DE GRUYTER OPEN

DOI: 10.1515/aet-2017-0010

PRELIMINARY REPORT

Acta Economica Et Turistica

Nikola Protrka
Kristijan Marić
Mihael Plećaš

CHALLENGES AND ASPECTS OF CYBER SECURITY OF THE REPUBLIC OF CROATIA

ABSTRACT: The development of the information and communication technology (ICT), regardless of its many advantages, unfortunately has its disadvantage – the abuse of the cyberworld. The global character of cyberspace is specific in terms of national legislation and its view of specificities. Some countries adopted the recommendation of the Convention on Cybercrime of the Council of Europe (Official Gazette NN-MU 9/02, 4/04) and amended their national legislation, whereas others kept implementing their criminal law solutions, which are outdated and cannot reach the level of this type of criminal offences. Consequently, governments are inclined to cooperate and exchange information about this type of crime due to the fact that the criminal offender may be anywhere, and the offence itself can take place at a great distance from the offender. In September 2015, the government of the Republic of Croatia adopted the National Cyber Security Strategy and the Action Plan for the Implementation of the National Cyber Security Strategy, the first all-encompassing strategy of the Republic of Croatia on cyber security. The paper also focuses on the role of the Police College in the Action Plan for the Implementation of the National Cyber Security Strategy.

KEY WORDS: cyber security, strategy, Convention, crime, international cooperation

Nikola Protrka, *univ. spec. inf., Police College in Zagreb, Croatia* **e-mail:** nprotrka@fkz.hr

Kristijan Marić, *mag. rel. int. et dipl., Libertas International University, Zagreb, Croatia* **e-mail:** kmaric@libertas.hr

Mihael Plećaš, *mag. ing., Libertas International University, Zagreb, Croatia* **e-mail:** mplecas@libertas.hr

INTRODUCTION

Although the official term used in Croatian language is computer crime, the term cybercrime is also commonly used. The Croatian word for computer has strong associations with the processing of certain mathematical operations and is thus closer to mathematics-computing than the information system. This is also one of the reasons why the English word "computer" has become commonplace in verbal expression.[1] Due to the accepted legal terms for this type of criminal offences the Croatian word for computer and computer crimes is used in the Criminal Code of the Republic of Croatia.[2]

There is a wide array of activities that are considered to be cybercrimes: unauthorised data access or illegal exchange of data and software code, unauthorised or illegal use of applications, software piracy, viruses, compromising computer devices (DDoS attacks), physical destruction of computer and communication devices, etc.

In today's world, modern society largely depends on smooth functioning of information and communication systems which are used for managing all the key systems such as the police, the army, the traffic, the supply system and other services as well as the critical national infrastructure. Since all these systems are increasingly being interconnected, the danger of these systems being attacked is also increasing. A wide availability of technology enables increased automation of attacks and the use of sophisticated tools for attacking. The development of ICT, with all its benefits, unfortunately has a resulting negative side – cybercrime.[3]

Due to different approaches there is not one term for crimes related to computer and information-communication technology. Several terms are currently in use, which are not mutually exclusive, such as cybercrime, computer crime and high-tech crime. All these terms are related to the English language and attempts to translate the English names and terms into other languages are often related to the inability to come up with a literal yet acceptable translation, which would be acceptable concurrently from the lexical, grammatical and professional perspectives.[4]

Convention on Cybercrime has introduced the term "cybercrime" in the daily language of the legal profession, which has taken huge steps in the co-operation of signatory states in combating cybercrime, while the National Strategy for Cyber Security and the corresponding action plan define and describe areas of information technology that need to be protected.

CONVENTION ON CYBER CRIME

Convention on Cybercrime was adopted by the Council of Europe, which is the oldest European organisation based in Strasbourg. It currently comprises 47 member states (all European countries except Belarus), and its main aim is to strengthen the collaboration and unity on the European continent by promoting human rights and fundamental freedoms as well as democracy and the rule of law. Alongside these three key pillars representing its fundamental values, the Council of Europe also deals with a number of specific social issues, such as social exclusion, racial, national and other intolerance, human trafficking, violence against women, children's rights, bioethics, terrorism, protection of cultural and natural heritage and other contemporary challenges of the European societies. On May 1949 the Council of Europe was founded in London by ten European countries in an attempt to strengthen democracy, the rule of law and the protection of human rights on the European continent. The Council of Europe has thus become the chief political forum for continuous dialogue and co-operation with countries of Eastern and Western Europe that have chosen the democratic form of running their countries.[5]

Convention on Cybercrime (hereinafter: Convention) is the most comprehensive European document on all crimes related to cybercrime.[6]

The Convention is the first international agreement on crimes committed on the Internet and other computer networks, which specifically regulates offences such as copyright infringement, computer and computer network frauds, child pornography on the computer or computer network and computer network security breach. The Convention also includes a number of authorisations and procedures such as computer network search and computer data interception. Its main objective, as stated in the preamble, is to continue developing joint criminal policies aimed at the protection of the society from cybercrime, especially by adopting appropriate legislation and strengthening international co-operation.[7]

Daily integration of information and telecommunication technology and their interdependence provide opportunities for abusing both, so the term "computer crime" is too narrow and thus the broader term "cybercrime" is used both in the Convention and in the daily talk.

