AARMS Vol. 17, No. 3 (2018) 19–46. **10.32565/aarms.2018.3.2**

Combating Cyber Crime[1]

Krunoslav ANTOLIŠ,[2] Ivančica VARJAČIĆ,[3] Mario JELENSKI[4]

Life in a modern society is determined by strategic drivers, the most important of which are the Internet and Information and Communication Technology (ICT). Their use is one that contributes to global development and enables it to be balanced globally. The sustainability of this development is directly dependent on the degree of Internet misuse and the misuse of ICT. That is why we are discussing computer criminality through the example of Croatia. In the second part, we analyse the misuse of new ICT and the ways and possibilities of legitimate opposition to ICT abuses.

Keywords: *Internet, ICT, abuse, misuse, cyber crime*

Introduction

New information technologies are unavoidable factors in the modern world changing it in technological but also in communicological sense. According to Antoliš: "both aspects of the changes, apart from new possibilities, bring along vulnerabilities, which must not be disregarded." [3: 121] The mentioned vulnerabilities open the doors wide to computer crime characterized by fast-spreading, a variety of forms aimed at material and non-material benefits, with perpetrators having technical knowledge, going global and by a high "dark figure of crime". An inseparable term related to computer crime is digital evidence which combines text, images, audio and video recordings. Information vulnerabilities have a direct impact on the security of modern economic systems where ICT is becoming a dominating information and communication platform. It is not only terrorists that we should be concerned about when thinking of the security of economic entities but also organized and economic crime, competitive states and companies, different hackers and even those who, due to various social and economic reasons, live on the margins of modern society. Of course, none of the mentioned categories is immune to committing terrorist acts and that is why, for prevention reasons, all of them should be observed and prevented in accordance with security estimates according to the views of Antoliš and Varjačić. [2: 231]

This paper also deals with the reasons why Darknet has become a safe haven for all those who want to protect their activities from the eyes of others. We are primarily interested in those who use this Darknet protection to deal with illegal activities such as organized crime, violent extremism, terrorism, radicalization, etc. But, to be able to devote this analysis to the abuses

---

1 All statements made in this article are solely those of the author and in no way reflect the official position or policies of the Republic of Croatia, the Croat Parliament, the Croat Government or Ministry of the Interior.

2 Ph.D., assistant professor, Ministry of the Interior of the Republic of Croatia, Police Academy, Police College in Zagreb; e-mail: kantolis@fkz.hr

3 Crime Investigation Specialist, Ministry of the Interior of the Republic of Croatia; e-mail: ivarjacic@mup.hr

4 Professional Bachelor of Criminal Investigation, Ministry of the Interior of the Republic of Croatia; e-mail: mario.jelenski@gmail.com

of Darknet, we must first understand how Darknet works for which this article should serve as a guidance. After that, we will point out the problems related to the control of the Darknet's work, especially those that are technology-related. Then we will analyse the existing legal norms available to members of the security system for legitimate monitoring, interception and analysis of Darknet. The conclusion of the paper deals with the collection and processing of digital evidence in order to prevent and prosecute perpetrators of criminal offenses.

The evolving strategic environment and strategic drivers of change determine the life of the contemporary man of the 21st century. Strategic drivers need to identify the most prominent ones, such as globalization, political geometry, demographic changes, climate change and the impact of new bio and nanotechnologies, as well as ICT and the Internet.

In September 2017 the European Cybercrime Centre (EC3) at Europol conducted Internet Organized Crime Threat Assessment (IOCTA) to inform the governmental bodies of the European police to shift its focus to cybercrime. They have set four top crime priorities:

- cyber-dependent crime;
- child sexual exploitation online;
- payment frauds;
- online criminal markets.

A cyber-dependent crime includes crimes that can only be committed using communication and information infrastructure (computers, servers, networks) and poses a real threat to the survival of modern society. Cyber-dependent crimes represent any threat to the loss of availability and integrity of the communication and information infrastructure, as well as any threat to the loss of integrity, availability and confidentiality of data in the cyber space. Cyber-dependent crimes can be divided into either negligent or malicious action of a user. In addition to these critical threats to cybernetic security, there are various other threats that affect human rights, identity of a person, intellectual property rights and other criminal offenses that pose a threat to the normal behaviour of users in cyberspace.

For conducting cyber-dependent crimes, most commonly, malicious computer content is used that expands through the existing communication and information infrastructure. Malicious content can be divided into four categories:

- spam;
- hoax;
- phishing;
- malware.

Spam is a malicious e-mail that aims to promote advertising content (mostly pornographic) or is a means of spreading malicious links. For his dissemination, he uses a variety of web sites, chat rooms, or blogs to collect email addresses and ultimately send malicious content. Unlike spam, hoax is a form of e-mail that does not cause harm, but only serves to spread untruthful content via e-mail or the Internet.

Phishing is a real criminal product through exploiting the vagueness and thoughtlessness of the user to collect key and secret personal information (such as username, password and other personal information) for financial gain. In phishing, the perpetrator uses a false identity by presenting itself as a financial institution that the user is a member of and asks him to update his security accreditation after which the perpetrator gains access to the victim's

financial services. There are a variety of types of phishing e-mails, from the simplest of which e-mails require access to the data, to the complicated approaches that send e-mails to sites that are fake as financial institutions sites.

Malware is a collective name for all types of malicious content whose purpose is to gain access to the computer system and data of users without their knowledge. Various viruses, worms, Trojan horses, ransomware programs, rootkits, spyware are included in the malware. Malware is closely related to the cybernetic crime itself because it is through it that it is realized. Once the perpetrator gets access to the desired computer system, he uses it further to blackmail the user or for further attacks to the real target.

A subcategory of Malware called Ransomware is today in common use. It is a malicious content that consists of two types of malware: Trojan and cryptolocker. The Trojan uses different holes in the system to make it noticeably plugged into the cybernetic system and spread to other computers on the network. After the "insert" into the cybernetic system, a cryptolocker is triggered that encrypts the user's file and asks for the ransom to restore the file to the previous state.

The 21st Century Information Environment

The world of the 21st century is a world where the use of information communication technologies determines the lives of people and creates their perceptions of events at the global, regional and local level. The power of media has multiple implications for the conclusion and creation of images of the world we are living in. Many of these facts are ready to be used to create an acceptable view of the world to their particular interest on the public interest account to the benefit of others. Manipulation enabled by the wide availability of information communication technologies is visible on a daily basis and is present in the most influential media infrastructure of today's Internet. The Internet is full of misinformation, conspiracy theories, gossip, which are unstoppable and with great speed of dissemination currently available to the modern people. In this overload with Internet information, it is difficult to distinguish truth from lies, good from evil, because creators of constant information attack on modern people are skilful and determined in their own way. [15]

The influence of media on contemplating of contemporary people is based on the principle: "Almost by definition […] a war waged on live television is a war in which political and public relations considerations become inextricably bound up with military tactics and strategy […] how victory is won is almost as important as victory itself." [23]

The modern world is facing a number of risks, such as the abuse of new technologies, especially ICT and the Internet, Cyberwars, Cyberterrorism and Cyber riot, Security of Critical National Infrastructure, Intellectual Property in Cyber Space, Networks and Networked Information Thinking, Censorship in Cyber Environment, Neutrality in Cyber Space, Privacy (GDPR) and Anonymity in Cyber Space.

The use and abuse of the Internet resource, for example, occurs at every moment, at all levels: surface web, deep web and especially the Darknet. Each of the above levels of the Internet is recognized from the point of view of its opportunities that are targeted, used and/or abused. Of course, in the further development of technology and also in the development of the legal system and legal norms, it is necessary to work on the opening of the space of use

and the closure of the space for abuse. It is important and unambiguous that internationally recognized socially unacceptable forms of behaviour on the Internet should be punished, no matter what its level is.

Abuse on the Surface Web

The reasons why the surface Internet is interesting are numerous: decentralization of infrastructures, easy access and anonymity, globalization of the world public, fast communication, cheap maintenance and web application development, news making…

Abuse on the surface web has many forms, especially those committed by violent extremists and terrorists with goals such as:

- publicity and propaganda in the form of psychological war in the service of networking as well as recruiting and mobilization of violent extremists and terrorists through the Internet forums;
- data mining of the targets and the information exchange—for instance on IED i.e. improvised explosive devices and possibilities to provide needed equipment;
- fund raising and donations for violent extremists and terrorists, etc.;
- planning and coordination of violent extremist and terrorist activities—along with preserving secrecy by coding the messages and communications.

