

[25] https://www.techopedia.com/definition/4870/defacement Downloaded: 21.11.2017

[26] MOLNÁR Op. cit. p. 950.

[27] NAGY (2014a) Op. cit. p. 598.

medium enterprises, who often lack the resources to fully safeguard their data and networks, are also key targets.[28]

One of the *aggravating circumstances* of this crime is accomplished if the attack affects a *substantial number of information systems*, although the Criminal Code does not define it, so the practice of the law enforcers has to deal with it.[29] For example, when the attacker obtain access in more information systems and infects them with malware. Nowadays the two most dangerous viruses are ransomware and botnet virus. In 2017, The WannaCry ransomware is believed to have rapidly infected up to 300 000 victims in over 150 countries, including a number of high-profile targets such as the UK's National Health Service, Spanish telecommunication company Telefonica, and logistics company Fed-Ex.[30] Another good example is a DDoS attack, which is launched from botnets. Botnets are large clusters of connected devices via Internet (*e.g.* PCs, smartphones, routers, other smart devices), infected with malware that allows remote control by the attacker – so-called botmaster – without the computer user's knowledge. These infected devices are called zombies. Some botnets might have a few hundred or a couple thousand computers, but others have tens and even hundreds of thousands of zombies at their disposal. Once created, the infected network of computers that constitute the botnet can be activated without the computer users' knowledge in order to launch a large-scale cyber-attack, which usually has the capacity to cause serious damage like a cyber-attack against national critical infrastructure have the potential to inflict significant, real-life disruption and prevent access to critical services that are vital to the functioning of our economy and society (*e.g.* energy, transportation, health and financial services).[31] After the first devastating Stuxnet worm, which was designed for a targeted attack and managed to stop Iran's nuclear plan for years by destroying large number of uranium enriching centrifuges, there are an increasing number of targeted cyber-attacks against SCADA systems, which is an industrial control system at the core of many industries as manufacturing, energy, water, power and more.[32] *Critical infrastructure* means the assets or systems essential for the maintenance of vital social functions, health, safety, security, and economic or social wellbeing of people.[33] The most commonly reported (to law enforcement) attacks against critical infrastructures in the EU were DDoS attacks, with over 20% of countries reporting cases.[34]

Another *aggravating circumstance* of this crime happens if the criminal offense is *committed against works of public concern*. According to the closing provisions, 'works of public concern' shall mean: public utilities, public transportation operations, electronic communication networks, d) logistics, financial and IT hubs and operations necessary

---

[28] EUROPOL (European Cybercrime Centre – EC3): Internet Organised Crime Threat Assesment, 2017. p. 19. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 Downloaded: 24.11.2017

[29] MOLNÁR Op. cit. p. 950.

[30] EUROPOL (2017) Op. cit p. 19.

[31] NAGY, Zoltán András – MEZEI, Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. [Ransomware and botnet virus as the most dangerous computer viruses]. In: Szent Lászlótól a modernkori rendészettudományig. Pécs, 2017. p. 163 – 166.

[32] *NAGY, Zoltán András: A kiber-háború új dimenzió – a veszélyeztetett állam biztonság (Stuxnet, DuQu, Flame – a Police Malware). [Cyber warfare as a new diemnsion – endangered state security (Stuxnet, DuQu, Flame – Police Malware] Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012. p. 225-226.*

[33] Directive 2008/114/EC on the identification and designation of European Critical Infrastructures

[34] EUROPOL (2017) Op. cit. p. 26.

for the performance of the tasks of universal postal service providers carried out in the public interest, plants producing war materials, military items, energy or basic materials destined for industrial use. It is noteworthy that the definition of works of public concern and critical infrastructure do not cover each other, since the social wellbeing, health-care institutions are missing from the enumeration, which may rise concern since cyber-attacks against health institutions are on the rise and this year the Hungarian government introduced e-health-care system which means our medical records, as sensitive and valuable data for the cybercriminals, are at more risk.