The term "cybercrime" has been widely accepted, but three is still no generally accepted definition despite all efforts made by the profession worldwide to define this term as well as its content and scope. The closest definition among professionals says that cybercrime comprises all offences committed within cyberspace with the aid of or on the very information and telecommunication technology that makes its infrastructure.

With its global reach, openness and today's wide availability, the Internet as the infrastructure of cyberspace is becoming the source of misuse, and competing with cybercrime requires tight international co-operation. As there has been no such co-operation before or it has been unorganised and sporadic, in 1997 the Council of Europe founded a special committee, Committee of Experts on Crime in Cyberspace, whose task is to assess the situation and start working on international instruments for combating crime in cyberspace.[8]

The draft of the Convention was first introduced to the public at the end of 2000. It stipulates that signatory states introduce provisions into their national legislations that are necessary for the prosecution of perpetrators of crimes committed in the area of computer data and systems (affecting confidentiality, integrity and availability), crimes related to computers and related devices, the contents on CDs and infringement of copyright and other related rights. Solutions have been adopted that relate to the process part of the procedure related to the search and evidence provision, investigators' licences and obligations of service providers for Internet access.

The Convention was adopted by the Council of Europe on November 23, 2001 in Budapest and was presented as an international legal document regulating problems associated with the use and transfer of information and data through information and telecommunication systems. It came into force on July 1, 2004.

The list of 49 countries that have signed and ratified the Convention with the date of enforcement has been published by the Council of Europe on their web sites.[9]

The Convention has been ratified, but not signed by the following non-member states: Canada, Japan, South Africa and the United States of America.

The Convention consists of four chapters: the first chapter contains the list of crimes as well as the definitions of key terms given for the purpose of this Convention, the second contains provisions that the signatory states have to implement in their legislations, the third chapter is related to the mechanisms of international co-operation and mutual aid and the fourth contains final provisions.

The first part of the Convention defines certain terms that are mentioned, e.g. the term *computer system* means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

The term *computer data* means any representation of facts, information or concepts in a form suitable for processing in a computer system, including

the software that can make the computer system perform a certain function. The term *service provider* means any public or private entity that allows the users of their services to communicate by means of a computer system and any other entity which processes or stores computer data on behalf of such a communication service or its users.[10]

The term *traffic data* means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, its destination, route, time, date, size, duration or the type of underlying service. All the above definitions are rather broad and general.

Although in its Criminal Code, the Republic of Croatia recognised cybercrime as *corruption and use of other people's data* as early as in 1997, it was necessary to elaborate legal regulations due to the obvious technological advances and thus the related crimes. Commitments undertaken by signing the Convention referred to the amendments in the Criminal Code, which was supposed to incorporate new crimes – illegal access, illegal data interception and interference, system interference; system interference, device misuse, computer counterfeiting, computer fraud, offences related to child pornography and copyright, cases where computers and the Internet are used for criminal activities, as well as incrimination of offences involving the attempt, aiding and abetting all the above criminal activities. Apart from other process activities of the signatory states, the Convention also defines forms of cooperation of signatory states, i.e. parties.

NATIONAL STRATEGY OF CYBER SECURITY

On September 29, 2015 the Republic of Croatia adopted the National Strategy of Cyber Security, which is the first comprehensive strategy in the field of cyber security in Croatia, and the Action Plan for its implementation. Therefore, even when looking at information technologies in their narrowest sense, the emergence of the Internet in the private sphere in the late 1990s, or even through its development and popularisation in the first decade of the 21st century, as mentioned in the strategy itself, the term "cybernetics" was introduced in the ratification of the Convention on Cybercrime, showing when the issue of cyber security was recognised. Therefore, it may be concluded, with the assessment being very optimistic, that the above strategy was adopted at least 13 years, and realistically speaking even more, after the actual emergence of the issue of cyber security. Given the very nature and rate of IT development, both in terms of software and hardware, which was recognised in the strategy itself, where it says that: "technological development has not been as dynamic and comprehensive in any field other than that of communication and information technology", it is no news to anyone who is familiar with these technologies at least at the information level, that these optimistic 13 years in this field represent a whole eternity.