Evidence of these is a number of websites such as: *Islamist Website, Jihadi Website, Terrorist Blog, Terrorist Forum*, Jihadists use mobiles as propaganda tools, *A Jihadist's Course in the Art of Recruitment,* Abu 'Amr's handbook.

FBI Director James B. Comey said that terrorist groups are turning to encrypted communications. He also said that the Islamic State has attracted at least 21,000 English-speaking followers on the Twitter social media platform, bombarding them with incitements to violence.

When the Islamic State operatives encounter a potential recruit, Comey said, "we see them giving directions" to move to a mobile messaging app that is encrypted, he said. "And they disappear." [10]

Terrorists Abuse WhatsApp

London terror suspect Khalid Masood sent a WhatsApp message to an unknown person just before Sunday's attack that killed four people and injured dozens. The message's contents—and its intended recipient—cannot be accessed by police because the popular, Facebook-owned messaging service encoded them. [8]

It is the burgeoning of these secret, inaccessible corners of the Internet that worries law enforcement agencies, which have been talking for several years about the dangers posed by criminals and terrorists who can now "go dark" by using strong encryption.

FBI Director James Comey said "That is a shadow falling across our work." "The darkness is spreading through the whole room", he also said last week at a security conference at the University of Texas at Austin. [14]

Amber Rudd, Secretary of State for the Home Department of the UK said: "We need to make sure that organizations like WhatsApp—and there are plenty of others like that—don't provide a secret place for terrorists to communicate with each other." [14]

Terrorists' Love for Telegram

Terrorism and intelligence experts have known for years that the encrypted messaging application Telegram is now the "app of choice" for terrorists and specifically for ISIS. [12] The ISIS members behind the 2015 Paris attacks used Telegram to spread propaganda. ISIS also used the app to recruit the perpetrators of the Christmas market attack in Berlin last year and claim credit for the massacre. More recently, a Turkish prosecutor found that the shooter behind the New Year's Eve attack at the Reina nightclub in Istanbul used Telegram to receive directions for it from an ISIS leader in Raqqa.

The Croatian Legal Framework for Information Security

The National Security Council and the Office of the National Security Council is on the first place. We can say that the Office of the National Security Council is like a "National Security Authority" and it performs administrative and professional staffs for the National Security Council. The Office of the NSC is a central state-level information security body that coordinates the adoption and monitoring of the application of measures and standards of information security in Croatia. [21]

The next important agency is the Computer Emergency Response Team (CERT). It is a national body for prevention and protection against computer threats to the security of public systems in Croatia. CERT deals with incidents if one of the parties is in Croatian or in the .hr domain or in the Croatian IP area. It is a member of the Forum of Incident Response and Security Teams (FIRST) and working group TF-CSIRT. [22]

The Information Systems Security Bureau (ISSB; Croatian acronym is ZSIS) is the Office for Security of Information Systems, the central state body for performing tasks in the technical areas of information security of the state bodies of Croatia, which include information security systems standards, security accreditation of information systems, cryptomatic management used in the exchange of classified information and coordination of prevention answers to computer threats to security of information systems. Also, it is responsible for regulating the technical areas of security information system safety regulations and their ongoing alignment with international standards and recommendations, and participates in national standardization of information system security areas. Standards of technical information security systems apply to all state bodies, units of local and regional self-government and to legal entities with public authority that use classified and unclassified data within their scope.

Together with these bodies, internet investigations, information security protection and the fight against abuse and misuse of the internet is under the jurisdiction of the Ministry of the Interior and the Ministry of Defence, for which separate departments were established.

The operational body established in the Republic of Croatia for the purpose of supervising the telecommunications operators' services is the Telecommunications Surveillance Operative-

Technical Centre (OTC). The legislation enacted in 2006 which is still effective today determines two agencies: the Security-Intelligence Agency (Croatian acronym is SOA) and the Military Security-Intelligence Agency (VSOA), i.e. civilian and military with operations at home and abroad, and the Telecommunications Surveillance Operative-Technical Centre, which is in charge of activation and management of measures for the confidential surveillance of telecommunications services, activities and traffic.

The laws of the Republic of Croatia allow the surveillance and legitimate interception of the Internet by the security intelligence agencies (SOA and VSOA) and the police.

The legal basis for the handling of security intelligence agencies is the Law on Security and Intelligence System of the Republic of Croatia, July 5, 2006. [24]

For the application of secret data collection measures to security intelligence agencies, a warrant is required from a Supreme Court judge.

"Article 33.

First secret surveillance of telecommunication services, activities and traffic:

a) secret surveillance of communications facilities,
b) the surveillance of telecommunications traffic data,
c) the surveillance of international telecommunications connections, […]

Third secret surveillance and technical recording of interior facilities, closed spaces and objects." [24]

Despite the capabilities and powers of the security services, the data and information they collect are not digital evidence for court proceedings in the Republic of Croatia. Even when they are based on suspicion that they indicate the perpetration of criminal offences for which they are prosecuted ex officio, and when the law is obliged to collect the collected data and information to the State Attorney's Office.

Since the police action must be proportional to threats, it usually goes hand in hand with actions that less distort the constitutionally guaranteed human rights and freedoms.

Such is, for example, the authority in Article 68. (the Act about police duties and powers) which enables them: "To reduce the risk, violence, prevention and detection of crimes for which the public prosecution, the police officer may from telecommunications service providers seek to: verify identity, duration and frequency of contact of certain telecommunication address." [24]

But when such measures are not enough then the ones that can be more effective are taken. If in the police surveillance and legitimate interception of data on the Internet the police are acting, then its powers come from the Code of Criminal Procedure, from October 11, 2011. [25] Special Collection of Evidence (Investigating judge-warrant):

"Article 332.

1) surveillance and technical recording of telephone conversations and other communications to remote,
2) the interception, collection and recording of computer data,
3) enter the premises for the purpose of conducting surveillance and technical recording of premises,
4) secret surveillance and technical recording of individuals and objects in dealing with the work of police officers in cases where there are reasonable grounds for suspecting that the abuse of Darknet is important to deter a perpetrator of a criminal offence in

committing a criminal offence. For these reasons, the legislator freed the police officer or civil servant in civil suit from the obligation of presentation." [25]

Law on police businesses and officials, June 30, 2009. [26]

"Article 17.

(1) A civil servant in a civilian suit shall be presented before the beginning of the application of police authority by displaying the official badge and the official identity card.

(2) A police officer in the chamber shall be presented by displaying the official badge and the official identification card at the request of the person to whom the police authority shall apply.

(3) Exceptionally, a police officer shall not be represented in the manner prescribed in paragraphs 1 and 2 of this Article if the circumstances of the application of police powers indicate that it could jeopardize the attainment of its objective.

(4) As soon as the circumstances referred to in paragraph 3 of this Article cease, the police officer shall be presented in the manner prescribed in paragraphs 1 and 2 of this Article.

(5) The provisions of paragraphs 1 to 4 of this Article shall not apply to the conduct of a police officer who undertakes concealed police actions: observation, escort, trap or, which under special law undertakes special evidence actions: monitoring and technical recording of telephone conversations and other remote communications, interception, collection and recording of computer data, entrance to the premises for supervision, secretly tracing and technical recording of persons and subjects and technical recording of rooms, use covert investigators and dependents, simulated sale and purchase of items and simulated bidding and simulated receipt of bills, providing simulated business services or concluding simulated legal transactions, supervised transportation and delivery of criminal offences." [26]

As police powers end up within the borders of a national territory, i.e. state, police actions that cross the state border are always possible to be questioned from the point of view of legality. Since the vast majority of police researches in the virtual environment, i.e. on the Internet, are such that they cross the boundaries of the national territory, they are legitimate only if we can legitimize them by international police co-operation. It is, therefore, important to rely on cooperation with, for example, Europol and/or Interpol in all such police proceedings.

