Cyber criminality

Bohumil Ptáček, Leopold Skoruša

Universityof Defence,Faculty of Military Leadership
Kounicova 65,66210Brno, Czech Republic

{bohumil.ptacek, leopold.skorusa}@unob.cz

Abstract. The article describes the use, respectively abuse of information and communications technology, with an emphasis on cyber-crime and possible approaches to its solution. The subject of the article is to identify the kinds of cyber threats and the types of cyber-attack relevant for the Czech Republic, the characteristic of some potential consequences of cyber-attacks and the description particular of the legal measures, methods and tools to fight the most serious forms of cyber-attacks.

Keywords: cyber, cybercrime,cyberspace,crime, information communication technology.

Introduction

The paper deals with the issue associated with information such as the most valuable goods at present. Information society, of which we are a part, adopted certain mechanisms, procedures and technologies to handle with information. We can say that today's advanced civilization is almost perfectly completely interdependent and interrelated. This is mainly due to the increasing availability of computers and other means of communication, and then another reason is the increasing technological sophistication of their connection. The primary role is played by the Internet, a network of networks, offering ever faster, cheaper and more versatile linkage of its individual components. This allows an obtaining and providing information without territorial and content restrictions. Technological advancements that information area is experiencing are unusually dynamic and we can also say difficult to control. The benefits of this progress go hand in hand with disadvantages, namely the misuse of computers and the Internet by criminally defective entities.

The question therefore arises whether the relationship between the benefits of information and communications technologies and their abuse does not remain the same and does change only the quantitative range. Unfortunately, the answer will not be found because the environment of the Internet, computers and information in general is changing every moment and it is hard to predict what direction it is going. The purpose of this article is to specify a computer and internet crime and to describe its peculiarities, especially with regard to a place of its sphere of activity, cyberspace,

as well as the entities involved in it. The fight against cyber-crime must be fought on many levels, the most important of which is a sufficiently effective cooperation in the field of legal regulation, especially at international level because of its cross-border operations. A significant role is played by the national, especially criminal law, which comprehensively regulates the merits of the crimes, under which can be subsumed the illegal dealings connected with computers and the Internet.

1 Informationcommunication technologies

The importance of information and communication technologies (ICT) today is enormous and unquestionable. We live in an information society that had adopted during its history numerous ways in communicating and receiving information. [1] The need to communicate has evolved, and it can be argued that its scope began with a newspaper and continued through electronic means such as the telegraph, telephone, radio, television up to the Internet. With some exaggeration, we can say that these means affect all human activities every day throughout the world. It is indisputable that the society itself is dependent on information technology in the sense that it is built on it. From another perspective, we also talk about its overuse. We got used to them, so that we use them more often than necessary and for the purposes other than expected. On the one hand it makes the information society profoundly integrated, coordinated and fast-growing; on the other hand, however, using these technologies, today's society is becoming increasingly vulnerable.

Increasing dependence of societies on information technologies leads to new forms of threats which these societies must be able to confront, regardless of whether they are deliberate threats, threats of anthropogenic nature or accidental, resulting from failures or natural disasters. Such, often repetitive sophisticated threats affect cyber, national and international security. Cyber threats are the product of different sources, they manifest witha divisive and disruptive activity directed against individuals, business entities, national infrastructure and they are characterized by specific features, such as their transnational nature, the anonymity of the attackers, dispersion, or the ability to attack from a great distance without direct contact with the target entity. Threat actors can be individuals, states or non-state entities. The main threats, which the nation states must face today,are hacking, cyber-crime, cyber terrorism, political and ideological extremism, hacktivism, cyber espionage or state-sponsored cyber-attacks and aggression, therefore cyber warfare.

2 New kind of criminality

As well as the benefits of information and communication technologies may be, and are used for beneficial purposes, in the same way they can be effectively misused. Inthe process of applyingemerging informationtechnologies issynergisticallydevelopedalso newtype of crime,namely computer, Internet or alsocybernetic crime. It is new because thesociallyharmfulactions, whichcharacterize it, cannotbe subsumed underexistingelements of the merits of the crimes in most

cases. This is reflectedin amendments to thelegislation in force, or in theadoption of a new one. This issue isalso thesubject of an adjustmentof international treaties, as well as European Union law. [2]

2.1 Cybercriminality

Under this term it must be understood committing a crime in which a computer plays a role in some way as a set of hardware and software, including data, or only some of its components, or a larger number of separate PCs or connected PCs to a computer network,either:

a) As a **subject** of this crime, with the exception of the crime, the subject of which devices are described as movable items, or
a) As an **instrument** of a crime. [3]