As this strategy is the first comprehensive strategy in the field of cyber security in the Republic of Croatia, it virtually provides the basis and it is important to first recognise key areas of use and problems the above mentioned technologies are facing. Also, it is necessary to find solutions to these problems at the same time dealing with a plethora of new, daily innovations, which give rise to new problems from the security point of view. Nevertheless, this programme is a positive move in the field of cyber security, as today these technologies are part of every aspect of daily life. The following chapters consider the principles, objectives, social sectors and forms of co-operation, their areas and links from the aspect of cyber security and the implementation of the plans stated in the strategy.

The strategy defines the links of the areas considered to be shared by everybody or the majority. They are:

1. Data protection;
2. Technical co-ordination in the processing of computer security incidents
3. International cooperation and
4. Education, research, development and raised awareness of security in cyberspace

Their definition is essential to the improvement and more efficient achievement of aims and measures in the areas of cyber security and special objectives essential to the enhancement of security have also been defined. In accordance with the Action plan for the implementation of the National Strategy of Cyber Security, the Police Academy has assumed the role of educating, researching and raising the awareness of cyberspace security as one of its measures, which is shown in Table 1.

INSTITUTIONAL CO-OPERATION

The character of cybercrime is specific to certain countries due to their national legislation, which we covered in previous chapters, and their perception of the specificity. Some countries have adopted the recommendations of the Convention and have modified their national legislations, whereas others maintained the legal solutions that do not keep pace with the present time and the scope of this type of crime.

Subsequently, countries are encouraged to co-operate and exchange information on this type of crime as the perpetrator may be anywhere and the offence may have been committed far from the perpetrator.

International co-operation has thus become essential and the responses can be seen through a number of specialists, regional, multinational and global organisations:[11]

1. United Nations

2. Interpol

3. Europol

4. European Centre for Cybercrime – EC3

TABLE 1. MEASURES FOR EDUCATION, RESEARCH, DEVELOPMENT AND RAISING AWARENESS OF CYBER SPACE SECURITY

MEASURE I.1.11 Permanent professional training of police officials in the area of information security and cybercrime that will be carried out by a specialised training academy and other organisational units of the Ministry of the Interior (MUP) in accordance with its competences, and the harmonisation of the programme will be implemented in co-operation with professional competent authorities.	
Implementer	Ministry of the Interior (MUP)
Co-implementer	Office of the National Security Council (UVNS), Information Systems Security Bureau (ZSIS), Croatian National Computer Emergency Response Team (National CERT)
Beginning of the implementation	Upon the adoption of the Strategy
End of the implementation	Ongoing
Additional funding (YES/NO)	NO
Implementation indicators	Defined plan of how specialist knowledge is to be acquired. Number of implemented professional training programmes.

Source: Action plan for the implementation of the National Strategy of Cyber security

CYBER RISK INSURANCE POLICY

The latest Allianz report entitled "A Guide to Cyber Risk: Managing The Impact of Increasing Interconnectivity" suggests that cybercrime risks have evolved and that they represent much more than database theft, invasion of privacy or tarnishing the company's reputation. Companies have to be prepared for the new generation of cyber risks, which change rapidly, threatening companies with huge damages, disruption of business operation and even possible losses of catastrophic proportions. Cybercrime insurance is not a substitute for robust Internet technology (hereinafter: IT) security, but it represents the second line of defence the purpose of which is to alleviate the consequences of cyber-attacks. Allianz Global Corporate & Specialty has recorded an increased need for this type of insurance and wishes to help their clients to understand and respond better to the increasing exposure to cybercrime risks.[12]

However, it should be emphasised that the protection from cybercrime is primarily expected at the micro location, in terms of IT security, but also through the behaviour of each Internet user. This is particularly important for achieving high levels of cybercrime protection. Besides IT infrastructure, the first line of defence involves protecting personal information and refraining from sharing it online. Also, it is important to use different passwords, which need to be a combination of small and capital letters and numbers. The use of antivirus software is mandatory, as well as its regular updating. Apart from the above, protection from cybercrime is possible through taking out an insurance policy, which represents a new fast-growing trend in the market.

Our vulnerability is also increased by the ever growing connection between devices in daily use and increasing reliance on technology and data in real time both on a personal and corporate level, which is known as Internet of Things. It is estimated that by 2020 a billion devices will have been connected to the Internet with 50 billion devices exchanging information daily. Industrial control systems (ICS), which had mostly been created before cyber security became a problem, represent another huge headache. An attack on ICS may result in a fire, explosion and disruption of business operation. In 2014 there were 245 cyber-attacks on ICS, mostly in the energy sector. Allianz also estimates that the scope of cyber insurance will have to increase in order to provide stronger and broader coverage, including that for disrupting business operation. Telecommunication companies, retail chains, power plants, the utilities and transportation sector and financial institutions have shown increasing interest in cyber insurance policies. The premium for cyber insurance will globally grow from the current $2 billion to over $20 billion in the next ten years, with an average annual growth rate of 20 per cent.[13]

The development of Internet technologies, as any other development, has many advantages, but there are always some drawbacks, too, in this case it is cybercrime. As the number of cyber-attacks increases, so does the need for the development of cyber insurance policies, in accordance with the demand. Currently cyber insurance policies are taken out by legal entities (companies), which increasingly use insurance as protection from cyber-attack risks. This is understandable considering the potential damage that a cyber-attack may inflict on the business. Also, it should be emphasised that the "Internet of Things" trends lead to increased exposure of individuals to cybercrime. Today a large number of devices used by individuals in their homes are connected to the Internet, which means that opportunities for cyber-attack are present all the time. Insurance companies still have not developed a sufficient number of products they could offer to individuals as cyber insurance policies, which is definitely a business segment that will experience growth in the near future.

Indeed, in the last 15 years the market for cybercrime risk insurance has increased worldwide from about 10 insurers to about 50 insurance

companies offering specific risk insurance policies. According to Moody's, this year the gross value of sold premiums was $2.75 billion (compared to $2 billion dollars last year). Other insurers, on the other hand, provide additional coverage related to cybercrime risk on insurance policies for general commercial liability or policies covering several risks (so-called multi-peril policies). It should be noted that the USA holds the largest part of the market, about two billion premiums, with about 35 insurers who provide specific cyber risk insurance policies. PricewaterhouseCoopers estimates that by 2020 the market for cyber risk insurance will have increased to 7.5 billion dollars in premiums, and some believe that this growth will be even faster. However, large retailers and companies providing health services, financial services and caterers actually have increasing problems to get governed as insurers have an increasingly difficult time estimating these risks, says Kevin Kalinich, global practice leader for cyber risk insurance at Aon Risk Solutions.[14]

Despite the growth of the cyber risk insurance market worldwide, both in terms of the number of insurers and in the number of policy holders, risk estimation by insurers is still extremely demanding, which makes it increasingly difficult for potential clients to get cyber risk insurance. This needs to change as fast as possible by insurance companies adapting to trends. They have to change their offer in accordance with market conditions in order to timely ensure their market position in the future, when cyber risk insurance will be one of the main segments in the insurance market.

Apart from legal entities (companies), which have, to a smaller extent, taken out cyber risk insurance policies, it is expected that individuals, too, will start buying these policies. This is supported by the fact that the majority of the world's population owns a mobile phone and a computer, as well as other devices which are connected to the Internet. Besides devices, applications, which may serve as a possible channel for cyber-attack, are increasingly used. Applications for making payments and handling bank accounts are particularly vulnerable and may become targets of cyber-attacks, which will be a growing trend in the future. In view of all this, it may be concluded that cyber risk policies will one day reach the level of the currently best-selling insurance policies, although at this moment human life, which is increasingly taking place online, is still not adequately protected.

CONCLUSION

Although many countries and institutions have recognised the cybercrime problem, there is still room for improving their co-operation in discovering and preventing cybercrimes.

When speaking about co-operation we should emphasise the fact that the largest number of servers that store data on potential perpetrators of cybercrimes are still in the USA, and that inquiries of countries that are members of the Interpol, which investigates such crimes, are directed towards the country where such a server is located.

The latest example of international co-operation is the international co-operation of Croatian and American institutions in fighting crime and arresting perpetrators. A good example is the extradition to the American authorities of the Ukrainian citizen Sergei Litvinentko, who was arrested in Split on August 25, 2012 and was extradited in January 10, 2014, when he was apprehended by the USA under the supervision of the US Marshals Service.

Sergei Litvinenko is a Ukrainian citizen for whom an international arrest warrant was issued for cybercrimes and financial frauds committed in several countries, the damage exceeding 50 million dollars.

This international co-operation serves as an example of collaboration on finding and arresting individuals accused of cybercrimes. The more the society relies on technology the more important the co-operation on fighting cybercrime becomes.[15]

As one of the ways of protecting electronic data, and thus security, various insurance companies have started offering cyber risk insurance policies. Nevertheless, the market has not recognised the importance of this yet, which will certainly change in the future, giving rise to further investigation of this topic.