Analysis of Computer Crime – Case Study Republic of Croatia (2004–2013)

The investigation of computer crimes is complex and demands a wide knowledge of technical distinctions between new technologies, primarily due to seeking for different types of evidence in digital form. There is a number of different definitions for computer crime. According to Dragičević: "If the term crime represents totality of criminal behaviour in a particular area within a certain period of time, then computer crime can be defined as totality of criminal offences committed on a computer system or by exploiting it in a certain field within a certain period of time." [6: 112] But according to Bača computer crime is: "A form of criminal behaviour of exploiting computer and information technology by using a computer as a tool or target to perpetrate criminal offence with relevant consequences according to criminal legislation." [4: 22] An inseparable term related to computer crime is digital evidence defined by the Criminal

Procedure Act of the Republic of Croatia (OG no. 152/08, 76/09, 80/11,121/11, 91/12,143/12, 53/13,145/13) as follows: "…electronic (digital) evidence is a data which is, as evidence in electronic (digital) form, obtained as stipulated by this Act." Digital evidence can also be explained as "any computer data which can either prove that criminal offence is committed or indicate a connection between" a criminal offence and an injured party, or "connection between criminal offence and its perpetrator" according to Protrka. [11: 2] Digital evidence combines text, images, audio and video recordings. We can only say that the investigation of a computer crime is very complex to carry out and that requires better knowledge of technical distinctions than the investigation of any other criminal offence, primarily due to its seeking for different types of evidence (electronic, i.e. electromagnetic type of evidence) as it deals with electronic equipment. [4]

This paper deals with computer crime in the Republic of Croatia for the period between 2004–2013 and analyses statistical indicators of computer crime based on the reports of the Ministry of the Interior on criminal offences referring to computer crimes and its perpetrators for the period between 2010–2013, according to K. Antoliš, I. Varjačić. [2] [13] The assumption is that the "dark figure of crime" of the reported development of computer crime is not connected with the increase in all reported criminal offences in the Republic of Croatia and that the computer crime rate is outstandingly low in all criminal offences in the Republic of Croatia. With regard to computer crime perpetrators, the assumption is that they are mostly males, the citizens of the RC, with a wide age span, and that on average, one perpetrator commits several criminal offences. Data analysis in this paper first represents data for the period between 2004 and 2012 and then for the year 2013, while for the period between 2004 and 2013 the data are united. There are two reasons for such data presentation, first, on 1 October 2004 Amendments to the Criminal Code harmonized with the Convention on Cybercrime entered into force introducing criminal offences related to computer crimes, and the second reason is that on 1 January 2013 the new Criminal Code entered into force in the Republic of Croatia.

Also, the analysis is carried out of the sentences pronounced to the perpetrators of computer crime in the RC according to the data of the Central Bureau of Statistics for the period 2009–2013; the year 2013 is analysed separately due to the new Criminal Code enforcement. It is assumed that the number of pronounced sentences is smaller in relation to the number of criminal offences for which the perpetrators are reported.

Computer Crime

Regarding the criminal law framework, it should be stressed that on 1 October 2004, the Amendments and Supplements to the Criminal Code were enforced. (Act on Amending and Supplementing the Criminal Code of the RC, OG no. 105/04) and that the data for 2004 include the period from 1 October 2004 to 31 December 2004. The mentioned Amendments to the Criminal Code define the following criminal offences: "Offences against the confidentiality, integrity and availability of computer data, programs or systems", "Offences related to child pornography on computer system or network", "Computer-related fraud".[5] Following that,

[5] See the complete legal description of offenses Act on Amendments to the Criminal Code, OG no. 105/04.

as mentioned in the introduction to this paper, on 1 January 2013 a "new" Criminal Code in the RC came into force (OG no. 125/11) in which criminal offences of cybercrime are separated in Chapter XXV. "Criminal offences against computer systems, programs and data", Article 266, "Illegal access"; Art. 267, "Computer system interference"; Art. 268, "Data interference"; Art. 269, "Illegal Interception"; Art. 270, "Computer-related forgery"; Art. 271, "Computer-related fraud"; Art. 272, "Misuse of devices", Art. 273, "Serious criminal offences against computer systems, programs and data".[6]

Looking nearly ten years back, we can see a development of computer crime in the RC. In the analysed period of time, the biggest number of the total reported criminal offences was recorded in 2010, while the analysis shows noticeable increase in each criminal offence in 2008, except for the criminal offences against Computer-related fraud, the highest number of which was reported in 2010 (903 criminal offences) making the biggest number of reported criminal offences in 2010.

The percentage of resolved criminal offences in 2004 and 2005 was 100%, with the smallest number of reported criminal offences in which 14 and 72 criminal offences were reported in 2004 and 2005, respectively. With the exception of these two years, the highest percentage of resolved offences was 97.3% in 2010, with the biggest number of reported offences. The average percentage of the resolved criminal offences analysed for the whole period of time was 93.64%, shown in Table 2. The number of reported, resolved and percentage of resolved criminal offences against computer crime in the RC for the period between 2004−2013 is given in Table 1.

Table 1. *Reported, resolved and percentage of resolved criminal offences of computer crime in the Republic of Croatia for the period between 2004−2013 according to the data of the Ministry of the Interior.* [19]

	Year									
	2004	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
Reported Criminal Offenses	14	72	109	174	653	367	1,002	863	631	707
Resolved Criminal Offenses	14	72	103	165	625	338	975	813	553	642
% Resolved	*100%*	*100%*	*94.5%*	*94.8%*	*95.7%*	*92.1%*	*97.3%*	*94.2%*	*87.6%*	*90.8%*

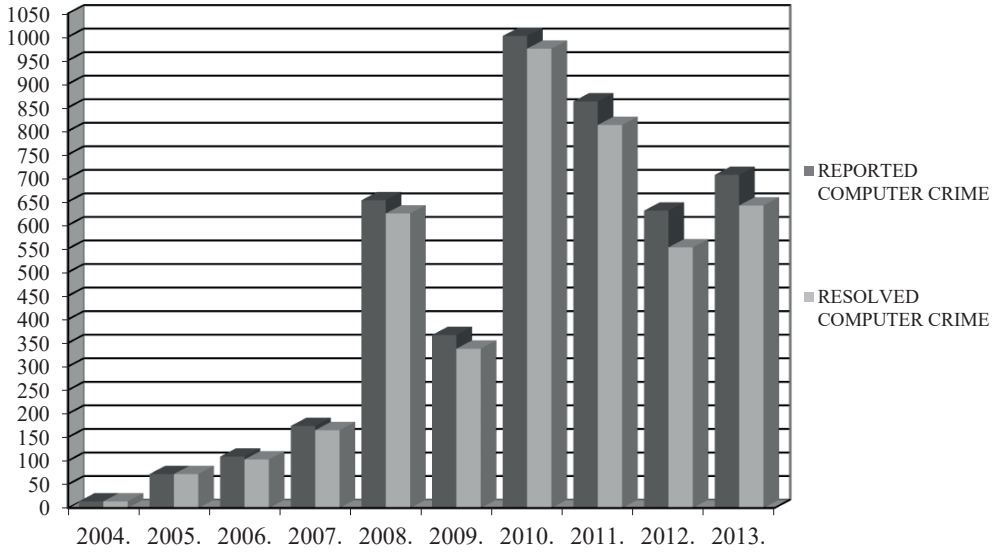
Table 2. *The total number of reported, resolved and percentage of resolved criminal offences of computer crime in the Republic of Croatia for the period between 2004−2013.* (According to the data from Table 1.)

	Reported	**Resolved**	**% Resolved**
Total Number	*4,592*	*4,300*	*93.64%*

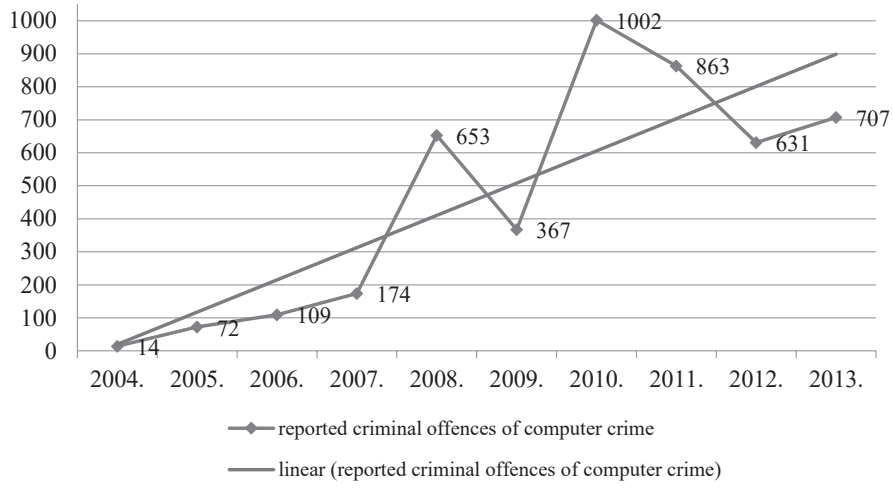
The conclusion is that the number of reported criminal offences had a linear trend of growth till 2008, followed by a decline after which the number of reported criminal

[6] See the complete legal description of offenses in Art. 266–273 in the Criminal Code OG no.125/11, 144/12.

offences increased; ultimately, it had the growth trend which is shown in Graph 2. Also, the ratio between the reported and resolved criminal offences shows a high percentage of the resolved criminal offences.