It is an *intentional crime*, which means it can committed with dolus directus and dolus eventualis. In Subsection (2) point b), the intent must be aimed at the fact that due to the attacker's act the information system is unlawfully disrupted. The *perpetrator* can be anybody, who commits the abovementioned criminal conducts.

The breach of information system or data's different basic scenarios may happen side by side or one after another, but the part actions forms a unit and the perpetrator is going to be called to account for the more serious case. For example if the attacker does hacking in a protected computer and after he or she installs a virus or delete data, then he will be responsible for the latter one, it is threatened with a more serious sentence.

The multiple counts of this offense depends on the number of the attacked information systems. The Criminal Code protects all information systems individually whether it has the same or different owners, operator etc.[35]

3.2. Compromising or Defrauding the Integrity of the Computer Protection System or Device

Section 424

(1) Any person who, for the commission of the criminal offense defined in Section 375 or 423: a) creates, transfers, supplies, obtains or places on the market passwords or computer programs required therefor or facilitating thereof; or

b) offers his economic, technical and/or organizational expertise to another person for the creation of passwords or computer programs required therefor or facilitating thereof; is guilty of a misdemeanor punishable by imprisonment not exceeding two years.

The *protected legal object* is the interest of the information system's operation without disruption and stability, authenticity and privacy of the stored, managed, processed or transmitted data.

The *subjects of the crime* are passwords or computer programs. According to Subsection (3), for the purposes of this Section 'password' shall mean any identifier comprised of a string of alphanumeric characters, codes, biometric data or the combination thereof, designed to gain entry into an information system or any segment thereof.

In Subsection (1) point a), the first criminal conduct is creating, transferring, supplying, obtaining or placing on the market passwords or computer programs. *Creating* means any conducts which has an outcome as a finished password, program like writing program, generating or overwriting a password. *Transferring* is referred to conveying profession from the creator to different person, although it may happen by making available the password or program or passing the knowledge. *Supplying* occurs

[35] NAGY (2014a) Op. cit. p. 598 -599.

when due to activity or negligence the program or password becomes available for not entitled person or people. *Obtaining* means gaining possession on the program or password from the program write or any other people. *Placing on the market* means the perpetrator intentionally makes available the password or program for more, just as well indefinite number of people which may happen by giving it to only one person while the offender is aware of that the chosen person is going to hand over for more people. In all cases, it is indifferent whether it happens free or for a valuable consideration or by deception or other way.

In Subsection (1) point b), a *sui generis act of aider* is punishable, which involves the psychic and physical form of aiding and abetting. The *criminal conduct* is offering economic, technical and/or organizational expertise to another person for the creation of passwords or computer programs required therefor or facilitating thereof. Offering expertise means that the involved person acquires the knowledge, which might be simple the knowledge or an object containing it (e.g. theoretical and practical knowledge of breaking passwords, writing malicious programs sharing contacts etc.). The perpetrator can be only that person who has the knowledge to offer.

In both cases it can be committed only intentionally and this Section also states an aim which means it has to be perpetrated in order to commit the criminal offense defined in Section 375 or 423.[36]

The legislator has set a *ground for exemption from criminal responsibility* in Subsection (2), which says that in the case of Paragraph a) of Subsection (1), any person who confesses to the authorities his involvement in the creation of any password or computer program required for the commission of the criminal offense, or facilitating thereof, before the authorities learned of such activities through their own efforts, and if the person surrenders such produced things to the authorities and assists in the efforts to identify the other persons involved, shall not be prosecuted.