REFERENCES

[1] This claim can be supported by quotations from the Dictionary of Foreign Words (v. Anić, V. – Goldstein, I., *Rječnik stranih riječi*, Zagreb, 2004, p. 710), where the computer is denoted as an electronic device which receives, processes, stores and retrieves stored information, does mathematical and logical operations in a short time and presents the obtained results.

[2] In the Croatian Encyclopaedic Dictionary (V. Anić, V., Brozović Rončević, D., Cikota, Lj., Goldstein, I., Goldstein, S., Jojić, Lj., Matasović, R., Pranjković, I., *Hrvatski enciklopedijski rječnik*, Novi Liber, Zagreb, 2004, p. 1085) the term "računalo" is described as a machine or device used for computing and processing dana expressed in figures, while the term "osobno računalo" (Personal Computer; PC) is denoted as a computer for personal use.

[3] Dragičević, D., „Novi izazovi kibernetičkog kriminala", *Hrvatska pravna revija*, srpanj-kolovoz 2005, p. 150.

[4] Škrtić, D., *Kaznenopravna zaštita informatičkih sadržaja*, Sveučilište u Zagrebu, Pravni fakultet, 2011, p. 85.

[5] Ministarstvo vanjskih i europskih poslova Republike Hrvatske, http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/vijece-europe/ retrieved 29/8/2015.

[6] Konvencija o kibernetičkom kriminalu Vijeća Europe, *Narodne novine* – Međunarodni ugovori 9/02, 4/04.

[7] Relevant data on the conventions of the Council of Europe can be found on: http://conventions.coe.int retrieved 29/8/2015.

[8] Agenda of the Council of Europe https://wcd.coe.int/ViewDoc.jsp?id=410081&Site=COE retrieved 29/8/2016.

[9] Situation on August 29, 2015.

[10] Convention, Article 1 – Definitions, In this Convention: a. the term *computer system* means any device or a group of interconnected or related devices one or more of which, pursuant to a program, performs automatic processing of data; b. the term *computer data* means any representation of facts, information or concepts in a form suitable for processing in a computer system, including the software that can make the computer system perform a certain; c. the term *service provider* means any public or private entity that allows the users of their services to communicate by means of a computer system and any other entity which processes or stores computer data on behalf of such a communication service or its users.; d. the term *traffic data* means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, its destination, route, time, date, size, duration or the type of underlying service.

[11] Škrtić, D., *Kaznenopravna zaštita informatičkih sadržaja*, Zagreb, Pravni fakultet Sveučilišta u Zagrebu, 2011, p. 8.

[12] http://www.svijetosiguranja.eu/hr/novosti/odrzana-2.-medunarodna-konferencija-cyber-risk,18766.html, retrieved 15/9/2016.

[13] Ibid.

[14] http://www.svijetosiguranja.eu/hr/clanak/2015/12/trziste-osiguranja-cyber-rizika-dramaticno-raste,527,17068.html, retrieved 10/9/2016.

[15] Ministry of the Interior of the Republic of Croatia, http://mup.hr/177100.aspx, retrieved 20/8/2016.

LITERATURE

DRAGIČEVIĆ, D. (2005), "Novi izazovi kibernetičkog kriminala". *Hrvatska pravna revija*, srpanj-kolovoz 2005.

IT Risk, http://www.svijetosiguranja.eu/hr/novosti/odrzana-2.-medunarodna-konferencija-cyber-risk,18766.html, retrieved 15/9/2016

(2002) Konvencija o kibernetičkom kriminalitetu Vijeća Europe. *Narodne novine* –Međunarodni ugovori 9/02, 4/04

KUČAN, B. (2014), "Europski centar za kibernetički kriminal". Časopis *Mreža*, 02/2014, http://www.bug.hr/mreza/tekst/europski-centar-kiberneticki-kriminal/96324.aspx, retrieved 29/8/2015

Ministarstvo unutarnjih poslova Republike Hrvatske, http://mup.hr/177100.aspx, retrieved 20/8/2016

(2015) Nacionalna strategija kibernetičke sigurnosti. *Narodne novine*, 108/2015

Svijet Osiguranja, http://www.svijetosiguranja.eu/hr/clanak/2015/12/trziste-osiguranja-cyber-rizika-dramaticno-raste,527,17068.html, retrieved 10/9/2016

ŠKRTIĆ, D. (2011), "Kaznenopravna zaštita informatičkih sadržaja". Sveučilište u Zagrebu, Pravni fakultet, 2011.