Revija za kriminalistiko in kriminologijo / Ljubljana 68 / 2017 / 4, 412–423

Ongoing Criminal Activities in Cyberspace: From the Protection of Minors to the Deep Web

Tina Tomažič[1], Noemia Bessa Vilela[2]

New technologies have changed our lives significantly. They have brought a new way of communication, greater accessibility plus many other benefits, but unfortunately, also misuse of the web, inappropriate online behaviour, greater control and supervision, as well as various addictions. Above all, adolescents quickly explore the various possibilities of the use (and abuse) of new technologies, unaware of all the implications brought about by inappropriate behaviour on the Internet and its misuse. In our article, we focus on the means to protect children and adolescents from inappropriate behaviour online, because anyone (and everyone) can easily access unsuitable content and contacts. We explore those offences committed via the Internet, which occur most frequently in Slovenia. People are unaware that as soon as they connect to the Internet, they disclose their identity. For those who wish to remain anonymous, there is a much more extensive anonymous Web, the so-called Deep Web. The main purpose of these (anonymous) web sites is to hold information not intended for the general public, often being used for online criminal activity involving drug markets, financial fraud, illegal weapons, espionage, sexual abuse of minors, *inter alia*. We explore the reality of the infamous Deep Web, how it works, which part of the Deep Web presents a Darknet, and why it is so untouchable, as even forensic research in this area has not been successful due to its complexity and endlessness.

Keywords: cyber crime, new technologies, deep web, darknet, Slovenia

UDC: 343.3/.7:004

1 Introduction

In recent years, new media have changed the way of communication significantly, and is at the same time, a rapidly evolving area of research. The non-existence of the Internet is inconceivable in today`s world which, without it, would not exist in its present form. The new media come as a poisoned apple, bringing not only benefits, but several disadvantages, such as increased,abusive, inappropriate behaviour, dependency, control, and new types of offences, as well. Most members of the younger generation are extremely quick to seize opportunities for private participation in the new, freely accessible and low-cost model of new technologies, not being aware of all the hazards and consequences arising from inappropriate, and even criminal, online activity, given how easy it is to come into contact with content and contacts that are not suitable. The risks of new media are not only hazardous for minors, but for the entire online population, as well. The Internet is the fastest way to exchange information and to have access to various services, as it is connected to almost every electronic device. The fact is that as soon as a connection is established, the user discloses his identity and, consequently, becomes potentially exposed to danger. Those wishing to remain amonymous can access the much more extensive Web, the Deep Web. The Deep Web is, according to Zulkarnine, Frank, Monk, Mitchell, and Davies (2016), a hidden part of the Internet, which is becoming an ideal hosting ground for illegal activities and services, including large drug markets, financial fraud, illegal weapons, espionage, and child sexual abuse. The main purpose of the Deep Web is to exchange information not intended for the general public.

This paper is aimed at exploring which inappropriate behaviours minors engage in while connecting to the web, and finding solutions to prevent such behaviours. Additionally, the authors take a closer look at the Deep Web, which is, due to its characteristics, very close to the topic of this research, given the localised occurrence of risky and criminal online behaviours, explaining how it works, and detailing what is it actually happening. The authors will attempt to explain its untouchablity, the reason why the users remain anonymous, and how it affects forensics research, which in this respect, is quite slow, ineffective and often never completed. The extent of cyber crime in Slovenia since 2011 will be explored in the

[1] Tina Tomažič, Ph.D., Assistant Professor, Institute of Media Communications, Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia. E-mail: tina.tomazic@um.si

[2] Noemia Bessa Vilela, Senior Research Assistant, Portucalense Institute for Legal Research, University Portucalense Infante D. Henrique Porto, Portugal. E-mail: noemia@uportu.pt

final part the paper. We will analyse those crimes committed via the Internet which have been reported to take place in Slovenia, and the overall awareness and perception of cyber crime. We will address developments and trends in the field of cyber crime which is a very young topic of study where forensics are increasingly successful. Developments in forensic research, tools and processes in the last decade has been increasingly successful but, in the Deep Web, this is still not a successful story due to its complexity and endlessness.

A descriptive, comparative, synthetical and analytical methodology will be based on reliable statistical data in criminal reports to the police in the field of cyber crimes since 2011. Furthermore, we will seek to identify the most common criminal offences and criminal web actions within the Deep Web, and how they can be detected.

2 New Media and Cyber Crimes

By connecting the media and the Internet, we can reach the new terminology "new media". The new media represent the convergence of two separate procedures: Computer Science and Media Technology. The most revolutionary social change caused by the Internet is so-called "internetization" (the penetration of the Internet in all aspects of individual and collective life and work) from private to public, during work and leisure time, in production and consumption, in the economy and policy (Golding & Splichal, 2014). With the development of the Internet, online communities and social networks have changed (Tomažič, 2017). Internetization brings not only benefits, but also more and more abuse, dependence and control (Splichal, 2016). The wide availability and use of information and communication technologies, and linking users with the help of these technologies, has opened up cyberspace, and it is being used by many as a place to carry out criminal activities (Bernik & Meško, 2011). Crime is a deeprooted pathological disorder in our society (Karmakar, 2016). Cybercriminology is an interdisciplinary subfield that brings together Computer Science, Psychology, Sociology, Criminology, and other disciplines (Jaishankar, 2011).

Cyber crime is an expansive term, and describes a constellation of deviancies with few similarities beyond their manipulation of Internet technologies, and is often inclusive of actions that have little or no physical bearing on the "real world" (Popham, 2017). Cyber crime is crime that is mediated by networked technology (Wall, 2007), and ld crimes, such as theft, fraud, and harassment, find new forms in cyberspace and information technologies. Other crimes, such as hacking or Internet-solicited prostitution, are contested deviance, with significant subgroups labelling certain actions as nondeviant and within a reasonable moral code, a code of conduct that would be accepted by anyone who meets certain intellectual and volitional conditions, almost always including the condition of being rational (Stalans & Finn, 2016). Cyber crime is a real and significant threat, and is becoming more and more aggressive. Technological developments lead to an increasing share of cyber crime and increases the risks of cyber security (Markelj & Završnik, 2016). According to Tsikrika et al. (2017), the deliberate misuse of technical infrastructures (including the Web and social media) for cyber deviant and cybercriminal behaviour, ranging from the spreading of extremist and terrorism related material to online fraud and cyber security attacks, is increasing.