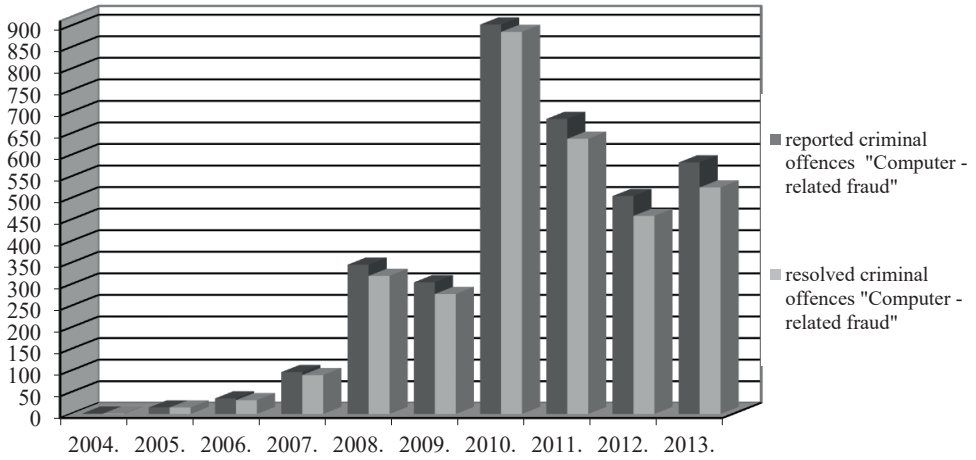


Graph 1. *Ratio of reported and resolved criminal offences of computer crime in Croatia for the period between 2004−2013.* (According to the data from Table 1.)



Graph 2. *Linear trend of growth in the number of criminal offences of computer crime reported in Croatia for the period between 2004–2013.* (According to the data from Table 1.)

The most numerous criminal offences in the analysed period of 10 years were "computer-related fraud", the total of reported offences were 3,475 and 3,244, i.e. 93.35% of them resolved. The percentage of criminal offences of computer crime in the RC is 75.67%. Also, it is apparent that the number of reported offences of computer crime had a linear trend of growth from 2004−2008, while in the period between 2009−2013 varied every year as shown in Graph 3.



Graph 3. *Ratio of reported and resolved criminal offences, "computer-related fraud" in Croatia for the period between 2004−2013 according to the data of the Ministry of the Interior.* [19]

Table 3. *Reported criminal offenses of computer crime, all reported criminal offenses and percentage of criminal offenses of computer crime in all reported criminal offenses in Croatia for the period between 2004−2013 according to the data of the Ministry of the Interior.* [19]

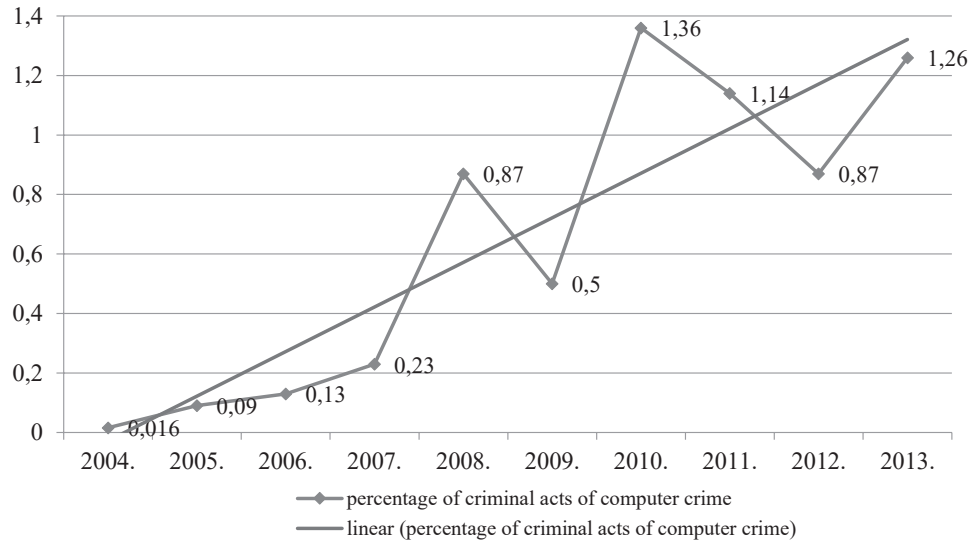
	2004	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
"Computer crime"	14	72	109	174	653	367	1,002	863	631	707
All reported criminal offenses[7]	85,416	79,946	81,049	75,857	74,571	73,497	73,328	75,620	72,171	62,708
% Computer crime in all reported offenses	0.016%	0.09%	0.13%	0.23%	0.87%	0.50%	1.36%	1.14%	0.87%	1.26%

If we compare the number of reported criminal offences of computer crime with the total number of the reported criminal offences (for which criminal proceedings are instituted ex

[7] The data relating to criminal offenses for which the prosecution initiated ex officio.

officio), we can find out that the biggest number of the reported offences was in 2004, whereas the largest number of offences of cybercrime was in 2010. Comparing the development of all criminal offences of computer crime, we can see that computer crime does not follow the growth or decline of the reported criminal offences; the conclusion is that computer crime is not related to the total number of reported criminal offences.

Table 3 shows the data on the number of reported offences of computer crime, all reported criminal offences and percentage of computer crime in the period between 2004–2013. The percentage of computer crime in all criminal offences was 0.65%, if we exclude the year 2004, the average percentage was 0.72%. Graph 4 represents the percentage of computer crime in all criminal offences in the RC for the period between 2004 and 2013, showing its growing trend.



Graph 4. *The growth trend percentage share of criminal offenses of computer crime in all reported criminal offenses in Croatia for the period between 2004–2013.*
(According to the data from Table 3.)

Perpetrators of Computer Crime

To obtain information on perpetrators of computer crime, the data of the Ministry of the Interior reports on criminal offences of computer crime were analysed for the period 2010 to 2013. In that period the total of 3,203 criminal offences were reported which makes 69.75% of the total number of offences for the period between 2004 and 2013. Of 3,203 criminal offences, 2,983 were resolved, which is 93.13% including 401 physical persons and two legal entities reported, which represents a satisfactory sample for interpretation. According to the mean value, each perpetrator committed ≈ 7.4 criminal offences. Table 4 represents the analysis of perpetrators according to their age, divided into age groups

for each year of the analysed period. The age group of 29 to 39 years includes the greatest number of perpetrators, 115 of them. Distribution of perpetrators by age groups is shown in Graph 5, referring to the data in Table 4. By nationality, 85.5% of offenders i.e. 343 of them were Croatian citizens, while 58 of them were foreign citizens.

Most of them were males (330), i.e. 82%. 401 of them were physical persons (99.5%) and two legal entities. Data on gender of perpetrators and citizenship for the period 2010 to 2013 are shown in Table 5, while Graph 6 shows the percentage of perpetrators by their citizenship and Graph 7 by their gender.

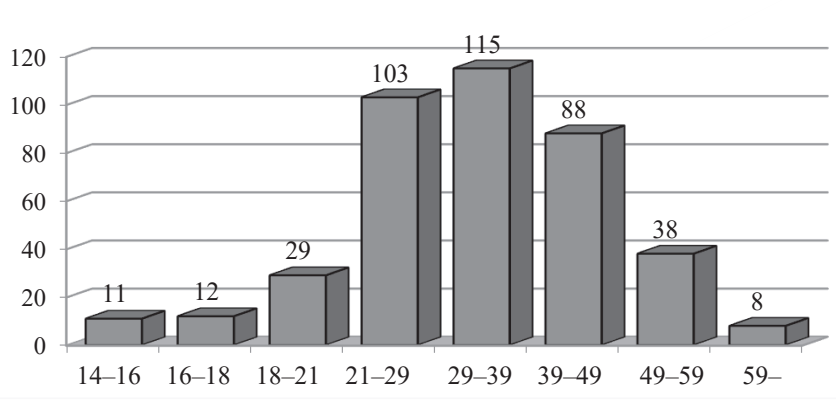
Comparison of data on the resolved number of computer crimes (Table 1) and data on the number of perpetrators (Table 4) shows that in 2010, the total of 83 perpetrators for 975 criminal offences were reported (≈ 11.75 criminal offences per a perpetrator), in 2011, the total of 142 perpetrators for 813 criminal offences (≈ 5.73 criminal offences per a perpetrator), in 2012, the total of 98 perpetrators for 553 criminal offences (≈ 5.65 criminal offences per a perpetrator) and in 2013, the total of 80 perpetrators for 642 criminal offences (≈ 8.02 criminal offences per a perpetrator) were reported.

Table 4. *Perpetrators of criminal offenses of computer crime according to age in Croatia for the period between 2010–2013 according to the data of the Ministry of the Interior.* [19]

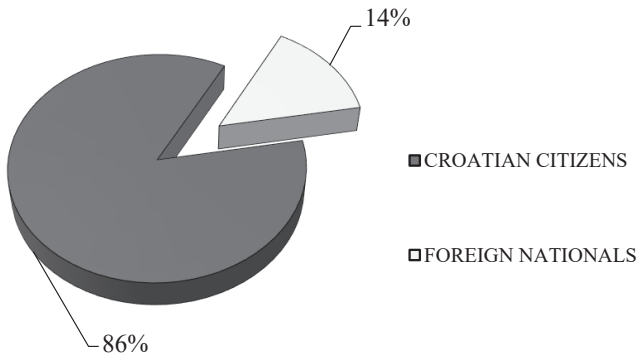
	Age							
	14–16	**16–18**	**18–21**	**21–29**	**29–39**	**39–49**	**49–59**	**59–**
2010	4	2	6	25	25	13	5	1
2011	4	5	12	32	39	37	10	3
2012	3	3	4	24	31	20	11	2
2013	/	2	7	22	20	18	9	2
Total	*11*	*12*	*29*	*103*	*115*	*88*	*35*	*8*
401								

Table 5. *Perpetrators of criminal offences by their gender and nationality in Croatia for the period between 2010–2013 according to the data of the Ministry of the Interior.* [19]

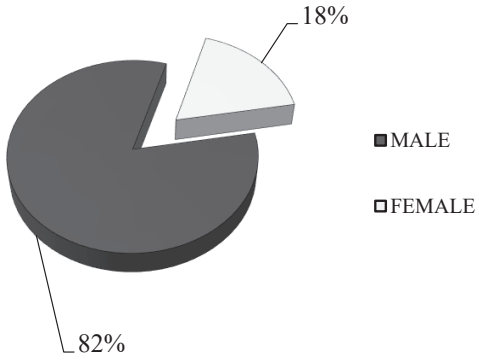
	Gender				**Nationality**	
	Female	**Male**	**Legal entity**	**Citizen**	**Foreign nationals**	**Croatian citizens**
2010	12	69	2	81	14	67
2011	30	112	/	142	19	123
2012	13	85	/	98	17	81
2013	16	64	/	80	8	71
Total	*71*	*330*	*2*	*401*	*58*	*343*



Graph 5. *Distribution of criminal offenders according to age groups in Croatia for the period between 2010–2013.* (According to the data from Table 4.)



Graph 6. *Criminal offenders according to nationality.* (Data from Table 5.)



Graph 7. *Criminal offenders according to gender.* (Data from Table 5.)

Sentences for Perpetrators in the Period 2009–2013

Analysis of the sentences pronounced over perpetrators of criminal offences of computer crime in the RC for the period 2009 to 2013 is based on the released data of the Croatian Bureau for Statistics. [20]

In the period from 2009 to 2012, 374 sentences were pronounced against perpetrators, the same period in which the perpetrators were discovered for 2,679 criminal offences shows a great disproportion between the number of sentences passed and the number of reports filed against the perpetrators of criminal offences. The growing number of sentences had a linear trend, from 51 to 125 sentences. Comparing the number of perpetrators reported in the period from 2010 to 2012 with the number of sentences pronounced, it was found that in 2010, 83 perpetrators were reported and 81 sentences were passed, in 2011, 142 perpetrators were reported and 117 sentences passed, and in 2012, 98 perpetrators were reported and 125 sentences pronounced and the total of reported perpetrators were 323 and 323 sentences pronounced. Table 6 shows the number of convictions against perpetrators for the period 2009–2012 according to years and criminal offences. Analysis found out that there were a total of 84 convictions for the criminal offence of child pornography on computer system or network, a total of 14 convictions for the offence against confidentiality, integrity and availability and 18 convictions for criminal offences of computer-related forgery and total of 258 convictions for criminal offences of computer-related fraud. It is evident that the most numerous convictions refer to computer-related fraud for which the biggest number of criminal offences were reported.

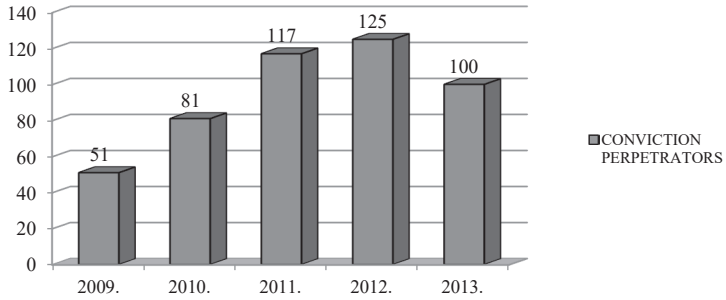
In 2013, a total of 100 sentences were pronounced (Table 7) and if that number is compared with the number of sentences from the years before, then a slight drop in the number of convictions can be seen. Most sentences (88) were passed for criminal offences of computer-related fraud, as expected. According to the data of the Ministry of the Interior in 2013, 80 perpetrators were reported for 642 criminal offences. If we compare the number of perpetrators which were police-reported with the number of convictions in 2013, the conclusion is that there were 25% more convictions than the number of the reported perpetrators which can mean that a number of offences were reported by the public prosecutor, not known to the police or, that during the procedure the criminal offence was classified differently or it was due to the completion of previous procedures. According to the data of the Ministry of the Interior, in 2013, three criminal offences of data interference were reported, four reports against criminal offences of illegal interception of data and ten reports against perpetrators committing criminal offence of misuse of device in 2013, for which there were no convictions.

Table 6. *Convictions of perpetrators for criminal offences of computer crime in Croatia for the period between 2009–2012 according to the data of the Croatian Bureau of Statistics.* [20]

	2009	**2010**	**2011**	**2012**	**Total**
Child pornography on a computer system or network					
Art. 197A para. 1	10	24	21	24	79
Art. 197A para. 2	3		1	1	5
Offences against confidentiality, integrity and availability of computer data, programs and systems					
Art. 223 para. 1		2		3	5
Art. 223 para. 2	2				2
Art. 223 para. 3		1	3	1	5
Art. 223 para. 4		1			1
Art. 223 para. 5		1			1
Computer-related forgery					
Art. 223A para. 1	2		3	2	7
Art. 223A para. 2			2		2
Art. 223A para. 3	5	1	1	2	9
Computer fraud					
Art. 224A para. 1	28	48	84	84	244
Art. 224A para. 2				2	2
Art. 224A para. 3	1	3	2	6	12
Total	*51*	*81*	*117*	*125*	*374*

Table 7. *Convictions of perpetrators for criminal offences of computer crime in Croatiafor the year 2013 according to the data of the Croatian Bureau of Statistics.* [20]

2013	
Unauthorized access	
Art. 266 para. 1	8
Art. 266 para. 2	1
Damage to computer data	
Art. 268 para. 1	1
Computer-related forgery	
Art. 270 para. 1	2
Computer fraud	
Art. 271 para. 1	82
Art. 271 para. 2	6
Total	*100*



Graph 8. *Convictions of perpetrators for the period between 2009–2013.* (According to the data from Tables 6 and 7.)

Table 8 shows the total of 115 prison sentences, 338 sentences of suspended prison, 4 fines for adults, 4 juvenile detentions, 11 juvenile warnings and 2 juvenile supervisions. Of 474 convicted perpetrators, 366 (77.21%) were males, which represent a smaller percentage than that of the police reported (82%). 13 sentences were pronounced for juveniles (2.74% of all sentences). The sentences pronounced over perpetrators according to age and gender for each year are shown in Table 9.

Table 8. *Pronounced sanctions by year for the period between 2009−2013.* (According to the data of the Croatian Bureau of Statistics.) [20]

Pronounced Sanctions						
	Prison	**Suspended Prison**	**Fine**	**Juvenile Prison-Suspension**	**Measures of Warning**	**Increased Supervision Measures**
2009	16	31	2	/	2	/
2010	25	52	/	3	1	/
2011	29	81	1	1	5	/
2012	26	96	1	/	/	2
2013	19	78	/	/	3	/
Total	*115*	*338*	*4*	*4*	*11*	*2*

Table 9. *Number of convicted perpetrators according to majority and sex in Croatia for the period between 2009−2013.* (According to the data of the Croatian Bureau of Statistics.) [20]

	Adult Perpetrators	**Juvenile Perpetrators**	**Total**	**Male**	**Female**	**Total**
2009	49	2	51	43	8	51
2010	80	1	81	65	16	81
2011	112	5	117	88	29	117
2012	123	2	125	95	30	125
2013	97	3	100	75	25	100
Total	*461*	*13*	*474*	*366*	*108*	*474*

Detailed presentation of the total of pronounced sanctions according to prison sentences ("P" in the table), suspended sentences ("S" in the table) and fines for every criminal offence for the period 2009−2013 is shown in Table 10. Analysis of the data on the mentioned sanctions[8] shows that the 6–12 month suspended prison sentences were pronounced in the greatest number (196)[9] followed by 3–6 month suspended prison sentences (111).

The greatest number of pronounced prison sentences (unconditional), were 3–6-month prison sentences (45), which makes 40% of prison sentences, they are followed by 6–12-month prison sentences (37). The strictest sentences were pronounced for the criminal offence of child pornography on computer system or network, 52 unconditional imprisonment (45% of all prison sentences) and 19 suspended prison sentences (17 sentences of 6–12 months in prison) and three sentences of 5–10 years in prison.[10]

This could be expected, as the strictest prescribed sentence is imprisonment. The lightest sentences were pronounced over perpetrators for the criminal offence of offences against the confidentiality, integrity and availability of computer data, programs or systems including 13 suspended sentences and one fine, five of them related to Item 1 for which the shortest sentence of all criminal offences is prescribed.[11]

For the most numerous criminal offences of computer-related fraud from Art. 224A para. 1, in the period 2009–2012, 243 sentences were pronounced, and 205 of them were suspended prison sentences (about 84%), mostly 6–12 month prison sentences (total 119), followed by 3–6 month prison sentences (total 70).[12]

Also, in 2013, computer-related fraud from Art. 271 para. 1, was the most numerous criminal offences for which 82 sentences were passed (82% of all sentences), 63 of them suspended prison sentences (about 77%), mostly 6–12-month prison terms (42 sentences) and 3–6-month prison terms (21 sentences).[13]

---

8 Compare with penalties prescribed in Articles 197A para. 1–2; 223 para. 1–5, 223A para. 1–3 and 224A para. 1–3. Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08) also and Art. 266 para. 1–2, Art. 268 para. 1, Art. 270 para. 1 and art. 271 para. 1–2. Criminal Code (OG no. 125/11, 144/12).

9 See detailed Art. 67 "suspended sentence" in Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08) and Art. 56 "suspended sentence" in Criminal Code (OG no. 125/11, 144/12).

10 Art. 197A para. 1 prescribes a punishment of imprisonment of 1–10 years, and paragraph 2 imprisonment for a term of six months to three years. Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08).

11 Art. 223 para. 1 punishable by a fine or imprisonment up to one year. Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08).

12 See detailed Art. 67 "suspended sentence" in Criminal Code (OG no. 110/97, 129/00, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08) in Art. 56 "suspended sentence" in Criminal Code (OG no. 125/11, 144/12).

13 Ibid.

Table 10. *Overview of pronounced sanctions according to prison sentences, sentences of suspended prison and fines to adult perpetrators for criminal offences of computer crime for the period between 2009–2013.* (According to the data of the Croatian Bureau of Statistics.) [20]

Pronounced Sanctions																	
	Prison																**Fine**
	Years								**Months**								
	5–10		**3–5**		**2–3**		**1–2**		**6–12**		**3–6**		**2–3**		**1–2**		
	P	**S**	**P**	**S**	**P**	**S**	**P**	**S**	**P**	**S**	**P**	**S**	**P**	**S**	**P**	**S**	
2009–2012																	
Art. 197a para. 1	3				2		5	1	11	13	30	1					
Art. 197a Para. 2										4	1						
Art. 223 para. 1										1		1		1		1	1
Art. 223 para. 2												1		1			
Art. 223 para. 3												3		2			
Art. 223 para. 4																1	
Art. 223 para. 5												1					
Art. 223a para. 1									1	4		2					
Art. 223a para. 2										2							
Art. 223a para. 3								2		2	1	2					2
Art. 224a para. 1			1		1		12	13	15	119	9	70		2		1	
Art. 224a para. 2												2					
Art. 224a para. 3							2	2	1	4		1	1				1
2013																	
Art. 266 para. 1										1	1	4		1			
Art. 266 para. 2										1							
Art. 268 para. 1												1					
Art. 270 para. 1										1		1					
Art. 271 para. 1							4	2	9	42	3	21				1	
Art. 271 para. 2							2			2							
Total	*3*	*/*	*1*	*/*	*3*	*/*	*25*	*20*	*37*	*196*	*45*	*111*	*1*	*7*	*/*	*4*	*4*

Conclusion for the Case Study of the Republic of Croatia

According to the research, a total of 4,592 criminal offences of computer crime were reported in the RC; for 4,300 of them the perpetrators were discovered (93.64% resolved). Their percentage in the number of criminal offences (instituted ex officio) was 0.72% on average (without data from the year 2004). In the analysed period, computer crime varied and was not dependent on fluctuations of other criminal offences. The most numerous criminal offences of computer-related fraud represent 75.67% of criminal offences (3,475).

In the period between 2010 and 2013, 403 perpetrators were reported for 2,983 criminal offences, which, according the mean value is ≈ 7.4 criminal offences per a perpetrator. Perpetrators are mostly Croatian citizens (85.5%) and males (82%). The age distribution of the perpetrators is wide and no significant data is obtained. A total of 474 sentences were pronounced, 346 of them (73%) for the criminal offence of computer-related fraud. According to the types of sanctions, most of them are suspended prison sentences (338), while the strictest sentences passed were for child pornography on computer system or network, 52 unconditional prison sentences (5–10-year imprisonment) and 19 suspended prison sentences. 461 adults were convicted and 13 juveniles (2.74%), mostly males (77.21%).

The results of the research proved the assumption that the development of computer crime in the RC is not related to the development of all other criminal offences and that the computer crime rate is very low.

Computer crimes in the RC are characterized by the "dark figure of crime" which can be explained by not reporting criminal offences by the injured party, disproportion is evident between the reported perpetrators, according to the data of the Ministry of the Interior and the number of pronounced sentences, which represents 2,983 reports in relation to 423 sentences.

This can be explained by a number of discarded reports by public prosecutors or by the court or by the court procedure changing the offence into extended criminal offence when filing the report on computer crime. [2] The results obtained in the research show that computer crimes in the RC are characterized by a prominent varying of the number of reported criminal offences, a high "dark figure of crime", high percentage of resolved offences and finally, a small number of convictions for perpetrators. [2] Characteristics of the perpetrators: they are physical persons, males, mostly citizens of the RC, while no particular result was obtained with regard to age.

Deep Web

The public information about the deep web is that it is currently 400 to 550 times the size of the World Wide Web. Deep Web contains 7,500 terabytes of data compared to 19 terabytes of data on the Web. The Deep Web contains almost 550 billion individual documents compared to 1 billion of the surface web. [9] Sixteen of the largest deep websites collectively contain about 750 terabytes of information—enough for yourself to exceed the size of the Web site forty-five times.

Deep Web is the largest growing category of new information on the Internet. The total content quality on Deep Web is 1,000 to 2,000 times the size of the Web. Deep Web content is very relevant to any information needs. More than half of the deep web content is contained in topic-specific databases. Full ninety-five percent of the deep web is publicly available (free).

Violent Extremists and Terrorists Abuse Darknet to Hide

Darknet is the hidden portion of the Internet that is only available through specialized browsers, Tor. It is not really a single entity but instead thousands of sites, most of them encrypted and all available only to those with information about how to find them and how to access them. [14]

"It's a place where all sorts of illicit activities can happen. It's the sort of place where you would go if you wanted to buy weapons," said Herb Lin, a senior research scholar for cyber policy at the Hoover Institution at Stanford University. [14]

The dark web also plays a key role in terrorists' overall communication strategy.