The multiple counts of this offense depends on the number of the attacked information systems as well as, but if the perpetrator accomplishes information system fraud or breach of information system or data then he or she will be prosecuted for those crimes and his or her preparation, which means the carried out compromising or defrauding the integrity of the computer protection system or device, will be an unpunished pre-action.[37]

It is noteworthy to mention, which present a great challenge to law enforcement especially regarded to investigations: the '*illicit online markets*, both on the surface web and *Darknet*, provide criminal vendors the opportunity to purvey all manner of illicit commodities, with those of a more serious nature typically found deeper in the Darknet. Many of these illicit goods, such as cybercrime toolkits or fake documents, are enablers for further criminality.'[38] The so-called *Crime-as-a-Service* (CaaS) business model drives the digital underground economy by providing a wide range of commercial services that facilitate almost any type of cybercrime. The anonymisation techniques (e.g. by using specialised browser like Tor instead of the regular ones and carrying out transactions by using hard-to-trade virtual currencies such as Bitcoin) used in parts of the Internet, known as Darknets and hidden services, allow users to communicate and trade illicit goods (such as online trade in drugs, child abuse material, cybercrime tools and services, data and weapons) freely without the risk of being traced and captured.

[36] NAGY (2014a) Op. cit. pp. 600-601.
[37] MOLNÁR Op. cit. p. 954.
[38] EUROPOL (2017) Op. cit. p. 48.

Cybercriminals generally use two platforms for this purpose: underground forums (such as Alphabay) or criminal marketplaces (like Silk Road). The cybercriminal's toolkit may include malware, supporting infrastructure, stolen personal and financial data and the means to monetise their criminal gains. Cybercrime toolkits are available to purchase or hire as a service (*e.g.* DDoS-as-a-Service, Malware-as-a-Service, Data-as-a-Service), it is relatively easy for cybercrime initiatives – even if the attacker has lack of experience and technical skills - to launch – even high scale -cyber-attacks not only of a scale highly disproportionate to their ability but for a price similarly disproportionate to the potential damage (e.g. a DDoS attack tool and a whole botnet infrastructure is available from 5$ to 1000$ and it is almost only one click for the attacker without any technical knowledge). Not to mention it allows experienced cybercriminals to focus on their core activities, becoming more efficient and specialised since they can buy everything else they need.[39]

3.3. Information system fraud

Section 375

(1) Any person who, for unlawful financial gain, introduces data into an information system, or alters or deletes data processed therein, or renders data inaccessible, or otherwise interferes with the functioning of the information system, and thereby causes damage, is guilty of a felony punishable by imprisonment not exceeding three years.

(2) The penalty shall be imprisonment between one to five years if:

a) the information system fraud results in damage of substantial value; or

b) the information system fraud involves a considerable value and it is committed in criminal association with accomplices or on a commercial scale.

(3) The penalty shall be imprisonment between two to eight years if:

a) the information system fraud results in damage of particularly considerable value; or

b) the information system fraud involves a substantial value and it is committed in criminal association with accomplices or on a commercial scale.

(4) The penalty shall be imprisonment between five to ten years, if:

a) the information system fraud results in damage of particularly substantial value; or

b) the information system fraud involves a particularly considerable value and it is committed in criminal association with accomplices or on a commercial scale.

(5) Any person who causes damage by using a counterfeit or forged, or unlawfully obtained electronic payment instrument, or by accepting payment with such payment instrument shall be punishable in accordance with Subsections (1)-(4).

(6) In the application of Subsection (5) cash-substitute payment instruments issued in other States shall receive the same protection as cash-substitute payment instruments issued in Hungary.

As far as the information system fraud is concerned in the new Criminal Code, *the protected legal object* of this felony is the interest of the function of the financial relations, information systems and cash-substitute payment instruments without any interruptions.[40]

---

[39] EUROPOL (European Cybercrime Centre – EC3): Internet Organised Crime Threat Assesment, 2014. p. 19 -23.

[40] AKÁCZ, József: A vagyon elleni bűncselekmények. [Offenses against property] In: Kónya István (editor), Magyar Büntetőjog Kommentár a gyakorlat számára 3. kiadás II. kötet; HVG-Orac Lap- és Könyvkiadó. Budapest, 2013. p. 1412.