The European Police Agency (Europol) set up a European Cybercrime Centre (EC3) in 2013 to strengthen the response of law enforcement agencies on cyber crime in the EU, thereby helping to protect European citizens, businesses and governments from cyber crime. According to Europol (2017), cyber crime is a growing problem for countries, in most of which the Internet infrastructure is well developed and payment systems are online. According to Stratton, Powell and Cameron (2016), development in computing, communications and other digital technologies has come to reveal the influence of key technological shifts in the world of criminological theory and research.

As has been stated by the Broadcasting Council (2011) and the Institute for Market and Media Research (2013), the last few years have been characterised by a transformation of passive acceptance into active media content, that has come to create its own content and comment on others, resulting in, for users and society, an important acquisition. Members of the younger generations especially have gained quick opportunities for private participation in the new, open (free), decentralised and low-cost model of media content production, which operates in the niche and local contexts, as well as globally. Among young people, the acceptance of audio-visual content from the Internet is increasingly widespread. But, despite some concerns about eligibility and actual possibilities for appropriate and effective regulation, such media, from the regulatory point of view, raises the need for new mechanisms developed to protect children and prevent the spread of intolerance. Due to the emergence of new challenges, especially in connection with new platforms and new products which allow access to harmful content, it is necessary to introduce rules to protect the development of children and minors, and human dignity in all audiovisual media services.

The media industry is increasingly dependent on the use of social media, especially considering the fact that this segment specialises in the sale of information and entertainment,

and this is the foremostand largest segment of social networks. While the emergence of social media has changed the lifestyle of virtually everyone, they are not used just for fun, information and a source of business opportunities, but also to abuse, defraud and damage. According to Europol (2016), for example, terrorist groups make extensive use of social media platforms to engage in recruitment campaigns, propaganda, incitement of terror acts, and for claiming responsibility for such attacks. Furthermore, social media are important engines, not only for the exchange of information, but also as an advertising channel for the sex slave trade and other illegal trading activities. According to Završnik (2017), the rulers of the world are data companies and companies that control the world with algorithms, or the connections of both when the differences between them are blurred. These companies also deal with social media, such as Facebook, which acts as a news broker alone, and does not create content. The online social networks namely deny the role of the editor because they avoid the obligations that apply to editorial-moderated content.

3 Minor's Risks in Cyberspace and their Protection

The ease with which children and young people access the Internet, convergent, mobile and networked media is unprecedented in the history of technological innovation (Livingstone, Haddon, Görzig, & Ólafsson, 2011). On the Internet, minors can easily come into contact with content and contacts that are not suitable for them, and it is important to understand the role that the Internet plays in their lives. According to Wright (2017), minors utilise electronic technologies to promote and/or maintain their social standing within their peer group. According to Šterk and Petek (2016), although it is necessary to take into account the safety tips for kids, the Web is also a place full of opportunities for learning, communication and entertainment.

Social networking is probably the fastest growing online activity among young people, as it allows accessibility and connectivity 24 hours a day, 7 days per week. New technologies also allow many opportunities for creativity, and with the integration of conversations, messages, contacts, photo albums and blogging functions, social networking can include online opportunities and risks more seamlessly than was previously possible. Children and teenagers who are very active in social networks and other communication channels like to express their identity, and at the same time, they can be very sensitive and deeply affected by the offensive insults and ugly talk about them, as they are just developing their personalities and have unstable self-esteem. Social networks have raised the age limit for their use, but unfortunately, children often overcome this obstacle by using fake data, lying about their year of birth, entering the world of social networks freely and establishing contacts with other users who are unaware that they are in contact with a child (Livingstone et al., 2011; Šterk, & Petek, 2016). However, the use of child-related social networking sites fulfills more social-emotional needs, as compared to more traditional forms of mediated communication that may fulfill more instrumental needs (Tanis, van der Louw, & Buijzen, 2016).

Some of the key online risks for children and minors:

Pornography, receiving sexual messages and sexting: There is some evidence and a huge amount of speculation that the Internet facilitates the exchange of sexual messages among peers. Originating with the spread of mobile phone messaging more than online communications, and so popularly labelled "sexting" (an amalgam of "sex" and "texting"), such acts lead to the popular and policy concerns. Exchanging messages containing sexual content, either with words or images, can only be made visible on the Internet, the types of practices in which minors are always engaged, and this can be a fun part of the flirtation, which includes research on the development of sexuality and intimacy. On the other hand, when distributed on the Internet, such messages can be sent to unexpected recipients and may be difficult to delete or edit, depending on their content. Furthermore, sexting is characterised as mainly for teenagers, who photograph themselves naked or half-naked, and then share their photos. Reasons for transmission are different, and if not forced into such an action, it can be a normal part of growing up and the development of gender identity. Pictures and letters were exchanged by people long before the emergence of the Internet, so that, in some ways, it is nothing new. However, there are some important differences which can have very unpleasant consequences, given that images can be sent via the Internet or to mobile phone. They could be also extended to others and, finally, a broader range of people can see them, many more than the sender wanted. Such events may cause problems in school, peer harassment, and parents and teachers becoming aware of the photos (Livingstone et al., 2011; Šterk & Petek, 2016). But transferring and viewing sexually explicit material when the subject is a minor can be considered child pornography, and serious legal consequences may arise from it. Several States have enacted legislation to help differentiate between child pornography and sexting by minors. The trend reflected in statutes has been that minors involved in sexting without other exacerbating circumstances should be charged with a less serious offense (Lorang, McNiel, & Binder, 2016).

- **Unsuitable contacts, offline meetings with online contacts:** Meeting new people online and then meeting these

people live is, perhaps, one of the more controversial activities of children in relation to the Internet and it can be a harmless means of expanding a social circle (Livingstone et al., 2011). However, there are also other online experiences that have, nevertheless, been identified as potentially harmful to children; for example, adult to child contact. According to Lovrec and Žišt (2017), such adult offenders are watching the open profiles on social networks, chat rooms and forums where children are present closely. With sophisticated tactics, and armed with information about the child, they initiate online contacts with them. They know their weaknesses and become their friends. The children, thinking that these are the peers of the offenders and that only they understand them, trust them with things from their intimate life, which can result in them both stripping and performing certain sexual activities. Perpetrators, of course, take advantage of subsequent blackmail. According to Europol (2016), the use of the Internet as a platform for child sex offenders to communicate, store and share child sexual exploitation material and to hunt for new victims, continues to be one of the Internet's most damaging and abhorrent aspects.

