DOI: 10.5604/01.3001.0012.9839 ASEJ ISSN: 2543-9103 ISSN: 2543-411X (online)

New threats in the cyberspace based on the analysis of The Onion Router

Anna Nastuła[1]

[1]The Department of Law and Administration, Universitas Opoliensis

Abstract — **New technologies transform modern societies and create new threats related to anonymity on the Internet. The aim of the present paper is to outline the history, functioning and current scope of application of The Onion Router. The paper analyses the issue of anonymity on the Internet which triggered a number of international, social and political problems and became the driving force for the development of TOR network. The author discusses the significance of TOR network for free flow of information and freedom of social communication and shows the wide thematic range of its resources. Other issues presented in the paper include: the payment system used in TOR network which is based on Bitcoin, a cryptocurrency which proved to be an ideal form of payment in illegal transactions; the most frequently committed cybercrimes and new, previously unknown forms of illicit cyberbehaviour based on anonymizing technologies which pose a challenge for law enforcement agencies and the judicial systems. TOR network by offering full *anonymity to the world of crime,* considerably contributes to the development of cybercrime and takes the illegal activity in an entirely new dimension. TOR network although originally created with good intentions, has turned into a global threat.**

Key words — TOR network, the Internet, cybercrime, threats, the Deep Web, the darknet

I. INTRODUCTION

The development of new technologies and wide access to the Internet causes an unprecedented increase in the number of threats in the cyberspace. Along growing number of the Internet users grows the number of potential victims. Technological advances are closely followed by members of the criminal underworld who are keen to use the well-meaning inventions and solutions for their evil purposes. Due to the volume of information disclosed by Edward Snowden and the recent Facebook–Cambridge Analytica data scandal, the issue of privacy protection has become the centre of attention of the public opinion. Nowadays, privacy protection on the Internet translates into the desire for full anonymity which gives the users individually understood feeling of security which may lead to the manifestation of behaviours which do not occur in the real world.

II. ONLINE ANONYMITY – ADVANTAGES AND DISADVANTAGES

Anonymity is becoming a more and more desirable value. In the positive aspect, anonymity is a driving force of communication, protecting individual rights and igniting bottom-up social movements. On the other hand, *anonymity* carries a series of threats and opens channels for conducting propaganda and disinformation activity while leaving those affected without any help. It must be emphasized that anonymity and privacy are two different concepts. The word anonymity is derived from the Greek word ‘anonymia’ meaning namelessness (Weber and Heinrich, 2012). Nowadays, *anonymity* is defined as the lack of possibility to identify an individual among other members of the same community. Privacy, in turn, is protected by regulations of constitutional rank and by international acts. Citizens can enjoy the right to privacy as it is guaranteed by legal systems of particular countries, the same, however, cannot be said of *anonymity*. As noticed by Brunon Hołyst, privacy assumes ‘the existence of boundaries, within which it is allowed to exert social pressure in order to obtain a real picture of occurrences. The privacy principles decide who may disclose the hidden information and to whom’ (Hołyst, 2014). These elements cannot be found in the notion of *anonymity*.

A*nonymity* combined with the absence of transparent legal regulations and rules of conduct in the cyberspace, makes the Internet a friendly zone for criminals. The latest technological solutions which have been developed with good intentions, in the hands of evil people generate more and more crime-inducing acts. Development of anonymisation tools, of which the TOR router is a perfect example, triggers new crime opportunities in the cyberspace which are very difficult to detect and prevent.