Since the delict consists of two statement of facts, consequently it has also two *subjects of crime*: on the one hand the information system,[41] which becomes the subject of crime through its data or program not by itself, and on the other the counterfeit, or unlawfully obtained electronic payment instrument (cash-substitute payment instruments issued in other States shall receive the same protection).[42]

The passive subject can be not only a natural person, but a legal person as well. The crime's injured party is the one to whom the damage is caused.[43]

The criminal conducts of the first statement in the Subsection (1) are the followings: any person who, for unlawful financial gain, introduces data into an information system, or alters or deletes data processed therein, or renders data inaccessible, or otherwise interferes with the functioning of the information system, and thereby causes damage, is guilty of a felony. *Introducing data* means uploading any fact, information or programs into an information system[44] in offline mode (for example with the help of keyboards, data mediums, external hard drives), or it could happen in online mode (with hacking). *Altering processed data* signifies that the modification is made in the content of the data, which is already in the information system (it can occur in various modes such as completing, deleting partially, or overwriting data). *Deleting data* means that the processed data is wiped.[45] *Rendering data inaccessible* occurs when the person, who is authorized for data the cognition, management or application, cannot access the data, even if it is hidden only temporarily.[46] The last perpetration conduct includes every action besides the enumerated ones, which *interfere with the functioning of the information system*.

The intention of these conducts is the unlawful financial gain, therefore it is considered to be an *intentional crime*. Damage causing[47] is needed for the consummated crime, which makes this crime *materialistic.* At the same time if the perpetrator starts the illegal intervention into the information system it means the attempt of the crime can be established.[48] The proved relation of the cause and effect between the perpetrator's conduct and the damage is a necessary condition. The intention of the unlawful financial gain assumes specific intent, though from the aspect of damage occurring and its extent the foreseeable intent is sufficient.[49]

The perpetrator can be anybody, who does the factual perpetration conduct, so it is not required to have an adequate qualification for committing the crime.[50] The following typical fraud actions with introducing data or altering processed data in the information system are regarded as information system fraud: opening a fictive bank account or credit account; transferring illegal payment to fictive/real bank account; transacting fictive transfers to the bank account; cutting down on someone's debt; duplicating

[41] Act C of 2012 Section 459. (1) 15.

[42] SINKU Op. cit. p. 623.; Act C of 2012 Section 459. (1) 19 and 20.

[43] NAGY, Zoltán András: A vagyon elleni bűncselekmények [Offenses against property] In: Tóth Mihály – Nagy Zoltán (editors): Magyar büntetőjog – Különös rész, Osiris Kiadó. Budapest, 2014. p. 461.

[44] PALLAGI Op. cit. p. 202.

[45] NAGY (2014b) Op. cit. p. 461.

[46] SZOMORA, Zsolt: A vagyon elleni bűncselekmények. [Offenses against property] In: Karsai Krisztina (editor): Kommentár a Büntető Törvénykönyvhöz, Complex Kiadó. Budapest, 2013. p. 788.

[47] NAGY (2014b), Op. cit. 461, 463.; Act C of 2012 Section 459. (1) 16.

[48] CSÁK, Zsolt: A vagyon elleni bűncselekmények. [Offenses against property] In: Polt Péter (editor), Új Btk. Kommentár 7. kötet, Nemzeti Közszolgálati és Tankönyv Kiadó. Budapest, 2013. p. 118.

[49] SZOMORA Op. cit. p. 788.