- **Bullying and harassment:** Due to the Internet and new technologies, this has become a widespread phenomenon. According to Završnik and Sedej (2012), it covers intimidation, bullying, or harassment on the Internet, understood in a broad sense, as well as the violence that is not connected to the Internet, but with mobile telephony services (for example, via short text messages, multimedia messages MMS, excessive calls). Minors are using the Internet and mobile phones for distributing threatening and derogatory messages, spreading degrading images and videos to reach a large audience in a very short time, and online it remains (until requested otherwise). They may also defame exchange of information and images on social networks between friends, which is a form of online harassment and bullying. According to Livingstone, et al. (2011), abusive behaviour among peers from both the harasser and the victim is often understood as a joke. For this reason, it is dangerous that the behaviour of "violence as entertainment" that takes place between young people, in their perspective, has grown to be acceptable, as it is offensive, and such kind of bullying may lead to serious consequences such as depression, isolation and self-harm, or even suicide. Bullying is one of many acts of risk that can harm minors when using the Internet. Web violence is a new form of violence and is the result of new technologies. Minors may be both victims and/or perpetrators of bullying, so it is important to teach children that online actions can have offline consequences that they may not be aware of, but which may be significant for those affected. This is a problem for young users. As they are the most vulnerable groups, there exists a huge gap between the youngters' technological skills and the (lack of) ability, and (im)maturity, to cope with harassment and bullying. Sexual harassment of children over the Internet has also become very frequent. Probably the biggest concern of public policy for the safety of children on the Internet is to focus on the risk that the child will meet someone new online who then abuses them in subsequent meetings face-to-face. However, the risk of injury from meeting face-to-face with someone whom one first met on the Internet is low, not least because children are using the Internet increasingly to expand their circle of friends. According to Vaillancourt, Faris and Mishna (2017), cyberbullying features some unique qualities that can both magnify the damage caused and make it more difficult to detect. These features include the pervasive, never-ending nature of cyberbullying, and the ability to reach large audiences quickly. The potential for anonymity and the related distance afforded by screens and devices compared to in-person interactions, allow the cruelty of cyberbullying to go unchecked. Despite the perceived anonymity of cyberbullying, it can be perpetrated by friends, who often have intimate knowledge about the victimised youth that can be devastating when made public.

- **Misuse of personal data and intelectual property rights infringment (piracy)**: A fundamental technological development in society in general is the digitization of information, as it has also led to a key threat in the form of illegal file sharing among consumers (i.e., piracy) (Papies & van Heerde, 2017). For users of illegal copies of computer programmes and multimedia content (movies, games, music), and users of P2P- networks, which copyrighted works were made available to the public and disseminate via the Internet, their actions may expose them to prosecution (Šterk & Petek, 2016). Furthermore, the illegal copying of data, selling pirated copies of computer programmes, and the possession and use of illegal copies is illegal in most countries. According to Bernik and Meško (2011), minors (and also adults) generally do not know that piracy is forbidden, just as much as theft is, so they should be made aware of the illegality of these actions, as most young people still perceive piracy as something normal and acceptable. Some factors are ambiguous: For example, downloading music or video hosting is funny, and creative, but you can break copyright, or exploit intimacy, or facilitate hostile interactions. Other risk factors are associated with the misuse of personal data in different ways. For example, minors can get into trouble if they are not aware of the consequences of reckless sharing of their personal information, as it can affect their online reputation, and it may facilitate the contact with a person that may wish to abuse them.

- **Internet addiction:** Internet addiction has appeared as a new mental health concern (Kuss & Lopez-Fernandez, 2016) and it is growing, with parallel efforts of researchers and

clinicians to measure it, and to decide whether the Internet is addictive in the same way as alcohol or drugs. Although the issue of "addiction" remains controversial, a consensus is growing that the "excessive" use of the Internet is worthy of investigation on the basis of preliminary measurements of "addiction" to computer games, where the Internet supplants the minors's social or personal needs in a way that cannot be controlled (Livingstone et al., 2011). However, Internet addiction is associated with psychosocial maladjustment in adolescence, and is a widespread problematic behaviour (Müller, et al., 2017).

According to Livingstone et al. (2011), the levels and patterns of Internet use are important in understanding the risks, as well as the opportunities, given that they form the context in which children are exposed to risk factors for which the policy should provide adequate safeguards. It is important that access rates and methods increase and vary, so that the security policy expands and becomes more diversified in order to keep up with the trends in a rapidly changing environment. It should be noted, in particular, that the policy must respond to new protection needs arising from children who start to use the Internet at a more tender age, as well as from the increase in the proportion of children who use the Internet independently of adult supervision, especially through mobile technology. "Digital Literacy" (or "media literacy" or "ability") plays an important role in a child's Internet usage.

For young children, it is already necessary to control the use of new technologies. When children become older, one should establish a dialogue for the safe use of the Internet and mobile devices, and what children may resort to, technologically, what they are to watch and with whom they may safely socialise. The educational process is, therefore, very similar to that in the real world. But, according to Završnik (2017), the ethical risks of new technologies can already be taken into account in the technological design. However, we must accept the fact that the Internet and other new technologies have become an important part of the social life of most children and adolescents.