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 22, No 4 (2018), 6 pages
DOI: 10.5604/01.3001.0012.9839
Received: 06 December 2018; Accepted: 14 December 2018

Regular research paper: Published: 07 January 2019
Corresponding author’s e-mail: k.anna.nastula@gmail.com

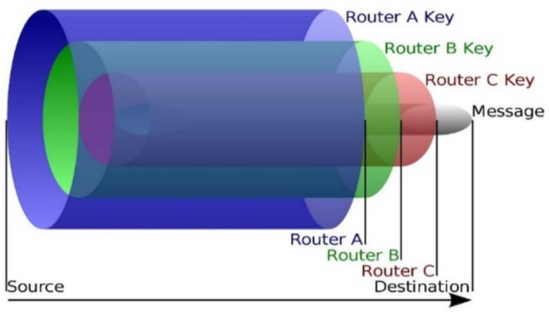
III. THE SURFACE WEB AND THE DEEP WEB

We are all now connected by the Internet, like neurons in a giant brain. This statement by Stephen Hawking reflects the scale and significance of social communication on the Internet which is now the biggest source of information and the platform for data transfer. While browsing the resources of the Internet by means of popular search engines, the user only touches upon the first layer (the Surface Web also referred to as the Clearnet). According to The Ultimate Guide to the Invisible Web, it is estimated that the most frequently used part of the Internet (the Surface Web) is just 0,03% of the whole web. The Clearnet is only the top of the iceberg of an extended, multi-layered network. The fundamental part of the world wide web is known as the Deep Web and is unavailable for users of the popular search engines. The term Deep Web was used for the first time in 1994 by Jill Ellsworth who referred to the parts of the world wide web whose contents are not indexed by standard web search engines so they are invisible or inaccessible for the Surface Internet users (Bergman, 2001) .The Deep Web is the most rapidly growing category of the world wide web. Within its resources there are websites of the National Aeronautics and Space Administration (NASA), specialist databases, internal websites or contents of the world libraries. A part of the Deep Web is called the Dark Web or the darknet, infamously known as the dark side of the Internet. The darknet differs from other peer-to-peer distributed networks because its sharing resources are completely anonymous as IP addresses are not disclosed (Wood, 2010). The darknet hosts networks whose contents are accessible through connections made by special types of software such as I2P (Invisible Internet Protocol), GNUnet and TOR network.

IV. STRUCTURE OF TOR NETWORK

The Onion Router (TOR) is a virtual network of computers based on the onion routing principle that protects users against 'traffic analysis' and, as a consequence, offers almost anonymous access to the Internet. The very name 'onion network' refers to the structure of the network which, like an onion, has a layered structure. Figure 1 shows the three-layered encryption of a transported message.

FIGURE 1. THREE-LAYERED ENCRYPTION (GRAPHIC FORM)



Source: https://cyberops.com.au/the-onion-router-aka-tor-darknet-or-deepweb/

The Onion Router was created by a mathematician Paul Syverson and IT specialists Micheal G. Reed and David Goldschlag from the US Marine Corps Laboratory. The Onion Routing Program was initially sponsored by the research laboratories of the Marine Corps Warfighting and was the effect of merging of a number of projects involved in research, design and analysis of anonymous traffic in communication networks, and its primary goal was to protect government communications during intelligence operations. From 2004 it was run by the Electronic Frontier Foundation (EFF), a non-profit digital rights group. Currently, the entity responsible for the development of the TOR software is a non-profit organisation called the TOR Project with the headquarters in the USA. The TOR Project is subsidized from various public and private sources. The sponsors of the project include governments of the United States and Sweden, the Ministry of Foreign Affairs of Germany, Google, Reddit, Mozilla, the Human Rights Watch, universities and research centres.

Anonymity on TOR network is achieved thanks to a multi-layered encryption of information and data transportation through a series of random relays called onion routers. Entrance to the network is possible after downloading the TOR application. The TOR Browser is based on Mozilla's Extended Support Release (ESR) Firefox branch. When the browser is activated, the user downloads a list of entry nodes from the official server. The first proxy server will replace the source address of the IP-Packet with its own address (Szydłowski, 2018). Then Onion Router A 'peels' away one layer of encryption uncovering the data's next destination and transfers it through a randomly chosen network of onion servers called nodes or relays. When the final relay on the path is reached (the exit node), the last layer of encryption is removed and then the data is sent to its final destination. Such architecture of the network guarantees that the sender of the information package remains anonymous since each path is randomly generated and none of the relays keep records of the traffic passing through, it is nearly impossible for the data transfer to be traced back to the sender through TOR's complex network. However, the system has one weakness, the exit node is the one that removes the final layer of data encryption. Although the exit node is not able to access the original location or IP address, it can spy on the sender's activity if he is visiting an unsecured HTTP website.