[50] CSÁK Op. cit p. 116.

lawful payments (such as salaries, pensions etc.). It does not matter whether these actions are committed in the interest of the perpetrator or a third party.[51]

The second statement of the crime includes *the misuse of the electronic payment instrument*, which is regulated in the Subsection (5): any person who causes damage by using a counterfeit or forged, or unlawfully obtained electronic payment instrument, or by accepting payment with such payment instrument shall be punishable in accordance with Subsections (1)-(4). Using the payment instrument as a perpetration conduct is known as the usage with the intended purpose (such as paying by credit card, collecting cash etc.). Accepting the payment instrument is virtually a sui generis physical accessory, both in the real (for example exchanging check or bill for cash, or paying with SZÉP card) and virtual space (online purchasing).[52] The perpetrator can be anybody in the first phrase, while in the second phrase it is necessary to be an authorized person for accepting the instrument. Culpability can be only intentional. The intention has to be regarded to the damage causing, and in the second case the authorized person has to be aware that the electronic payment instrument is counterfeit or forged, or unlawfully obtained.[53]

The aggravating circumstances are defined by the extent of the damage and the commitment in criminal association with accomplices or on a commercial scale. The basic case includes the damage of the minor and considerable value, the classified cases start from the damage of a substantial value. This crime does not have a minor offence form, so the action will be considered as a crime if it is in compliance with the requirements of the statement of facts. *The count of the crime* is determined by the numbers of the injured parties (typically the number of the bank account owners).[54]

4. Conclusion

The information systems are not regarded to the national borders, by the virtue of the connected information systems through the networks allow to access the data files from distance. The development of the ICT is rapid and as a consequence a lot of various new types of crime commitment has appeared, therefore the number of the committed cybercrimes is gradually increasing year by year and becoming more sophisticated. On that score, it is essential to harmonize the criminal laws and frame minimum rules on the international level. The EU legislation has set these minimum rules by the new Directive and the Hungarian Criminal Code meets its requirements, though there are still some parts regarding the information system crimes which need further harmonization (for example de lege ferenda extending the classified cases considering the organized crime commitment and sanctioning identity theft).[55]

---

[51] GYARAKI, Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN kód megadása sikeres vagy biztonságos az internet?! [Economic crimes in the computer environment. Giving the PINcode or is the internet safe?!] = Pécsi Határőr. Tudományos közlemények. 13. [köt.], 2012. pp. 317-318.; NAGY (2014b), Op. cit. p. 462.

[52] NAGY (2014b) Op. cit. p. 461.

[53] PALLAGI Op. cit. p. 206.

[54] SZOMORA Op. cit. p. 789.

[55] NAGY, Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról. Budapest, 2014. p. 5.

http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf – Downloaded: 28.11.2017.

Since cybercrime presents a complex problem it needs a solution in more steps including focusing on the prevention, raising public awareness since in most cases cybercrime could be avoided if the average users are more aware of the danger of different cyber trends. It is also essential to provide up-to-date training and education for the law enforcement, judges and prosecutors on this specific field of expertise. It is also important to make it a curriculum for the related law enforcement and law faculties.

References

AKÁCZ, József: A vagyon elleni bűncselekmények. [Offenses against property] In: Kónya István (editor), Magyar Büntetőjog Kommentár a gyakorlat számára 3. kiadás II. kötet; HVG-Orac Lap- és Könyvkiadó. Budapest, 2013.

CLOUGH, Jonathan: Principles of cybercrime. Cambridge University Press, 2010.

CSÁK, Zsolt: A vagyon elleni bűncselekmények. [Offenses against property] In: Polt Péter (editor), Új Btk. Kommentár 7. kötet, Nemzeti Közszolgálati és Tankönyv Kiadó. Budapest, 2013.

Directive 2008/114/EC on the identification and designation of European Critical Infrastructures

Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013 on attacks against information systems

DORNFELD, László: A kiberbűnözés elleni küzdelem kihívásai. [The challenges of fight against cybercrime] Diskurzus: Batthány Lajos Szakkolégium Tudományos Folyóirata 5.

EUROPOL (European Cybercrime Centre – EC3): Internet Organised Crime Threat Assesment, 2017.

EUROPOL (European Cybercrime Centre – EC3): Internet Organised Crime Threat Assesment, 2014.