4 Neverending Deep Web's Forensics' Investigation

The Dark Web is a small part of the Deep Web, which is deliberately hidden and inaccessible through standard web browsers (Anticounterfeiting Committee, 2015), and is home to hidden sites that would rather stay in the dark (Cole, 2016). Today's Internet has multiple layers. According to Europol (2014), the surface web is what Google and other search engines index links are based. Essentially, the surface web is the master index of publically available indexes providing returns to searches based on search terms and links. The surface web is small, constituting only 4% of the whole web. The second, called the Deep Web, consists of roughly 96%, or the rest of the web. The Deep Web consists of protected sites that require users to input data to get access (email or online banks), unlinked content (unpublished blogs or organisational databases), proprietary data (study results, financial records, research & development), and personal data (medical records or legal documents) (Cole, 2016). The Deep Web is generally inaccessible and hidden from the typical Internet search. It is a self-contained market place that functions under a set of informal institutions (Hardy & Norgaard, 2016). Standard search engines do not have access to these sites, and, therefore, it cannot be easily found. The deepest Web is the Dark Web, which requires specific software, logins, and knowledge on how to access it. There, the majority of underground forums, criminal marketplaces, and various other sites are hosted, and can be accessed via the Tor (The Onion Router) browser, as these sites use onion URL's instead of the normal website extentions such as .com, .net, and .org. (AlphaBay Market, 2017), and through so-called proxy sites that enable the user to browse the Tor network through a regular web browser. Sites on the Dark Web are usually porn sites, fetish sites, forums, blogs, and darknet markets that are full of drugs, porn, weapons, counterfeit items, stolen data, compromised credit card information, fake documents, hacking goods, and offering services like hiring killers, and the like. Specialised forums and chat rooms found in this part of the web have been created in virtual space to allow networking, and to form trustworthy underground markets for illicit drugs, prostitution, and child pornography markets, and ideological deviant groups to incite terrorism, engage in espionage, view sexual abuse of children live, engage in harmful health risks such as "bugchasers" who seek sexual interactions with HIV-infected persons, or to participate in illegal medical experiments normally carried out on the homeless. These forums provide widespread outreach across the globe, establish reputations of sellers of illicit goods or services through customers' reviews, allow the sharing of evasive strategies to avoid arrest, and create market norms that deter cooperation with law enforcement (Jaishankar, 2011; Lavorgna, 2014).

The most relevant aspect of the Deep Web is anonymity all its levels. Each buyer and seller is known by a unique name; their true identity remaining unknown and untraceable. The most used software is Tor, which was founded originally by the US Navy at the start of the Millennium and is used by numerous agencies to transmit and receive sensitive information (Luo & Liao, 2007). Tor software encrypts web traffic in layers, and redirects that traffic around the world through randomly-chosen computers, each of which removes a single layer of

encryption before passing the data on to the next computer in the network. The goal of such a process is to prevent anyone – even anyone who controls one of those computers in the encrypted chain – from matching the traffic's origin with its destination. When web users run a Tor browser, the sites they visit cannot detect the web user's IP address. Tor also provides anonymity to websites and other servers, which are configured to receive inbound connections through Tor only, and are called "hidden services." Tor is necessary to access hidden services through their onion address, which hides the service's server IP address (hence its network location). The Tor network recognises these addresses and routes data to and from hidden services, including those hosted behind firewalls, while preserving the anonymity of both parties (Anticounterfeiting Committee, 2015). When users communicate through the surface web, their messages are unencrypted and travel directly from sender to receiver. According to Hardy and Norgaard (2016), messages are 'bounced' between nodes in the Tor network, making them virtually untraceable. The random path the message takes, coupled with its encryption while travelling through the network, secures the anonymity of the users and security of the content. Equally, according to Luo and Liao (2007), within the Tor, one can mask one's identity and travel the surface web with total anonymity. Transactions of ordered goods are also anonymous.

The transaction of ordered online goods may be analysed by looking into the Agora market. All products bought from this site are usually delivered by a private courier, thereby minimising the risk of detection (Agora Drugs, 2017; Anticounterfeiting Committee, 2015; Hardy & Norgaard, 2016; Upadhyaya & Jain, 2016). Such need is justified, given the fact that things that are sold on these online stores are often illegal, and the intentention is to keep the identity of both the seller and the buyer anonymous. Therefore, sending money by post physically is absurd, as it reveals the sender`s and the recipient's addresses. The same applies to the transfer of banking and credit card or transaction accounts. Therefore, for online transactions on the Deep Web, currency is used as a means of payment, especially Bitcoins. They are used as payment for criminal services or to receive payments from victims of extortion. Bitcoin is a computer currency, which is encrypted, and is based on open source protocol. Since the value of the currency varies from hour to hour on the Stock Exchange, it is impossible to determine how much it will be worth tomorrow[3]. According to the Anticounterfeiting Committee (2015), and Hardy and Norgaard (2016), a bitcoin is electronic money, a crypto-currency that does away with the need for banks by combining a limited quantity digital currency with state-of-the-art cryptographic security and a peer-to-peer network. All transactions are irreversible and also free, unlike Visa or PayPal.

According to Lusthaus (2013), another area of the Dark Web is the "bulletproof hosting", whereby the provider secures a place for cybercriminals to operate illegal activities, safe from being shut down by the authorities. As a result, such bulletproof hosting is very attractive to cybercriminals, and is well-known for providing services to pornography sites and spammers, among others.

According to Europol (2016), given the additional challenges inherent to undertaking investigation on the Darknet presented to the law enforcement agents, effective deconfliction, collaboration and the sharing of intelligence is essential. The adoption of the enumerated (necessary) measures helps to prevent duplication of effort, facilitate the sharing of tactics and tools, and increase understanding of the threat. Darknet and surface net platforms also allow the exchange of techniques for dodging and hindering law enforcement activities. Mutual support and camaraderie is a worrysome trend.

The Internet facilitates deviance and crime by providing visibility and accessibility to alternative justifications and normative viewpoints on forms of cyber crime. The fragmented and layered nature of the Internet has beeb proven to stimulate deviant and criminal activity, given that there is no control body that not only establishes rules, but also monitors its compliance, enforcing an appropriate set of rules of conduct and cyber criminal laws in specific countries, as well as applying the corresponding sanctions. Unlawful behaviour is, in some countries tolerated, and the same happens to illegal behaviour in other countries, allowing offenders to choose between several more or less permissive jurisdictions for hosting their websites. These cyber criminals tend to chose those countries where the least harsh legal consequences are foreseen. Moreover, maintaining anonymity or bogus identities during the commission of crime is easier in virtual space than in a real physical space. Apps, avatars, disposable devices, and the Deep Web, where search engines cannot detect websites due to an added layer of security, facilitate the concealment of criminal transactions, socialization into subcultures, and networking of those involved in illicit or nonconventional behaviour (Jaishankar, 2011; Lavorgna, 2014).

Although the Dark Web is known to be a safe haven for those who traffic drugs, weapons, counterfeit documents and child pornography, not everything on the Dark Web is "illegal." According to the Anticounterfeiting Committee (2015), there are some who use the Dark Web for legitimate purposes. For instance, many activists and political dissidents use the

[3] Example: The value of a bitcoin on April 5, 2017, was $ 1,131.62 (CoinDesk, 2017).