Onion sites use pseudo-domains (the special use domains) which are placed behind an additional firewall and are hidden from the Networks Address Translation (NAT) i.e. a service which remaps one IP address space into another which is more 'readable'. As TOR network operates all around the globe, the identification of individual users is almost impossible. As the result of data encryption between consecutive relays, the data transfer in TOR network is much slower, which considerably hinders browsing its resources and determines the appearance of sites and forums which are all very simple as any graphic design is limited to the absolute minimum. The websites are content-oriented and the volume of resources is really impressive, ranging from perfectly legal material to completely illegal contents which explains why TOR network came to be known as the dark side of the Internet.

V. TOR NETWORK AND ITS USERS

TOR network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Surface Internet. The access to encrypted contents is only possible when the required server is switched on. TOR network is used by about 2 000 000 people per day and its popularity is rising each year. The biggest number of the darknet users is to be found in Russia, the United States, Turkey, Indonesia, India, China, Brazil, Vietnam and Egypt. The TOR users may be persons who do not intend to commit any crime, they only treat the TOR router as a safe haven *anonymity-wise for conducting their business or social activity*. TOR is a forum on which democratic values, citizen rights and freedom of the press are propagated by e.g. international organisations, non-governmental organisations such as Reporters Without Borders who fight for freedom of information, news agencies who are the source of information for titles such as The Washington Post, The New York Times or The CBC. Used in this way, TOR is a tool facilitating safe communication for example for initiating national and liberation movements fighting to overthrow the present day tyrannies. In 2011 thousands of Egyptian citizens used TOR to communicate despite considerable limitations in the access to the Internet imposed by the regime of Hosin Mubarak (Watson, 2012). Yet another example were Syrian rebels who used TOR network to publish a digital body of evidence related to crimes committed by the regime (SecDev Foundation, *Syrian Regime Tightens Access to Secure Online Communications,* 2015). Anonymity and confidentiality are also very significant for investigative journalists, war correspondents, the Police and other law enforcement agencies as well as cyber security analysts. Also more and more private individuals turn to TOR network as a reaction to media campaigns which show the degree of interference of national entities, security agencies and international corporations in the private sphere of citizens. The governments and law enforcement agencies of many countries fear that TOR network may be an anonymous hub on which terrorists can safely share information on propaganda, conduct recruitment, make financial transactions, and finally, organize attacks.

VI. WHAT'S ON THE DEEP WEB

The thematic diversity of websites on TOR network is impressive. There are commercial services offering mobile phones (CARDEDSTORE), Apple products (Apple Palace), weapons (EuroGun), financial services, hacker related websites (HeLL Forum), sites which expose all kinds of interrelations between companies, national agencies and organisations (RelateList), even sites devoted to art and culture. There are also rich library stocks of controversial or illegal nature.

In order to move freely around TOR resources and get to the darkest corners of the Deep Web, users have at their disposal special darknet search engines such as: the Hidden Wiki, notEvil or TORCH. There are even social networking sites such as Hidden Answers or BlackBook i.e. the darker version of Facebook. TOR is also a forum on which views and opinions are exchanged and secret information exposed (e.g. the WikiLeaks site where anonymous whistleblowers publish often confidential governmental and corporate documents in order to name and shame unlawful behaviour). Finally, on the darknet there are various blogs and guides e.g. ToR Metrics with the biggest collection of facts and curiosities in the darknet, or DEEP.DOT containing detailed information on TOR network and anonymity-related news. What is interesting, the counterpart of this website is also available on the Surface Web.