The legal definitions of the term cybercrime initially could not include offenses related to linked computers in a computer network, the Internet, for example, massively expanded in our country in the second half of the 90s of the last century. Wall [4] considers computer crime for the **first generation** of cyber-crime, such as crimes using computers as helpers for a committing a "classic" crimes. Cyber-crime can now evoke memories on crimes of a typeof the theft of a machine time, which is already rather outdated form of misuse of information technology, especially as a result of making access to computers to exponentially larger community of users. Another argument to oppose this term is the fact that in the legal theory there is not common practice to specify the category of offenses by the means used. [5]

With technological advances there occurred means allowing, in particular a communication between computers, as well as new devices connecting previously separate communications technology (calledhybrid appliances). The common denominator of these technologies has become a presence of data and networks - hence the term originated "**offense in information-communication theory**". Internet is a specific network among the many information-communication networks, which uses a special communications protocol - the Internet Protocol (IP). Hence the **Internet criminal offense**. [6]

2.2 Cyber criminality and cyber-crime

Cyber criminality is sometimes equated with the term of cyber-crime. So it is also in the Convention on *computer*criminality. Its original name, however, is "Convention on Cybercrime" convenient translation would therefore be the Convention on Cybercriminality. Cyber criminality was defined also by the 10th UN Congress on Crime Prevention and a treatment of offenders in two senses:

a) Ina narrower sense: Any illegal conduct carried out by means of electronic operations aimed at the security of computer systems and their data being processed.
b) In a broader sense: Any illegal conduct committed by means of a computer system or network, or in connection therewith, including such crimes as illegal possession, offering or distributing information by computer.

These efforts on legal definitions have undoubtedly of paramount importance in the field of harmonization of national laws, however compelling and consistent definition of cybercriminality, cyber-crime (cybercrime) do not provide. Volevecký [7], the term cyber-crime finds crimes committed using information technology. Cyber criminality in this sense can be described as any illicit dealings operated in cyberspace. Then it goes beyond the term of computer and internet criminality and undoubtedly it will include such activities committed using the handsets and not only those mobile handheld computers.

Cybercrime is then, according to in the legal environment more or less accepted definition understood (cumulatively) as:

a) The offense endangering ICT - Information and network security (a crime against the computer integrity or even a crime in the narrower sense).
b) The offense using ICT to commit traditional offenses; and
c) The offense is related to the content of computer data (such as child pornography, defamation and violation of intellectual property rights).

This concept can be considered the most suitable from a professional point of view because it replicates the Convention, where such conductsare explained.

2.3 Difference from the traditional criminality

Information technologies play the key and decisive role in this field. Specific technologies and procedures, which are necessary for their use, they give advantage to those consecrated and let ordinary users behind. On one side are specialists, experts that determine the direction in which these technologies will go, on the other hand, subjects with minimal knowledge. However, availability, simplicity and convenience of their use permit to acquire the status of the perpetrators of cybercrime almost to everyone. Computers are becoming powerful tools, which in the wrong hands can cause immense damage.

Different is **the crimescene** (cyberspace), which is fundamentally different from the real one and as such offers different environment to commit a cybercrime. Typically, this is an issue of the ratio of an activity and an effect. No other environment does not allow to cause so considerable damagesfrom the comforts of home by a just few acts. The followed attack is not directed against one victim, but is mostly determined to an unclosed number of users. The attack may occur immediately or after some time. Speed data exchange is unprecedented and therefore also the movement in cyberspace, of which the offender may simply disappear, leaving only the consequences of an attack. This makes a detection and investigation difficult. Another factor is the anonymity. The user does not have his unique identification, face; he can "create" it according to his will, or to impersonate someone else. In this regard, it is called Identity theft.

Similarly, the view of the society on this intangible environment is different. Some of the offenses are not considered as despicably as their equivalent counterparts. For example, an offender who carried out an armed robbery of a bank is perceived differently than an offender who unlawfully transferred tens of millions on his behalf.

The condition of a minimizing cyber-crime is sufficiently effective legislation of the issues, leading to the effective definition and to criminalization of the most harmful activities affecting information security. The creation of the required legal standards is easier in traditional crimes that occurred over hundreds of years in the legal systems of the vast majority of civilized countries. However, legislative process is more complicated due tothe rapid development in information technology, ingenuity of offenders,and a need of expertise by lawmakers. This contributes to significant delays of a legal regulation and it allows offenders almost with impunity to develop socially harmful activities. Another reason, inter alia, is the low legal awareness of the public on cybercriminality. The publicdoes not consider certain practices as the crime.

Cyber criminality is committed with the use of very sophisticated technological tools and specialized knowledge. The detection and prove of cyber criminality require usually very specific tools, knowledge and practices. There is therefore a need for highly skilled workers from the technological and legal aspect. Classic police investigation methods often fail, it is mainly due to the different nature of the evidence (traces) in cyberspace, their durability and applicability in evidentiaryproceedings. DNA does not remain at the scene, also fingerprints or scent traces do not remain. Although expressions of cyber criminality area crime, it is not always easy to detect such activity, prove and convict the perpetrators. [8]

2.4 The need for legal regulation of cyber criminality

Information structure of a cyberspace represents the values that should be according to the majority of opinion protected by means of criminal law. The existing criminal law was not written with the knowledge of online society in a cyberspace. The cyberspace is a reality since the 90s of the last century and its impact is unprecedentedly enormous and criminal law does not kept pace with it initially, moreover,at cyber criminality resulteddelays of legal regulation even more than in ordinary criminal offenses. Some cyber-attacks could be subsumed under existing merits of a crime, for example, typically under a merit of a crime of fraud. But the question is whether lawmakers wanted to underpin actions which at the time of enactment not existed in the real world. Instead of extensive interpretation, lawmakers came to the amendment and recodification of criminal laws in accordance with the principle of precaution, where potential offender in cyberspace must also be sufficiently clearly warned with adequate predictability that certain practices are not tolerated.

Law is seen territorially; geographical boundaries divide the territory in which there are different jurisdictions. State may exercise jurisdiction only in principle in its own territory. The principle of territoriality, however, has a leading role. The offense is then possible to prosecute not only where it was committed, but also where their consequences occurred. It is therefore not ruled out the possibility of prosecuting an offender on the territory of several countries. The question, therefore, is a place of committing a crime in cybercrime, typical negotiations with an international element, which is cyberspace. It is specific unlimited space with the disregard to the

boundaries of states, space for new illegal activities or new ways of committing the existing ones.

To effectivelyprosecutecybercriminalitythere isnecessityformultilateral internationalcooperationwith a view toregulatecertainsociallyharmfulconduct,methods oftheir punishment, which seems to bean essentialway how toovercome thebarriers ofnational jurisdiction. Effortsto harmonize, however, are not without difficulty, because of the point of viewof differentattitudes tothe regulation ofspecific individualconducts. Evenin the event ofa finding of a solution inthe form ofinternational documents,it may occur their differentapplicationdue todifferent legalcultures.

3 Conclusion

Today's advanced society is almost completely interconnected and interrelated. This is mainly due to the growing availability of means of communication; another reason is the ever increasing technological sophistication of their connection. The primary role is played by the Internet offering ever faster, cheaper and more versatile linkage of its individual elements. This allows an obtaining and providing of information without territorial, content, and quantitative restrictions.

Technological advancements that information area is experiencing are unusually dynamic and we can say hardly controllable. The benefits of this progress go hand in hand with disadvantages. The question therefore arises whether the proportion between the benefits of information and communications technologies and their abuse does not remain the same and does not change only the quantitative range. Unfortunately, the answer cannot be found easily, since cyberspace is changing every moment and it is hard to predict what direction it is going. It is closely related to the huge **expansion of cybercriminality**.

A certain way of combating this type of crime will be an introduction of the most efficient measures to minimize the risks. Cyber security deals with this measures, emphasizes a protection against unauthorized tampering with computer systems, data, secure communication and data transmission and other security aspects.

Despite all precautions, it should be noted that all technology has been created by man and still has not been invented safety feature that would be impossible to circumvent. Whether we will apply all security, legal, educational, and other measures we must realize that an essential element of a progress and at the same timean abuse of all achievements of modern information society is a natural person itself. There will therefore be necessary to start and to realize the danger and the possible impacts of the seemingly innocuous activities such as computer work.

The fight against cyber criminality must be fought on many levels, from which the most important thing for us will be sufficiently effective legal regulation with the possibility of enforcing behavior at national and international level, especially because of its cross-border operations.

4 References

1. WEBSTER, F. *Theories of the information society*. 2nd ed. London: Routledge, 2002, 304 pp. International library of sociology. ISBN 04-152-8201-2.
2. Council of Europe Convention no. 185 dated 23 November 2001 on cyber (computer) crime. Also available from the Web: http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm,
3. SMEJKAL, V., SOKOL, T., VLČEK, M. Computer Law. Prague: C. H. Beck, 1995, p. 220.
4. Wall, DS Cybercrime: The Transformation of Crime in the Information Age. Policy Press, 2007.
5. POLČÁK, R. Grivna. T. *Cybercrime and the law.* Ed. 1. Praha: Auditorium, 2008, 220 pp. ISBN 978-80-903786-7-4.
6. Ibid
7. VOLOVECKÝ, P. Conference on Advances in criminology: Proceedings of the International Conference held on 24 to 25 September 2008. Ed. 1. Praha: Czech Republic Police Academy, 2008, 1 CD-ROM. ISBN 978-80-7251-290-4.
8. Jirovský, V. Cyber-crime: not only about hacking, cracking, viruses and Trojan horses without secrets. 1st ed. Praha: Grada, 2007, 284 p. ISBN 978-80-247-1561-2.