Dark Web to exercise their right to express their opinions freely, or as a way to exchange and receive information that is censored or controlled.

5 Reported Cyber Crimes in Slovenia

The Internet, mobile applications, and information technologies are now embedded in social structures, finances, health, education and business in many countries around the world. More than three and a half billion of the world`s population used the Internet in 2017 (Internet live stats, 2017). Availability and efficiency of the Internet and the information technology infrastructure to support social institutions promote the development of cyber crime and deviant subcultures (Stalans & Finn, 2016).

According to Bernik and Meško (2011), technology is accessible to everyone today, work procedures are simplified to the point where the use of devices and communication systems can be used without any previous knowledge, and there is no need understand what is actually happening in the background, the cyberspace. The lack of understanding of the functioning of the cyberspace leads to misusage of several necessary preventive measures, or, in an easier word, self-protection. As a consequence of the lack of attention to protection and lack of awareness, in many cases the criminals operate by taking advantage of the ignorance of the users. The number and types of offences in Slovenia for the period 2011-2015 forselected criminal violations which are connected to the Internet, are presented in Table 1.

Table 1: The number and type of offences in question for the period 2011-2015 in selected criminal indications, which are connected to the Internet (Policijska akademija, 2017).

Article in the Criminal Code of the Republic of Slovenia	Description of Classification of violations	Criminal designation	Year and Number of offences					
			2011	2012	2013	2014	2015	Total
139	**Violation of secrecy of communications**	Accessing the contents of a message transmitted online.	1	0	0	0	0	**1**
140	**Unlawful Publication of Private Writings**	On the Internet	0	0	0	1	0	**1**
143	**Abuse of personal data**	Unauthorised use of personal data	23	20	23	16	12	**94**
		Unauthorised publication of personal data	17	4	0	1	1	**23**
		Unlawful use of personal data online (assuming someonelse's identify)	18	5	7	3	6	**39**
148	**Copyright Violation**	Illegal reproduction of and distribution of copyright protected computer programmes	0	0	1	1	0	**2**
158	**Insult**	On the Internet	0	1	12	5	4	**22**
		Online Publications	7	5	13	1	9	**35**
159	**Slander**	Circulating false information on the Internet	0	1	3	0	1	**5**
		Authoring Online Publications capable of damaging the honour of reputation	6	0	1	1	1	**9**
160	**Defamation**	Circulating false information on the Internet	0	1	1	0	3	**5**
		Publishing false information that is considered to be damaging	1	5	6	2	2	**16**
165	**Insult to the Slovenian People or National Communities**	Online Publications of Insult, Slander and defamatory statements against the Slovenian people or against the Hungarian or Italian national communities living in the Republic of Slovenia	0	1	0	0	0	**1**

175	**Exploitation through Prostitution**	Advertisement of sexual services with the pourpose of exploring another person	2	1	1	0	0	**4**
176	**Presentation, manufacture, possession and distribution of pornographic material**	Online comercialization, presentation or publicity of material of pornograph material concerning minors	32	14	11	21	16	**94**
211	**Fraud**	Unlawful online trade (spoofing)	49	55	61	83	73	**321**
		Abuse of payment / credit card fraud on the Internet	35	34	55	81	52	**257**
221	**Attack on Information Systems**	Usage of spyware (sniffer)	3	1	0	0	0	**4**
		Illegal interception of usernames, passwords	9	9	10	2	6	**36**
		Illegal use of data in an information system	2	11	25	5	3	**46**
		Interfering with data transmission	0	1	37	4	0	**42**
		Intrusion of Internet	15	22	41	19	64	**161**
		Intrusion to workstation	0	0	0	1	0	**1**
		Intrusion in network / server	5	3	2	5	2	**17**
237	**Breaking into Business Information Systems**	Tampering with operating information systems	0	1	0	0	0	**1**
		Interfering with data transmission	1	0	1	0	0	**2**
		Intrusion of Internet	0	1	2	0	1	**4**
		Assault through the "side door" (former programmers…)	0	0	1	0	0	**1**
		Intrusion in a workstation	0	1	1	0	0	**2**
		Intrusion in network / server	0	1	1	0	1	**3**
247	**Use of a Counterfeit Bank, Credit, or Other Card**	Acquiring card information or the recognition of unlawfully copied cards through the Internet	85	93	658	105	149	**1.090**
306	**Manufacture and Acquisition of Weapons and Instruments Intended for the Commission of Criminal Offences**	Commercialization of unauthorised criminal devices online	2	1	0	0	0	**3**
		Commercialization of unauthorised criminal tolls online	0	0	0	1	0	**1**
Total			310	288	934	354	405	**2.291**

* Individual offences may have linked several criminal indications

In Slovenia, reported cyber crime and its enforcement is relatively low (Policija, 2011). The lack of reporting is probably due to the fact that people are feeling embarrassed, under a stong belief that it's "their fault" that they lacked awareness and that they were " tricked", and at the same time, experiencing a feeling of guilt. Those two feelings, guilt and shame, are probably the basis of non-reporting of cyber crime. The use of counterfeit, non-cash means of payment with acquisition through the Internet has recorded 1,090 offences from 2011 to 2015. Next are two forms of fraud; the first is false trading on the Internet, or spoofing, with 321 acts counted in the same timespan, and misuse of payment or credit card use on the Internet, with 257 offences in the same time frame. According to Bernik and Meško (2011), this does not mean that users are less afraid or are not aware of threats, and do not take into account the risk factors. The fact that there are minor threats from cyberspace in Slovenia is, among other things, a consequence of the Slovenian language being an active language mastered by only 2 million people, and the contents, before the global threats, are "encrypted" linguistically.

Due to the nature of cyber crime, few activities associated with cyberspace are prosecuted. The power of formal social control in the case of complex offences is significantly lower

than in the case of minor acts of violence (often refered to as torts) and property crime. Responding to cyber crime requires specialization and the ability to collect evidence so that the perpetrators are monitored and may be properly punished. The problem is the lack of clarity as to what cyber crime actually is and what actions should be penalised. An important question is whether the fear of cyber crime is justified, and whether people are actually at risk from this type of crime. Threat perception and awareness of it and fear of the use of cyberspace depend on the individual user, but as discussed by Japelj (2016), in accordance with technological development, it is reasonably expected that the number of such offences will increase in the long run.