TOR is a base for many hidden thematic forums and online shopping sites. Each market offers fully functional e-commerce solutions with thematic sectors, shopping baskets, cash management as well as payment and deposit services. The number of such websites is growing on daily basis. The research shows that the most frequent application of TOR hidden services is criminal activity such as drug dealing, illegal finances, sales of guns, explosives or human organs. The darknet websites offer violent pornography featuring children and animals (Moore and Rid, 2016), drastic photographs of accidents and homicide. Other services specialize in intimidation, wiretap, change of identity and murder for hire which is offered for example on the Hitman Network website. Hitman services are offered virtually all around the world from Europe, the United States to Asia. The offer excludes persons below 16 years of age and politicians. Additionally, some 'hitmen' offer the possibility of betting on the murder. The person who determines the time of the victim's death most accurately, scoops the entire pool (Daily Mail Reporter 2013). The cost of the 'service' is determined individually depending on the requirements of the clients. The only currency accepted by hitmen is Bitcoin (Lake, 2013).

TOR network became infamous as the result of the first online black market called the Silk Road which offered drugs, child pornography, explosives, weapons of mass destruction, stolen payment cards and murders for hire. The website was operated by the pseudonymous Dread Pirate Roberts. The website was shut down in 2013, when the FBI arrested its owner Ross Ulbricht. The seizure notice popping up while trying to connect to the Silk Road server is shown in Figure 2.

The goods offered on hidden markets range from soft drugs such as cannabis, to heroin, cocaine, ecstasy, LSD or methamphetamine. One of the TOR tycoon drug vendors claimed that: 'the Deep Web makes shopping for drugs safe and risk-free. Customers do not have to look for dealers in dark corners of their cities. They get door-to-door delivery'. Due to recommendation system, big competition and a certain ruthlessness of the consumer market, the drugs available on the darknet are of much higher quality than those available on more traditional markets. All these factors as well as the guarantee of anonymity for consumers considerably impact the demand. Persons who in the real world do not have the courage or the access to illicit substances, can overcome these barriers in the cyberspace and the delivery arrives safely to their door sometimes even by regular post.

FIGURE 2. IMAGE PLACED ON ORIGINAL SILK ROAD AFTER SEIZURE OF PROPERTY BY THE FBI

Source: (Nl.wikipedia.org, 2019)

The number of the darknet customers is constantly growing, including underaged customers who prefer to buy 'safe' for fear of being detained by law enforcement. On the other hand, the buyers can easily fall prey to fraud. Sometimes instead of the ordered goods they receive a wrapped brick or sugar. These things happen all the time. What is interesting, the 'victims' officially report such incidents to law enforcement. In 2017 AlphaBay and Hansa were seized and closed thanks to the cooperation between Europol, FBI, DEA and the Dutch Police (Golański, 2017). Unfortunately, in place of the shut down websites new ones pop up taking over the suppliers and the customer base of their predecessors.

TOR is also a marketplace for illegal pharmaceuticals and medicines such as various acids, anabolic steroids or Viagra. The medicines are offered by individual suppliers-producers and on specialised TOR markets. Easy and uncontrolled access to medicines gives rise to a number of threats. First of all, the buyers are at risk of consuming fake or unauthorized medicines. Secondly, the goods purchased on the TOR markets may become the object of fencing and trigger legal and health hazard for those engaged.

TOR is also an arena for hacker activity and a market for hacker goods such as spyware, Trojan horses, encrypting tools, zero-day exploits (holes in popular software or systems for which patches are still unavailable), malicious software (malware) e.g. keyloggers (a technology that tracks and records consecutive key strokes on a keyboard). Because sensitive information such as usernames and passwords is often entered on a keyboard, a keylogger can be a very dangerous technology thanks to which it becomes possible to empty the user's bank account or take a loan in his name. The hacking forums feature information (for which the users often have to pay) on how to crack a password or wear a wire. TOR hackers offer services related to stealing information from individuals and companies, snatching full databases or blackmailing individual persons or institutions. The victims of such attacks usually decide to pay the required charge in order to reclaim stolen data and retrieve access to their devices. They are desperate to avoid possible leaks of data which may destroy the image of companies and expose them to massive financial penalties related to GPDR regulation on protection of personal data (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Finally, they want to put an end to further attacks.

Apart from hacker services the darknet offers forged banknotes, payment cards, stolen PayPal accounts and bank accounts. Sometimes the accounts are full of money, sometimes they are empty. Other goods for sale in the darknet include false IDs, university diplomas, driving licences or passports. For an additional fee it is possible to have one's false data put in the official government databases. For instance, full American citizenship i.e. passport and birth certificate costs $ 5 900 (Majdan, 2016).

VII. CURRENCY

The main method of payment in TOR network are cryptocurrencies. Their popularity is determined by the lack of central issuer and absence of efficient surveillance of cash flows. The most popular and the most frequently used cryptocurrency is Bitcoin which, according to the most credible version, was created in 2009 by a person or a group of persons using the name Satoshi Nakamoto. It is an algorithm consisting of a cryptographic chain of blocks with an assigned value (Szymankiewicz, 2014). To authorise transactions private cryptographic keys are used, the keys are stored on a PC in a special software called Bitcoin wallet file or on external wallet servers. Only 21 million bitcoins will ever exist, according to the design of the cryptocurrency's anonymous founder. In the Bitcoin marketplace, digital exchanges are held between buyer and seller which adds an extra layer of security. Therefore TOR network creates an ideal platform for illegal trading transactions, frauds or dirty cryptomoney laundering (Mazurczak, 2015).

It must be stressed that owners and users of Bitcoins are vulnerable to various risks and threats caused by the very TOR network. The risks include theft or hidden usage of the computing power. Due to malpractices committed by e-stores administrators and operators which resulted in a large-scale fraud, it became necessary to secure transactions in TOR network. The first safeguard was the introduction of a third party – an external wallet to which the cryptocurrency is transferred. The next solution securing the financial turnover are Bitcoin 'laundries' which use external servers to break the link between the address from which the Bitcoin is sent and the destination address. The operating principle of a Bitcoin 'laundry' (otherwise known as a 'mixer' or 'tumbler') is similar to the *anonymity enhancing mechanisms in the very* TOR network i.e. the bigger number of transactions in the 'laundry', the higher level of the currency *anonymity*. And further, the 'washed' Bitcoins are transferred to the next wallet (e.g. the Onion Wallet), after which point they can be safely withdrawn from a cash machine. Thanks to such solutions, the necessity to use the Surface Net is completely eliminated and the identification of the user becomes impossible. TOR network

has had a considerable impact on the development of the cryptocurrency community. After Bitcoin, new cryptocurrencies (Ethereum, Litecoin, Bitcoin cash and Ripple) emerged and are now gaining popularity. Those interested in cryptomoney have access to extensive knowledge and consultancy forums devoted entirely to cryptocurrencies (HiddenWallet or MyBitcoin).

VIII. TOR AND PORNOGRAPHY

Anonymity on the web generates the feeling of confidence and unpunishability which is a consequence of the absence of relevant legal norms with respect to online criminal activity. As indicated above, TOR network is full of sites and hidden forums where users exchange links to child pornography, necrophilia, manuals how to torture and sexually abuse children, how to kill a person. Even more horrifying are detailed descriptions of how to rape a child of what age and from which country, and how to desecrate corpses. There are links to films showing violent rapes on women and children. One such film showed a twelve-year-old girl raped at school by four boys (Moore and Rid, 2016). The biggest forum for pedophiles was opened in 2011. It was called the Lolita City and featured softcore and hardcore images of new-born babies, small children and teenagers of both sexes. In 2011, a group of Internet activists called the Anonymous, conducted 'Operation DarkNet' directed against child pornography and the involved child abuse groups active on the darknet. The hack was aimed at shutting down all pedophile sites or replacing them with phishing scams. Although 190 child pornography vendors were deprived of their identity, the victory was only apparent as the news circulated the world and the issue of pornography hit the headlines. The following day, the Anonymous published the contents of the seized websites which not only advertised sites like the Lolita City but also attracted a great number of new users to the darknet (Howell O'Neill, 2014). In 2013 the website had 15 000 members and approximately 1 400 000 photographs.

The issue of child pornography is appalling even for other users of TOR network. In 2017 an anonymous hacker attacked a company called Freedom Hosting II which ran several child abuse websites on the darknet. The material obtained through the hack was handed over to the cybersecurity experts and law enforcement agencies. The hacker's activity although illegal, due to the motives i.e. fight with dissemination of child pornography, was considered ethical by the Internet community.

The *effects of child sexual abuse* can be devastating for the child itself and for its immediate environment. Both prosecutors and victims admit that exposing children to pornographic images of rape or violent sex has the same effect as actually abusing the child (Howell O'Neill, 2014). When the pedophiles settled down in TOR network it only strengthened their feeling of togetherness and allowed them to exchange their international experiences. In this way TOR contributed to the wide-scale spread of pedophilia. The Love Zone which replaced the Lolita City, gathered 50 000 of active users which was probably the biggest number of pedophiles so far gathered in one place. The website required each new member to go through an initiation ritual. The ritual consisted of committing a sex-related crime i.e. uploading a fresh hardcore child porn content. The same procedure is usually applied in the admission process to gangs. To become a gang member the candidate must commit a public crime (Howell O'Neill, 2014). Despite efforts of law enforcement agencies all over the world to make sure that perpetrators do not feel anonymous and safe on the Internet, when particular porn and child abuse sites are shut down new ones immediately emerge. For sure, this is the most menacing face of the darknet which is the real Kingdom of Evil.

IX. TOR IN POLAND

Hidden illegal websites can also be found in the Polish segment of TOR network. The so called Polish Black Market established in 2012 by an individual using the name of Zdzisław Dyrma was the first website of this kind. The registered users could access information on how to evade taxes, how to open a 'mule' account, how to commit fraud or extortion. Other threads on the forum referred to rape, prostitution and pornography. The website was put on sale in 2013 and in the following year returned to the dark web under a new name the Polish Board&Market. However, it was only a limited version for former users to log on the old forum and delete their own posts (Handlujbezpiecznie.pl, 2014). The successor of the first Polish darknet sites was the Victor's forum which featured extended sections on drugs, tax frauds and blackmail. The forum's registered users could create false accounts of real people, most of all women, with detailed personal information such as name, surname, height and weight, CV or even scans of IDs, passports and other documents. The data was supplemented with incriminating photographs of the stalked women stolen from their private computers. The database was created for blackmail purposes. (Lisiecki and Kucharski, 2016). Currently, the only active website on the Polish darknet is called Cebulka. Luckily, while the TOR underworld is expanding everywhere else, in Poland its development seem to have come to a halt.

X. PROBLEMS WITH TERRITORIALITY AND NEED FOR COOPERATION

The Internet is the most popular arena for cross-border crime due to the international character of the Internet and its anonymity. This issue is connected with a considerable impediment in prosecuting and punishing cybercrime i.e. the determination of the place where the crime was committed. This issue is of high significance as it determines which country's jurisdiction must be applied in a given case. The basic rule behind the applicability of criminal law and prosecution of crimes in a specific country, is the so called principle of territoriality whose expression in the Polish legal system is article 5 of the Polish criminal code of 1997 (Journal of Laws no 88, item 553 as amended). The territorial principle is also present in public international law under which a sovereign

state can prosecute criminal offences that are committed within its borders, excluding such jurisdictions which would openly violate democratic principles.

The issue of territorial jurisdiction of countries to prosecute crimes committed online is also in the centre of attention of international institutions. The rules of national jurisdiction are included in the EU legislation such as the European Union Convention on Cybercrime signed in Budapest on 23 November 2013 and Directive 2013/40 of the European Parliament and of the Council on attacks against information systems. Due to loculation of crimes committed in the cyberspace, it is essential to assure appropriate level of cooperation between law enforcement agencies and legal organs of many countries while conducting evidentiary proceedings. As for the legislature, TOR network exposes all its deficiencies in application of international agreements in a concentrated effort to eliminate the danger of cybercrime. Unfortunately, the law enforcement agencies and judicial authorities fall behind with updating existing legal norms and the cyber underworld is always a few steps ahead.

XI. CONCLUSIONS

Illegal activity and all shades of the dark side of life seem to dominate in TOR network. Former vice president of the TOR Project, Adrew Lewman, estimates that between 2015 and 2017 the number of dark sites offering malicious software, personal data and intoxicants increased dramatically. As much as 95% of contents of the darknet are illegal contents related to copyrights theft, drug dealing, human trafficking, child and woman abuse (Howell O'Neill, 2017). TOR network is an example of a tool which was created with good intentions but with time became a powerful tool in the hands of cybercriminals who eagerly exploit new technological solutions and create new, previously unknown illicit acts and find out more and more refined ways of their implementation. To counteract such phenomena and to overcome all difficulties related to cybercrime exposure and prosecution, it is necessary to introduce changes of legislative nature and changes in the functioning of specialized law enforcement units. Although for the moment TOR environment assures anonymity and security and seems to be a perfect haven for the world of crime, cybercriminals should not feel safe.

XII. REFERENCES

Bergman, M. (2001). The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing*.
Golański, A. (2017). Upadek narkotyków bazarów AlpaBay i Hansa: prywatność jest za trudna?. *Dobreprogramy.pl*.
Handlujbezpiecznie.pl. (2014). *Polish Black Market*.
Hołyst, B. (2014). *Bezpieczeństwo jednostki*. Warszawa: PWN.
Howell O'Neill, P. (2014). The darkest net. *The Kernel Issues- kernelmag.dailydot.com*.
Howell O'Neill, P. (2014). The Deep Web's biggest child porn sites are closing ranks. *The Kernel Issues- kernelmag.dailydot.com*.
Howell O'Neill, P. (2017). Tor's ex-director: The criminal use of Tor has become overwhelming. *Cyberscoop.com*.
https://Dailymail.co.uk
https://metrics.torproject.org/userstats-bridge-table.html
https://new.secdev-foundation.org
https://oedb.org/ilibrarian/invisible-web/
https://web.archive.org/web/20130610072640/http://weirderweb.com/2013/06/06/back-in-booming-lolita-city-the-online-child-pornography-community-is- thriving
https://www.torproject.org/about/sponsors.html.en
Lake, E. (2013). Hitman network says it accepts Bitcoins to murder for hire. *Thedailybeast.com*.
Majdan, K. (2016). Tu jest wszystko co nielegalne. Odsłaniamy tajemnice ukrytej sieci. *Forsal.pl*.
Mazurczak, K. (2015). Anonimowe płatności internetowe wykorzystywane w cyberprzestępczości. Istota kryptowaluty Bitcoin. *De Securitate et Defensione. O Bezpieczeństwie i Obronności*.
Moore, D. and Rid, T. (2016). Cryptopolitics and the Darknet. *Survival*.
Szydłowski, T. (2018). Wszystko co trzeba wiedzieć o sieci cebulowej. *Komputerswiat.pl*.
Szymankiewicz, M. (2014). *Bitcoin. Wirtualna waluta Internetu*. Warszawa.
Watson, K. (2012). The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks. *Washington University Global Studies Law Review*.
Weber, R. and Heinrich, U. (2012). *Anonymization,*. Springer.
Wood, J. (2010). The Darknet: A Digital Copyright Revolution. *Richmond Journal of Law and Technology*.