"One of the things they do is they train each other on how to run all the traffic on their Android mobile phones through the dark web so all their Internet and voice traffic is sent through encrypted channels and so unreadable by law enforcement," said Aaron Brantly, a Professor of cyber studies at the US Military Academy. [14]

Tor

Layered routing is one of the most widely used technologies by anonymization networks. The objective of the layered routing is to provide anonymous communication between the entities on the network. This analogy is called the onion. Each router, when receiving a message, "eats" one layer of such a "port". It works in a way that it uses its own encryption key, and thus provides the necessary data for routing the rest of the data structure. The remainder passed contains a message and routing instructions intended for all of the following routers. The last routing removes the last encryption layer. It also sends the original message to the destination.

The Tor Network functionality is based on the onion routing; speaking of pseudo anonymous (or anonymous) communication within a computer network developed by David Goldschlag, Michael Reed and Paul Syverson. [7] The onion routing is based on the mixed networks of David Chaum. In addition to mixed networks, it includes many modifications and upgrades of this technique. The most important is the introduction of the concept of the onion router. The goal of routing mail is to maintain the privacy of the sender's and recipient's message privacy while also protecting the content of the message while travelling through the network. That is exactly what we can do by using Chaum's mixed cascades.

So, the message travels through a network of proxy servers, and they call it the onion servers in this case and point the message unpredictably. It is being crypted before being transmitted between servers. This prevents unauthorized browsing of the message content, so-called eavesdropping. The basic advantage of the onion routing is the fact that for anonymous communication it is not necessary to work properly through all the servers with which the connection is made. It is important to emphasize that if an attacker still manages to access one or perhaps even a few servers, the user's animation is not compromised. Messages are in the Onion Routing (OR) network multiply encrypted, and this is precisely why the anonymity is not compromised. In order to gain control over all servers, it is possible to reconstruct the message path of the OR network.

Tor networking routers use special routing onions. They are used to establish a connection to send the message. The start-up router randomly selects a number of onion routers and sends a message to each. It contains a symmetric message decryption key, and the forwarding instructions

for the next router. These messages are encrypted with the public key of the appropriate router. Specifically, as the resulting layered data structure encrypted, it is first necessary to decrypt the outer layers in order to get inside.

VPN and IP Address

Provide users with the ability to send and receive data over public or shared networks as if their computers are locally connected. VPN allows: security, functionality, manageability, anonymity. The traffic between you and the VPN service you use is encrypted so it is impossible for someone to see what you are doing on the Internet. As long as you are connected to a VPN, you will have access to the entire Internet without any censorship that could affect you. You can access services and geographically limited web pages if you are using a VPN server located in the region where these services or websites are available. The servers you are connecting to will not see your IP address, they only see the VPN server address. You can surf the web, read your e-mails, or send important information on public networks, without the risk of someone spitting you.

For example, Netflix and YouTube may sometimes limit the display of content in a particular region. If you type the name in the search engine, you will get a response "Content not available in your region". Using VPN, you can hide your location. If a VPN has servers in the US, the services you use "think" that you are there, not in your home, wherever you are. VPN is also useful if you need to hide your identity when using peer-to-peer services, such as BitTorrent. Your Internet service providers can see data that travels through a VPN, but not where they are or where they come from. This is useful because it adds yet another level of privacy, but also because some operators are driving traffic through BitTorrent.

Special technological advances in communication have been achieved by a hybrid approach that integrates Tor and VPN communication techniques. There are two possibilities. The first possibility is that a user first connects to Tor, and then to the VPN. Another possibility is that a user first connects to the VPN, and then to Tor. Everywhere the two possibilities have their advantages and disadvantages, which are further explained in detail below.

Tor through VPN

In this configuration you connect first to your VPN server, and then to the Tor network before accessing the internet: your computer → VPN → Tor → internet; your apparent IP on the internet is that of the Tor exit node.[14]

[14] Crawford D. "Pros: Your ISP will not know that you are using Tor (although it can know that you are using a VPN), The Tor entry node will not see your true IP address, but the IP address of the VPN server, If you use a good no-logs provider this can provide a meaningful additional layer of security, Allows access to Tor hidden services. Cons: Your VPN provider knows your real IP address, No protection from malicious Tor exit nodes. Non-HTTPS traffic entering and leaving Tor exit nodes is unencrypted and could be monitored, Tor exit nodes are often blocked. We should note that using a Tor bridge can also be effective at hiding Tor use from your ISP (although a determined ISP could in theory use deep packet inspection to detect Tor traffic)." [5]

VPN through Tor

This involves connecting first to Tor, and then through a VPN server to the internet: your computer → encrypt with VPN → Tor → VPN → internet.

This setup requires you to configure your VPN client to work with Tor, and the only VPN providers we know of to support this are AirVPN and BolehVPN. Your apparent IP on the Internet is that of the VPN server.[15]

Some Challenges

When using Tor, the last exit node in the chain between your computer and the open internet is called an exit node. Traffic to or from the open internet exits and entries leaves this node unencrypted. Unless some additional form of encryption is used (such as HTTPS), this means that anyone running the exit node can spy on the users' internet traffic. SSL connections are encrypted, so if you connect to an SSL secured website (https://) your data will be secure, even if it passes through a malicious exit node.

End-to-end timing attacks is a technique used to de-anonymize VPN and Tor users by correlating the time they were connected, to the timing of otherwise anonymous behaviour on the Internet. An incident where a Harvard "bomb-threat idiot" got caught while using Tor is a great example of this form of de-anonymization attack in action, but it is worth noting that the culprit was only caught because he connected to Tor through the Harvard campus WiFi network. If such an attack (or other de-anonymization tactic) is made against you while using Tor, then using VPN as well will provide an additional layer of security.

Speed is a limiting factor in the use of communication techniques with a high level of anonymity, as evidenced by the concrete outcomes of the communication analysis presented in the following illustrations.

---

[15] Crawford D. "Pros. Because you are connected to the VPN server through Tor, the VPN provider cannot 'see' your real IP address – only that of the Tor exit node. When combined with an anonymous payment method (such as properly mixed Bitcoins) made anonymously over Tor, this means the VPN provider has no way of identifying you, even if it did keep logs, Protection from malicious Tor exit nodes, as data is encrypted by the VPN client before entering (and exiting) the Tor network (although the data is encrypted, your ISP will be able to see that it is heading towards a Tor node), Bypasses any blocks on Tor exit nodes, Allows you to choose server location (great for geo-spoofing). All internet traffic is routed through Tor (even by programs that do not usually support it). Cons. Your VPN provider can see your internet traffic (but has no way to connect it to you). Slightly more vulnerable to global end-to-end timing attack as a fixed point in the chain exists (the VPN provider)." [5]

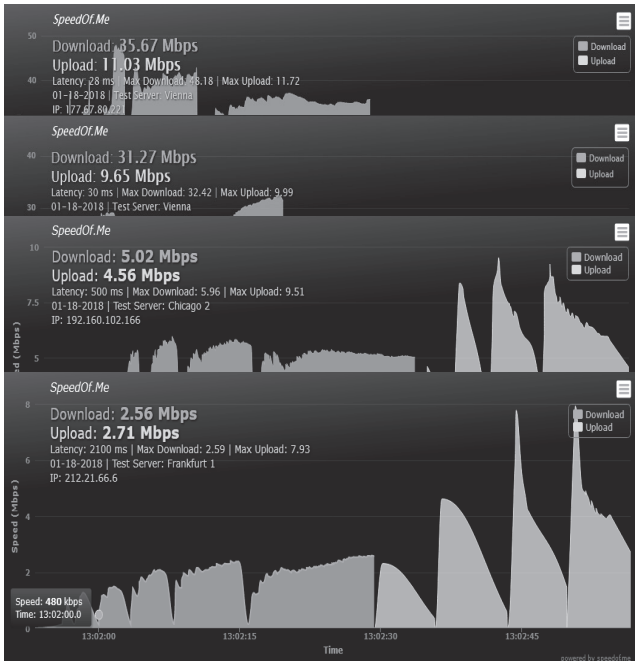


Figure 1. *Comparative view of how much speed is a limiting factor in the use of communication techniques with a high level of anonymity.* (Created by the authors.)

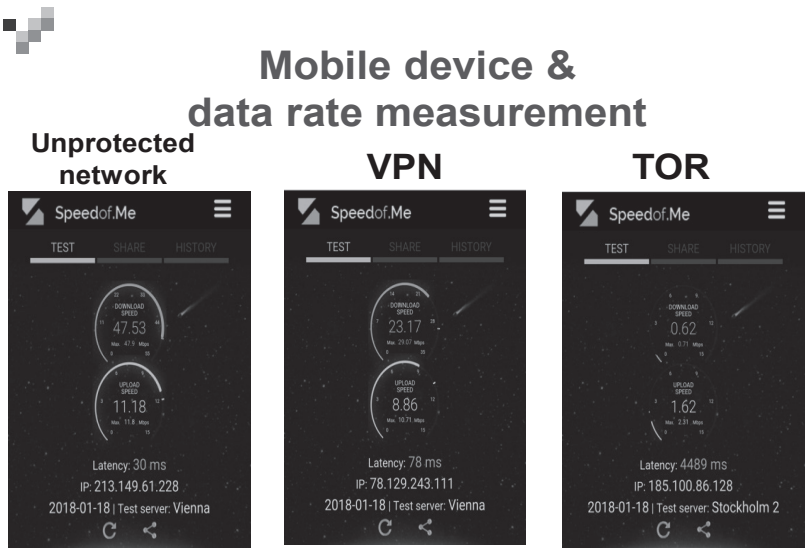


Figure 2. *Comparative view of how much speed is a limiting factor in the use of communication techniques with a high level of anonymity using a mobile device.* (Created by the authors.)

Conclusion

Numerous cases of police practice confirm that new information-communication technologies are abused by criminals, violent extremists and terrorists. The abuse of new technologies is not overwhelming. The goal of a high level of anonymity is achieved in full. In order for the police to cope with these abuses, they must be provided with hardware, software and human resources. A small police, such as the one of Croatia does not have the strength to develop hardware and software, so it needs to be purchased from partner countries. The Croatian police have created an organizational framework for combating cybercrime, which needs to be filled with experts in the field of combating cybercrime. Completing a structured organizational structure with a quality staff should not be a big problem since the Croatian Academic Community creates human resources that can handle the most demanding technological challenges. It is only necessary that police managers allow them to be employed in the police, so that they can be actively involved in combat teams against all forms of cybercrime as soon as possible.

References

[1] ANTOLIŠ, K.: Police Investigation and Abuse of Darknet. *9th International Conference "Days of Corporate Security 2018"*, 14.03.2018, Ljubljana.

[2] ANTOLIŠ, K., VARJAČIĆ, I.: Analysis of Computer Crime in the Republic of Croatia. *Suvremeni promet*, 32 3–4 (2015), 231–238.

[3] ANTOLIŠ, K.: Internet forensics and cyber terrorism. *Journal: Police and security,* 19 1 (2010), 121–128.

[4] BAČA, M.: Introduction to Computer Security. *The Official Gazette*, (2004).

[5] CRAWFORD, D.: *Using VPN and TOR together.* 2016. www.bestvpn.com/using-vpn-tor-together/ (Downloaded: 19.03.2018)

[6] DRAGIČEVIĆ, D.: *Computer Crime and Information Systems. Zagreb,* IBS – Informatorov biro sustav d.o.o., 2004.

[7] GOLDSCHLAG, D., REED, M., SYVERSON, P.: Onion Routing communications of the ACM for Anonymous and Private Internet Connections. *Communications of the ACM,* 42 2 (1999), 39–41. www.cs.bgu.ac.il/~dsec121/wiki.files/j2b.pdf (Downloaded: 19.03.2018)

[8] KATZ, G.: UK minister: WhatsApp must make itself accessible to police. *The Times of Israel* (online), 26 Match 2017. www.timesofisrael.com/uk-minister-whatsapp-must-make-itself-accessible-to-police/ (Downloaded: 19.03.2018)

[9] MARJANOV, S.: Šta je to Deep Web? (What is Deep WEB?) *saznaj novo* (online), 04.04.2015. www.saznajnovo.com/2012/07/sta-je-to-deep-web/ (Downloaded: 19.03.2018)

[10] NAKASHIMA, E.: FBI chief: Terrorist group turning to encrypted communications. *The Washington Post* (online), July 8, 2015. www.washingtonpost.com/world/national-security/fbi-chief-terror-group-turning-to-encrypted-communications/2015/07/08/89167f74-2579-11e5-aae2-6c4f59b050aa_story.html?utm_term=.7a219b3a255e (Downloaded: 19.03.2018)

[11] PROTRKA, N.: Computer data as an electronic (digital) evidence. *Journal: Police and Security,* 20 1 (2011), 1–13.

[12] TAN, R.: Terrorists' love for Telegram. *Vox* (online), Jun 30, 2017. www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter (Downloaded: 19.03.2018)
[13] VARJAČIĆ, I. : *Computer crime and digital evidence*. Zagreb, Police Academy, 2014.
[14] WEISE, E.: 2017. Terrorists use the Dark Web to hide. *USA Today* (online), Mar 28, 2017. www.usatoday.com/story/tech/news/2017/03/27/terrorists-use-dark-web-hide-london-whatsapp-encryption/99698672/ (Downloaded: 19.03.2018)
[15] WILSON, E.: *The Dual State: Para politics, Carl Schmitt and the National Security Complex*. London and New York: Routledge, Taylor & Francis Group, 2016.
[16] *Convention on Cybercrime.* Chart of signatures and ratifications of Treaty 185. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (Downloaded: 01.10.2014)
[17] Criminal Code. *The Official Gazette of the Republic of Croatia "Narodne novine"*, number: 110/97, 27/98, 50/00, 129/00, 51/01, 11/03, 190/03, 105/04, 71/06, 110/07, 152/08, 125/11 and 144/12.
[18] Criminal Procedure Act. *The Official Gazette of the Republic of Croatia "Narodne novine"*, number: 152/08, 76/09, 80/11,121/11, 91/12,143/12,53/13,145/13
[19] Ministry of the Interior of the Republic of Croatia, Statistics:
Overview of basic indicators for public saftey in the Republic of Croatia for 2004–2013. www.mup.hr/UserDocsImages/statistika/2014/PREGLED_OSNOVNIH_POKAZATELJA_JAVNE_SIGURNOSTI_%20U_RH2004.%20%E2%80%93%202013.pdf (Downloaded: 04.10.2014)
Survey of safety indicators in 2010. www.mup.hr/UserDocsImages/statistika/2011/statistika2010.pdf (Downloaded: 27.10.2014)
Survey of safety indicators in 2011. www.mup.hr/UserDocsImages/statistika/2012/pregled%202011.pdf (Downloaded: 28.10.2014)
Survey of safety indicators in 2012. www.mup.hr/UserDocsImages/statistika/2013/statistika2012.pdf (Downloaded: 29.10.2014)
Survey of safety indicators in 2013. www.mup.hr/UserDocsImages/statistika/2014/Statisticki%20preg2013_konacni%20prom_WEB.pdf (Downloaded: 30.10.2014)
[20] Republic of Croatia, Central Bureau of Statistics. Publications by Statistical Subject Matter Areas, Administration of Justice. www.dzs.hr/ (Downloaded: 19–20.11.2014)
Adult Perpetrators of Criminal Offences, Complaints, Charges and Convictions 2009, Statistical reports (SR) 1421. (2010)
Adult Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2010, Statistical reports (SR) 1451. (2011)
Adult Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2011, Statistical reports (SR) 1478. (2012)
Adult Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2012, Statistical reports (SR) 1504. (2013)
Adult Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2013, Statistical reports (SR) 1528. (2014)
Juvenile Perpetrators of Criminal Offences, Complaints, Charges and Convictions 2009, Statistical reports (SR) 1422. (2010)

Juvenile Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2010, Statistical reports (SR) 1452. (2011)
Juvenile Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2011, Statistical reports (SR) 1479. (2012)
Juvenile Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2012, Statistical reports (SR) 1505. (2013)
Juvenile Perpetrators of Criminal Offences, Reports, Accusation and Convictions 2013, Statistical reports (SR) 1529. (2014)

[21] *The Office of the National Security Council.* Republic of Croatia. www.uvns.hr/hr (Downloaded: 21.03.2018)

[22] *National CERT.* Republic of Croatia, Computer Emergency Response Team. www.cert.hr/onama/ (Downloaded: 21.03.2018)

[23] *Washington Post*, March 24, 2003.

[24] *Act on Security and Intelligence System of the Republic of Croatia.* July 5, 2006.

[25] *Code of Criminal Procedure.* October 11, 2011.

[26] *Act on Police Businesses and Officials.* June 30, 2009.