6 Conclusion and Discussion

Whatever the image of a lonely child in front of the computer, children live most of their lives in different types of social interactions, some of which can be transmitted to their use of the Internet. When promoting media and digital literacy skills and inclusion of the audience in the media, it is absolutely necessary to achieve security and the protection of vulnerable social groups in cyberspace, including children and adolescents. As for the protection of minors from inappropriate behaviour online it is, according to Livingstone, et al. (2011), important to use the privacy settings, which limits the access to their public profile on the social network. Furthermore, it is important to know that, in the social network, it can only be published information, photos, comments, videos, that is to be accessible by others. Nude photographs, offensive, and defamatory comments do not belong on the Internet, even though they are made available to all users and, once published, remain online until its contents are required to be deleted, according to Directive 95/46/EC of the European Parliament and of the Council of 24 October, 1995, for the protection of individuals with regard to the processing of personal data and on the free movement of such data (European Parliament & Council, 1995). Minors must also be careful when posting personal information about other people without their permission, including photographs as it can also be a criminal offence. Inappropriate content, contacts or harassment should be reported, even on their own website social networks, where the mechanisms to report abuse already exist. It is also important that the passwords are kept to oneself and that they are changed frequently.

The most relevant sources of social support and awareness rasing methods for minors on the safe use of the Internet are outlined beow (Bertok, Wikström, Hardie, & Meško, 2012; Livingstone et al., 2011):

- Parents: There should be enhanced parental awareness of risks and online safety. Parents must inform children as to the nature of the risks that they are to likely to encounter on the web, it can be achieved by encouraging dialogue and greater understanding between parents and children in relation to online activities of young people. The balance between parental education and the parents' trust in the child which deals with the online experience, is a difficult task to achieve. However, the more children trust their parents, and the more parents are informed qas to their children's whereabouts, the less likely it will be for those children to engage in delinquent behaviour.

- Teachers: Teachers should be the most trusted source of information on Internet safety.

- Peers: Minors would rather turn to their friends than talk to an adult if they are worried or annoyed about something on the Internet. However, little is known about whether and how the minors are, in fact, mutually supportive to each other in terms of Internet safety.

- Additional Resources: There are also additional sources of information for children on how to use the Internet safely. These are: Other relatives, mass media, websites, governments and regulators, industry etc. Governments and regulators, for example, could encourage the development of positive online content through funding programmes, schemes and production incentives. Industry – this applies to Internet service providers, content developers, service developers or the representative industry associations – plays a key role in facilitating and promoting online safety. The industry also has a strong interest in ensuring that minors have a positive experience online.

Education and training on the dangers of cyber crime must become a part of everyday life at all levels of social interaction, to enable an informed individual to use the Internet thoughtfully and responsibly without fear of abuse (Bernik & Meško, 2011). However, law enforcement, policy makers, legislators, academia and training providers need to become even more adaptive and agile in addressing the phenomenon. Law enforcement needs to have the tools, techniques and expertise to counter the criminal abuse of encryption and anonymity (Europol, 2016). We also showed how dangerous the Internet can be and, despite all the protection you can get today, there are still paths where someone accesses personal data and abuses them.

According to Europol (2016), prevention campaigns should not focus solely on preventing citizens and businesses from becoming victims of cyber crime, but also on preventing potential cybercriminals from becoming involved in such

activity. Such campaigns must highlight the consequences of cyber crime for both the victim and the perpetrator. The criminals themselves have also been changing. They have become more industrialised, forming an underground economy. They specialise in different services, such as recruiting money mules, distributing malware, maintaining botnets, etc., and sell these services to other criminals. The technical expertise needed is decreasing as criminals move to a «Crime-as-a-Service» model, where cybercriminal activity is easier to execute, and support from the seller is provided. Criminals are creative and and are always looking for and finding new ways to commit crimes. The global crime fighting community needs to evolve, together with the criminals, to keep society safe. In 2001, the Council of Europe accepted the Convention on Cyber crime (Council of Europe, 2001), which is intended to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, and provide facilitating criminal offences` detection, investigation and prosecution at both the domestic and international levels by providing arrangements for fast and reliable international cooperation. Slovenia should also follow the recommendations of the EU.

Cyber crime activity is growing fast and evolving at a rapid pace, becoming both more technically proficient and aggressive. Tackling the threat of cyber crime requires a broad-based strategy that recognises the diversity of offences, actors, and motivations (Saunders, 2017). In the last decade, cyber crime and cyber-enabled crime have grown in parallel with rapid developments in technology, and show no signs of decelerating anytime soon (Europol, 2016), which is a very worrysome trend.

One barrier may be that cases are dismissed due to insufficient evidence, which reinforces the invulnerability of perpetrators. Cyber-forensics involves the scrutiny of hard discs on computers/digital devices, and searching for 'digital footprints' to uncover a perpetrator's actions (Kaur, Kaur, & Khurana, 2016). Cyber-forensic methods ultimately lead to a specific computer/device and not a person who can be prosecuted (Bocij, 2004; Griffiths, Rogers, & Sparrow, 1998). The simplification of collection of evidence has been made easier by means of cyber-forensic measures, simplifying also the establishment of the burden of proof, and allowing the tracing of perpetrators who attempt to remain anonymous (Salter, 2016; Wall, 1998). However, cyber-forensics places high demand on resources (i.e., time, money, and technology) that may impact detrimentally on apprehending perpetrators. Furthermore, perpetrators of cyber crime are becoming more adept at utilising anti-forensic measures as technology advances (Millman, Winder, & Griffiths, 2017; Yeboah-Boateng & AkwaBonsu, 2016). However, in the field of cyber crime, forensics has much work to do, especially in the Deep Web, because it will take a lot of research, investigation, discovery and additional work, so the users of the darkest pages in the Deep Web are also easier to track and, ultimately, will be discovered and punished for their most wicked acts on the Neverending Deep Web.

This study provides a sample of all crimes reported in Slovenia since 2011, out of which we only address those related to cyber crimes. Its major limitations are that not all crimes are reported, and that a more profound approach is still difficult, as first instance court decisions are not easily accessible to the public, so the outcome of those complaints reported to the Police cannot be analysed, nor can it be determined how many did, in fact, end up in Court as a matter of Criminal Court litigation. A further limitation is the fact that we have investigated Deep Web (and Darknet), which, because of their complexity and hidden nature, are still quite unexplored, as forensics in this field are not the most effective. We wanted to find out whether any criminal web acts had been discovered in Slovenia within an anonymous web, and to conduct a structured interview with a competent person in the Slovenian Police, but our request was rejected.

References

1. Agora Drugs. (2017). *How to find agora drug market and stay anonymous*. Retrieved from https://agoradrugs.com/
2. AlphaBay Market. (2017). *Some users panic as AlphaBay Market temporarily went offline*. Retrieved from https://alphabaymarket.com
3. Anticounterfeiting Committee. (2015). *Report: Anticounterfeiting on the Dark Web.* Anticounterfeiting Committee, U.S. Subcommitee, Public Awareness Task Force. Retrieved from http://www.inta.org/Advocacy/Documents/2015/ACC%20Dark%20Web%20Report.pdf
4. Bernik, I., & Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto [Internet study of familiarity with cyber threats and fear of cybercrime]. *Revija za kriminalistiko in kriminologijo*, *62*(3), 242–252.
5. Bertok, E., Wikström, P. O., Hardie, B., & Meško, G. (2012). Starševski nadzor nad najstniki v osnovni in srednji šoli ter s tem povezana odklonskost [Parental control of teenagers in primary and high school and related deviance]. *Revija za kriminalistiko in kriminologijo*, *63*(4), 311–320.
6. Bocij, P. (2004). *Cyberstalking: Harassment in the internet age and how to protect your family*. Westport: Praeger.
7. Broadcasting Council. (2011). *Ocena stanja na področju radiodifuzije in predlogi Državnemu zboru Republike Slovenije za izboljšanje stanja* [Assessment of the situation in the field of broadcasting and proposals to the National Assembly of the Republic of Slovenia for the improvement of the situation]. Ljubljana: SRDF.
8. CoinDesk. (2017). *Bitcoin.* Retrieved from http://www.coindesk.com/price/

9. Cole, J. (2016). Dark Web 101. *Air & Space Power Journal*, *1*(2), 3–8.
10. Council of Europe. (2001). *Convention on cybercrime*. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
11. European Parliament and Council. (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Retrieved from: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
12. Europol. (2014). *The Internet Organised Crime Threat Assessment (IOCTA) 2014.* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014
13. Europol. (2016). *Internet Organised Crime Threat Assessment (IOCTA) 2016.* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
14. Europol. (2017). *European Cybercrime Centre – EC3.* Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
15. Golding, P., & Splichal, S. (2014). *Media in Europe: New questions for research and policy*. Strasbourg: ESF.
16. Griffiths, M., Rogers, L., & Sparrow, P. (1998). Crime and IT: "Stalking the Net". *Probation Journal, 45*(3), 138–141. doi: 10.1177/026455059804500303.
17. Hardy, R. A., & Norgaard, J. R. (2016). Reputation in the Internet black market: An empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics*, *12*(3), 515–539.
18. Institute for Market and Media Research. (2013). *Redna letna raziskava stanja medijskega pluralizma v republiki Sloveniji za leto 2012 na področju slovenskih tiskanih medijev, radijskih in televizijskih programov ter elektronskih publikacij* [Regular annual survey of the state of media pluralism in the Republic of Slovenia for 2012 in the field of Slovene printed media, radio and television programs and electronic publications]. Ljubljana: Mediana.
19. Internet live stats. (2017) *Internet live stats*. Retrieved from http://www.internetlivestats.com/
20. Jaishankar, K. (2011). *Cyber criminology: Exploring Internet crimes and criminal behavior*. Boca Raton: CRC Press.
21. Japelj, B. (2016). Kriminaliteta v Sloveniji leta 2015 [Crime in Slovenia in 2015]. *Revija za kriminalistiko in kriminologijo*, *67*(2), 140–170.
22. Karmakar, S. (2016). Popular conceptions of crime: as created by the media. *International Journal of Social Science & Interdisciplinary Research*, *5*(5), 61–68.
23. Kaur, M., Kaur, N., & Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. *International Journal of Advanced Research in Computer and Communication Engineering*, *5*(1), 23–28. doi:10.17148/IJARCCE.2016.5106.
24. Kuss, D. J., & Lopez-Fernandez, O. (2016). Internet addiction and problematic Internet use: A systematic review of clinical research. *World Journal of Psychiatry*, *6*(1),143–176.
25. Lavorgna, A. (2014). Internet-mediated drug trafficking: Towards a better understanding of new criminal dynamics. *Trends in Organized Crime*, *17*(4), 250–270.
26. Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. London: EU Kids Online.
27. Lorang, M. R., McNiel, D. E., & Binder, R. L. (2016). Minors and Sexting: Legal implications. *The Journal of the American Academy of Psychiatry and the Law, 44*(1), 73–81.
28. Lovrec, V., & Žišt, D. (March 8, 2017). Policija na sledi izprijencem [Police on the trail of evildoers]. *Večer*, p. 26.
29. Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security, 16*(4), 195–202.
30. Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52–60.
31. Markelj, B., & Završnik, A. (2016). Kibernetska korporativna varnost mobilnih naprav: zavedanje uporabnikov v Sloveniji [The corporate cyber security of mobile devices: The awareness of Slovenian users]. *Revija za kriminalistiko in kriminologijo*, *67*(1), 44–60.
32. Millman, C. M., Winder, B., & Griffiths, M. D. (2017). UK-based police officers' perceptions of, and role in investigating, cyber-harassment as a crime. *International Journal of Technoethics*, *8*(1), 87–102.
33. Müller, K. W., Dreier, M., Duven, E., Giralt, S., Beutel, M. E., & Wölfling, K. (2017). Adding clinical validity to the statistical power of large-scale epidemiological surveys on internet addiction in adolescence: A combined approach to investigate psychopathology and development-specific personality traits associated with internet addiction. *Journal of Clinical Psychiatry*, *78*(3), 244–251.
34. Papies, D., & van Heerde, H. J. (2017). The dynamic interplay between recorded music and live concerts: The role of piracy, unbundling, and artist characteristics. *Journal of Marketing*, *81*(4), 67–87.
35. Policija. (2011). *Kriminaliteta* [Crime]. Retrieved from http://www.policija.si/index.php/statistika/kriminaliteta
36. Policijska akademija. (2017). Število in vrsta obravnavanih kaznivih dejanj za obdobje 2011–*2015 po izbranih kriminalitičnih označbah, ki so vezane na internet* [Number and type of criminal offenses investigated for the period 2011–2015 according to selected Internet crime-related identifiers]. Ljubljana: Center za raziskovanje in socialne veščine Policijske akademije.
37. Popham, J. (2017). Microdeviation: Observations on the significance of lesser harms in shaping the nature of cyberspace. *Deviant Behavior*. doi: 10.1080/01639625.2016.1263085.
38. Salter, M. (2016). Privates in the online public: Sex(ting) and reputation on social media. *New media & society*, *18*(11), 2723–2739.
39. Saunders, J. (2017). Tackling cybercrime – the UK response. *Journal of Cyber Policy*. doi: 10.1080/23738871.2017.1293117.
40. Splichal, S. (2016). Raziskovanje medijev in novinarstvo: »integralnost« med javnostjo in profesijo [Media research and journalism: »integrity« between the public and the profession]. *Javnost - The Public*, *22*, 17–27.
41. Stalans, L. J., & Finn, M. A. (2016). Understanding how the internet facilitates crime and deviance. *Victims & Offenders*, *11*(4), 501–508.
42. Stratton, G., Powell, A., & Cameron, R. (2016). Crime and justice in digital society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy, 6*(2), 17–33.
43. Šterk, T., & Petek, A. (2016). *Napotki za otrokom prijaznejši internet* [Tips for a child-friendly internet]. Ljubljana: Točka osveščanja o varni rabi interneta SAFE.SI.
44. Tanis, M., van der Louw, M., & Buijzen, M. (2016). From empty nest to social networking site: What happens in cyberspace when children are launched from the parental home? *Computers in Human Behavior, 68*, 56–63.
45. Tomažič, T. (2017). The importance of social media from the wine marketing perspective. *Lex localis – Journal of Local Self-Government*, 15(4), 827–844.

46. Tsikrika, T., Akhgar, B., Katos, V., Vrochidis, S., Burnap, P., & Williams, M. L. (2017). WSDM ,17 Proceedings of the Tenth ACM International conference on web search and data mining. *1st International workshop on search and mining terrorist online content & advances in data science for cyber security and risk on the web*. ACM New York, USA. doi 10.1145/3018661.3022760.
47. Upadhyaya, R., & Jain, A. (2016). International Conference on computing, communication and automation (ICCCA2016). *Cyber Ethics and cyber crime: A deep delved study into legality, ransomware, underground web and bitcoin wallet*. Greater Noida, India.
48. Vaillancourt, T., Faris, R., & Mishna, F. (2017). Cyberbullying in children and youth: Implications for health and clinical practice. *The Canadian Journal of Psychiatry, 62*(6), 368–367.
49. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Malden: Polity Press.
50. Wright, M. F. (2017). Adolescents' perceptions of popularity-motivated behaviors, characteristics, and relationships in cyberspace and cyber aggression: The role of gender. *Cyberpsychology, Behavior, and Social Networking*, *20*(6), 355–361.
51. Yeboah-Boateng, E. O., & Akwa-Bonsu, E. A. (2016). Digital forensic investigations: Issues of intangibility, complications and inconsistencies in cyber-crimes. *Journal of Cyber Security*, *4*(2), 87–104.
52. Završnik, A., & Sedej, A. (2012). Spletno in mobilno nadlegovanje v Sloveniji [Internet and mobile phone bullying]. *Revija za kriminalistiko in kriminologijo*, *63*(4), 263–280.
53. Završnik, A. (2017). Algoritmično nadzorstvo: veliko podatkovje, algoritmi in družbeni nadzor [Algorithmic control: large data, algorithms and social control]. *Revija za kriminalistiko in kriminologijo*, *68*(2), 135–149.
54. Zulkarnine, A., Frank, R., Monk, B., Mitchell, J., & Davies, G. (2016). *Surfacing collaborated networks in dark web to find illicit and criminal content.* Canada: International CyberCrime Research Center (ICCRC).

Kriminalne dejavnosti v kibernetskem prostoru: od varstva mladoletnikov do globokega spleta

Dr. Tina Tomažič, docentka, Fakulteta za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, Slovenija.
E-pošta: tina.tomazic@um.si

Noemia Bessa Vilela, višja raziskovalka, Inštitut za pravne raziskave Portucalense,
Univerza Portucalense Infante D. Henrique Porto, Portugalska. E-pošta: noemia@uportu.pt

Nove tehnologije so nam popolnoma spremenile življenje. Prinesle so nov način komunikacije, večjo dostopnost in ogromno drugih koristi, vendar pa žal tudi spletne zlorabe, neprimerno vedenje na spletu, večjo kontrolo in nadzor ter tudi razne odvisnosti. Predvsem mladostniki so izredno hitro osvojili različne možnosti uporabe in tudi zlorabe novih tehnologij, saj se ne zavedajo vseh posledic, ki jih prinaša neprimerno vedenje na spletu ter zloraba le-tega. V našem članku proučujemo, kako otroke in mladostnike obvarovati pred neprimernim vedenjem na spletu, saj lahko zlahka prav vsi dostopajo do vsebin in stikov, ki zanje niso primerni. Nadalje raziskujemo, katera kazniva dejanja, storjena preko spleta, se najpogosteje pojavljajo v Sloveniji. Marsikdo se ne zaveda, da takoj, ko se priključimo na splet, razkrijemo svojo identiteto. Če želimo ostati anonimni, obstaja še veliko obsežnejši anonimni splet, t. i. globoki splet (angl. *deep web*). Glavni namen tovrstnih spletnih območij je izmenjava informacij, ki niso namenjene širši javnosti in se pogosto uporabljajo za kriminalna spletna dejanja, ki vključujejo trgovanje s prepovedanimi drogami, finančne prevare, nezakonito orožje, vohunjenje, spolne zlorabe otrok itd. V našem prispevku raziskujemo, kaj je zloglasni globoki splet, kako deluje, kakšen del globokega spleta predstavlja temni splet (Darknet) in zakaj je tako nedotakljiv, saj niti forenzične raziskave na tem področju niso uspešne, ker je le-ta preveč kompleksen in neskončen.

Ključne besede: kibernetska kriminaliteta, nove tehnologije, globoki splet, temni splet, Slovenija

UDK: 343.3/.7:004

View publication stats