GÁL, István László – TÓTH, Mihály: Az uniós jog és a magyar jogrendszer viszonya – büntető anyagi jogi jogharmonizáció. In: Tilk Péter (editor): Uniós jog és a magyar jogrendszer viszonya. Pécs, 2016.

GYARAKI, Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN kód megadása sikeres vagy biztonságos az internet?! [Economic crimes in the computer environment. Giving the PINcode or is the internet safe?!] = Pécsi Határőr. Tudományos közlemények. 13. [köt.], 2012.

MCQUADE, Samual C. III.: Encyclopedia of cybercrime. Greenwood Publishing Group 2009.

MITNICK, Kevin D. – SIMON, William L.: A legendás hacker – A megtévesztés művészete. Perfect Kiadó Budapest, 2003.

MOLNÁR, Gábor Miklós: XLIII. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. [Illicit acces to data and crimes against information systems] In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál (editors): Büntetőjog II. – Különöse Rész. HVG-Orac Lap és Könyvkiadó Kft. Budapest, 2016. november

NAGY, Zoltán András – MEZEI, Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. [Ransomware and botnet virus as the most dangerous computer viruses]. In: Szent Lászlótól a modernkori rendészettudományig. Pécs, 2017.

NAGY, Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról. Budapest, 2014.

NAGY, Zoltán András: A kiber-háború új dimenzió – a veszélyeztetett állam biztonság (Stuxnet, DuQu, Flame – a Police Malware). [Cyber warfare as a new diemnsion – endangered state security (Stuxnet, DuQu, Flame – Police Malware] Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012.

NAGY, Zoltán András: A sértett szerepe néhány kibertérben elkövetett bűncselekményben –alkalmazott viktimológia. . [The role of the victim in commited crimes in the cyberspace - applied victimology] In: Finszter Géza – Kőhalmi László – Végh Zsuzsanna (editors) Egy jobb világot hátrahagyni… Tanulmányok Korinek László professzor tiszteletére. Pécs, 2016.

NAGY, Zoltán András: A vagyon elleni bűncselekmények [Offenses against property] In: Tóth Mihály – Nagy Zoltán (editors): Magyar büntetőjog – Különös rész, Osiris Kiadó. Budapest, 2014.

NAGY, Zoltán András: Számítógépes környezetben elkövetett bűncselekmények. Ad Librum Kft. Budapest, 2009.

NAGY, Zoltán András: XLIII. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. [Illicit acces to data and crimes against information systems] In: Tóth Mihály – Nagy Zoltán (editors.): Magyar Büntetőjog – Különös Rész. Osiris Kiadó, Budapest 2014.

PALLAGI, Anikó: A vagyon elleni bűncselekmények. [Offenses against property] In: Blaskó – Hautzinger – Madai – Pallagi – Polt – Schubauer, Büntetőjog – Különös Rész II.; Rejtjel Kiadó. Budapest - Debrecen, 2013.

PARTI, Katalin – KISS, Tibor: Informatikai bűnözés. [Cybercime] In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia 2. Wolter Kluwer, Budapest, 2016.

SIMON, Béla: Hactivism and its status in Hungary. Magyar Rendészet. 2016. 16:(2)

SINKU, Pál: A vagyon elleni bűncselekmények. [Offenses against property] In: Busch Béla (editor): Büntetőjog II., HVG-Orac Lap- és Könyvkiadó. Budapest, 2012.

SZOMORA, Zsolt: A vagyon elleni bűncselekmények. [Offenses against property] In: Karsai Krisztina (editor): Kommentár a Büntető Törvénykönyvhöz, Complex Kiadó. Budapest, 2013.

The Convention on Cybercrime of the Council of Europe (CETS No.185)

The Explanatory Report to the Convention on Cybercrime. Budapest, 2001.

WANG, Qianyun: A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. 2016.

https://www.techopedia.com/definition/4870/defacement

http://www.kormany.hu/hu/belugyminiszterium/hirek/senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast