Dilemmas related to the functioning and growth of Darknet and the Onion Router network

Anna Nastuła [A]

Received: March 18, 2020 | Revised: April 21, 2020 | Accepted: April 30, 2020

DOI: 10.33445/sds.2020.10.2.1

Abstract

It is inevitable that the rules for using various sources of information in cyberspace keep changing. We are still searching for the best possible form. A form that would, on the one hand, provide us with reliable material, and on the other hand guarantee utmost security and ensure that our interests or any exchange of correspondence or opinion will not be seized by unauthorised individuals or even used against us. In order to meet such needs and expectations, Darknet has been created, in particular TOR network (The Onion Router). The starting point for this paper was the history and principles of TOR, as well as the issue of anonymity and payments with cryptocurrencies. In the further part of the article there is a discussion on the positive and negative opportunities that TOR offers. The paper ends with an indication of possible directions for further work and elaboration.

Key words: TOR network, Darknet, cyberspace, cybersecurity, privacy, Bitcoin.

Introduction

Contemporary world is characterised by uncertainty and turbulent variability in science, technology, production as well as the speed of transmission and the significance of information in social life. It is in front of our very eyes that the Fourth Industrial Revolution takes place as we speak. Its traces date back to right after World War II, when such interdisciplinary branches of science appeared as: cybernetics, regulation theory, information theory, game theory, systems theory, decision theory, optimization theory, exploitation theory, theory of fluent functioning (praxeology) [1].

A significant feature of this revolution is the specific direction of technological, educational and cultural changes in social life. There has been a significant shift in the nature of the material processed in contemporary systems: from energomaterial processes in these mechanisms towards information-processing machines such as e.g. computers. At the same time, the dynamic growth of information technology results in a specific dualism observed in the attitudes of the users of such solutions. On the one hand the society expects greater security, which entail a more or less conscious acceptance of interference with the privacy on the part of private service providers. What is symptomatic is also the reluctance towards modern e-services, resulting from the fear of compromising the security of entrusted information. On the other hand, network users do not wish for cybersecurity mechanisms to be expanded if they are to be used by public authorities through mass electronic surveillance. This problem is known in the literature on the subject as the "cybersecurity paradox" [2]. As a result, interest in programmes that can ensure anonymity in the network is on the increase. One of such mechanisms is the TOR network.

The Onion Router is a virtual computer network which implements second-generation onion routing. The network prevents the analysis of network traffic and, consequently, makes it possible for the users to publish and

[A] Military University of Technology, MUT, doctoral on the Faculty of Security Studies, Warsaw, Poland, Master degree (in law), e-mail: k.anna.nastula@gmail.com, ORCID: 0000-0002-2061-5067

browse information on the Internet with almost 100% anonymity. It allows the users to override censorship and network filters, and to gain access to hidden Darknet resources. It is therefore a tool that, depending on the user's intentions, may be used for noble purposes or for illegal actions and often brutal crimes. Regardless of the space for possible illegal actions, the possibility to identify the perpetrator is one of the features underlying the effectiveness of security measures. In the TOR this possibility is reduced, if existent.

Considering the fact that the cybersecurity dilemma is not a well-studied topic and we have no sufficient information on this subject, it seems legitimate to commence exploratory research in this respect. The main research problem can therefore be summarised in the following question: to what extent does the functioning and growth of Darknet condition the actual positive and negative impact on the security of the social system? The major assumption underlying the study is that it is only an attempt to outline the research area. The main goal of this paper is to define the cybersecurity dilemma, as well as a preliminary determination of positive and negative aspects of using and developing the Darknet and TOR network. Proper studies are envisaged as the next step of the broader, teamwork-based research project.

Results and discussion

History and community

"The Onion Routing Program" was a project originally developed in the mid-1990s by two employees at the United States Naval Research Laboratory: mathematician Paul Syverson, and computer scientists Michael G. Reed and David Goldschlag. The program was developed for the purpose of protecting government communications. In 2004-2005 the project was continued by non-profit organization the "Electronic Frontier Foundation". This organisation has a remit of defending civil liberties in the digital world and dealing with activisim for human rights. Since 2006, the development of software and popularization of the project is supervised by a non-profit research-education organization called "The TOR Project". The organisation has its headquarters in the USA. It raises funds not only from international private donors, but also from public sources (including governments namely the United States, Sweden and Germany), international organizations (including The Human Rights Watch), Universities, research centers and corporations (including Google, and Mozilla).

The attitude of particular governments to the TOR network can be extreme in some cases. Some countries, including the United States, support the development of the TOR network. In fact, information from 2014 indicates that the US government officially took steps to help strengthen the network by highlighting its potential bugs and loopholes. Internal documents in the USA National Security Agency (NSA) refer to Tor as "the king of high-secure, low latency internet anonymity" [3]. In contrast, other governments such as those of Saudi Arabia, the United Arab Emirates and Iraq openly condemn the operation of the TOR network and block its sites and access to entry nodes.

Curiously enough, in 2014, the Russian interior ministry offered $ 110,000 in a contest seeking a way to crack the identities of users of the Tor network [4]. The competition was intended only for Russian citizens. Such significant interest in the TOR network by the authorities was due to two facts. Firstly, Russia's lower house of parliament passed a law requiring internet companies to store Russian citizens' personal data inside the country, (a protectionist security measure). Secondly anti-government actors began to use the TOR network for their internal communication. Countries where the Internet has been heavily censored, such as Venezuela or China, have banned Tor and similar technologies, including virtual private networks (VPNs).

World Wide Web and anonymity

In most democratic societies, privacy is considered as an essential part of the individuals rights, which impacts all other forms of political

expression and is legally protected both by national law and international activism. At present from a legal standpoint, it is not the case with anonymity, and it is anonymity that has become a desirable objective in recent years.

Anonymity has become more important for a number of reasons. The scandal associated with the activities of Cambridge Analytica for example and also the associated technological capabilities of international corporations such as Facebook or Google is now unprecedented in terms of the scope of information collection. Internet users want to decide for themselves where, when and what information they will share and for what purpose. Therefore, the number of technological projects that increase data security is constantly growing, ranging from the simplest ones available for every "average" Internet user to tools that require specialized IT knowledge. Among the most popular are: proxy servers, tunneling and Virtual Private Network (VPN), bypassing Domain Name System (DNS) blocking and onion routing [5]. It is also possible to combine different methods to increase the level of difficulty in identifying the user. The TOR network, which implements the third generation of onion routing, is the most popular tool among other solutions for anonymity on the Internet.

Oscar Wilde wrote: "*Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth*" [6] In the Darknet, the "truth" that is spoken may unfortunately be created for the needs of the moment to achieve a desired outcome. Anonymity contributes to freedoms of expression; it allows for freely voiced opinions, and helps in achieving objective assessments, and improved legal and even social advice. On the other hand, however, the anonymity of the TOR network can make some crimes easier to facilitate and might incentivise expansion of these nefarious activities, and expansion that would not take place without the network. Moreover, unrestricted anonymity, could lead to intimidation and harassment, and could undermine freedom of expression, if the harassment prevents others from participating in the public debates and expressing their views. However, if their views are anonymous, a way round it exists.

When performing daily activities such as electronic payments, phone calls, browsing the web, using social media, each user leaves an electronic trace that can facilitate their identification in the real world. The above activities are carried out in the easiest accessible layer of the Internet called Surface Web. This part of the World Wide Web, otherwise known as the Visible Web or Indexable Web, is available from popular search engines. However, much larger resources are found in the Deep Web, otherwise known as the Hidden Web or the Invisible Web, and in contrast to the superficial Web, they are that part of the Internet that is not indexed by standard search engines. The Deep Web is the most dynamic growing category of the World Wide Web, containing specialized and verified information [7]. These contents are of high quality and professionalism, as they are often created on the initiative of experts and specialists in specific requirements [8]. Its resources include among others websites of the National Agency for Aeronautics and Space (NASA), specialised databases and contents of world libraries. And it is within the deep web that the Dark Web, otherwise known as Darknet, often referred to as the dark side of the Internet, can be distinguished. It is a place that is both frightening and fascinating. There are many networks in Darknet where content is accessed through connections created by special software such as I2P (Invisible Internet Protocol), GNUnet, Freenet and TOR network.

Principles of operation of the TOR network

The essence of the TOR network operation is based on the principle of multiple data encryption and its transmission through several network nodes, called routers or onion nodes. The entrance to the network starts with downloading and installing the TOR browser, which visually resembles the modified version of Mozilla Firefox and is also available in Polish for Windows, Mac and Linux. Encrypted information packets pass through consecutive onion routers that remove one layer of cipher to reach the address of the next traffic node and pass on. The software that creates the Internet connection can use the TOR network via the SOCKS interface.

The last node, referred to as the output node, is the "weakest link" of the TOR network, as the

information transmitted between the output node and the destination server is not encrypted. The TOR network is developed by the users themselves, who create the node servers. The publishers of the TOR network stress that this tool does not solve all the problems related to anonymity in the Internet and indicate additional technological protection which should be used in parallel with the TOR browser [9].

Since 2018 it is much easier to use TOR network also on smartphones. A response to the market demand was the test service in the form of Onion3G SIM cards issued by the English company Brass Horn Communications, which automatically manages all mobile data through the TOR network and does not require additional configuration. The card is prepaid, so it can be topped up at any time using credit card or cryptocurrency such as Bitcoin, ZCash and Monero [10].

Due to their design and multiple encryption, TOR pages are ascetically pleasing but the browser itself works much slower. The URL of sites in the TOR network, often called "Onionland" by its users, consists of a sequence of sixteen random letters and numbers, ending with the onion domain. The onion domain is located behind an additional firewall and is hidden from Networks Address Translation (NAT), a service that changes the address of a site to a more readable one. Such a solution causes that only users who know the addresses of specific pages have access to the content. Hidden page search engines such as The Hidden Wiki, notEvil, TORCH or DuckDuckGO also provide help.

Financial settlements and mafia activities.

The main method of payment in TOR network are cryptocurrencies and among them the most commonly used-Bitcoin. Cryptocurrencies have gained immense popularity due to their decentralized, secure and anonymous character which is supported by *peer-to-peer* architecture and enables the transfer of funds and other digital assets between two different persons without a central issuer. Bitcoin payments have become popular in the TOR network since the Silk Road forum founded by Ross Ulbricht in 2011.The service offered drugs, child pornography, explosives, weapons of mass destruction, stolen payment cards and homicides. The platform was called the "drug Amazon". It is estimated that the turnover on Silk Road was over 9 million Bitcoins, which would be about 1 billion dollars [11]. In 2013, a routine error of forum administrators led to its seizure and closure by the FBI, which did not, however, stop this type of activity in the TOR network. In its place other international black markets were created. It is believed that Bitcoin was created by the founder of Silk Road Ross Ulbricht. According to the report on cryptographic crimes, published in January 2019 by "Chainalysis", a company dealing with blockchain analysis [12]. In 2018 the total volume of trade on the black market was at the level of USD 600 million, and at the end of the year it was over USD 2 million per day.

Since March 2019 TOR expanded its option and accepted donations in the form of cryptocurrencies in a direct way. The new payment methods for donations range from Bitcoin, Bitcoin Cash, Dash, Ethereum, Litecoin, Monero though Stellar Lumens, Zcash and the Augur project's REP tokens. Although it is not completely novel, as previously these donations were accepted through BitPay, a company that converts crypto payments to fiat before passing it on to its merchant clients, opens the possibility to make direct payments to "TOR Project" which contributes to protecting the privacy of its users. TOR fundraising director Sarah Stevenson made public the reason for this decision: "We decided to accept cryptocurrency because more and more donors requested that option. The Tor Project and the cryptocurrency communities both value privacy, so it makes sense" [13]. The lack of effective control over the organization's financing and the fact that donors become nameless creates another "layer of onions", which strengthens the anonymity of the entire TOR network.

The TOR network community has also found a solution for verifying the quality and reliability of services offered in full anonymity. It is a system of recommendations for both the seller, the goods and the buyer as each party to the transaction is exposed to provocative actions and must be kept cautious. The credibility of new members using services in the TOR network is also verified on the basis of the evaluations. The vendors, as in the generally accessible Internet, receive trust points

for their completed transactions. And just like in generally available stores, they compete for customers, among others through free samples of offered goods or promotional campaigns such as recommend a new customer, you will receive 5% of the amount of his purchases in the form of cryptocurrency. It should be emphasized that due to complete anonymity, the assessments made are absolute, short and factual, without marketing and courtesy elements. For supporters of the TOR network, this is a very important element that determines the attractiveness of the black market, which conditions the possibility of obtaining the best prices while maintaining the highest quality of goods, including in drug trafficking. At the same time, for the mere fact of placing a buy-sale offer or the possibility of starting the auction as a buyer, a small fee is required to authenticate the person and the service proposed. It is worth noting that the system of recommendations in TOR network resembles the mafia system. In both systems, the transition to the circle of "higher trust" requires a violation of the law in the current activity. Probably in the TOR network, it is sometimes a minor, incidental violation of the regulations in force in a given country, but as the proverb says "*From a thong to a clover*".

Discussion on the present and future of the TOR network

In its assumption, the TOR network is primarily to be a place for the free exchange of ideas and views, as well as a space free of manipulation and ensuring safe and anonymous access to the truth. These slogans are part of the activities of international human rights organizations, including Human Rights Watch, Global Voices and Reporters without Borders. These organizations recommend using the TOR network. Private citizens also decide to use the TOR network to take action on both the business and social forum, for fear of their privacy, identity theft, misinformation and restriction of privacy on the part of both state entities and international corporations. Officers of the police and other law enforcement agencies, the military or special services, as originally intended by the creators of the TOR network, use it to secure and transmit information acquired through operational activities. IT security analysts and managers also use the TOR network to guarantee the confidentiality of network correspondence or to test the effectiveness of implemented Firewall systems.

The price for free services on the Internet is control by corporations that, for obvious financial reasons, and often for political goals, profile and select information for specific users. Unlimited choice and free access to the entire spectrum of knowledge is already an illusion. Popular Google search engines have now become "technological gatekeepers" [14]. As Alexander Halavis states: "Search engines not only contribute to the selection of more significant sites, but are also influenced by them" [15].That is why the TOR network is an important tool for journalists, war correspondents or even employees of security services for whom, for both ideological and security reasons, it is important to reach reliable, cross-sectional and reliable information.

In many totalitarian countries, where governments restrict citizens' access to unrestricted communication, the Tor network enables these blockades to be circumvented and to come into contact with the democratic world, free and independent media and uncensored literature. In Egypt, during the Arab Spring, thousands of citizens used the Tor browser to exchange information, despite severe Internet restrictions imposed by Hosini Mubarak's regime. Likewise, the rebels, in conflict-affected Syria, who sought to reveal digital evidence of the crimes committed by the regime via the Internet, used the TOR network as a tool for free communication [16]. In 2010, the Free Software Foundation awarded the TOR network in the category of public benefit design for the contribution it makes to whistleblower activity, human rights campaigns, and the activities of dissident movements. The Foundation motivated "The Award for Projects of Social Benefit" as follows "Tor has enabled roughly 36 million people around the world to experience freedom of access and expression on the Internet while keeping them in control of their privacy and anonymity. Its network has proved pivotal in dissident movements in both Iran and more recently Egypt" [17].

Revolutionaries also use the TOR network for self-organisation, without fear of intervention by the authorities they stand in opposition to. It is

also a tool for activists, whistleblowers and people fighting for freedom and civil rights. An example of this was the action organised by the Mauritanian Nasser Weddady, who, through the TOR network, began the fight against slavery practised in Mauritania.

Anonymity is the driving force of the TOR network, but in the case of the issues described above, it takes a human face. Although idealistic slogans of freedom and privacy protection for TOR network adversaries are not commensurate with the potential losses that may result from its use by the criminal world and people who have evil intentions, solutions should be found that will only negate such activities on the margin of using the TOR network. There is an undeniable need to create a tool to ensure free communication in the world of accelerating digitization, globalization and increasing surveillance. And this is where the TOR network appears.

The dark side of power

Jamie Bartlett describes Darknet as a strange mix of crime and idealism, where dissidents' sites are adjacent to drug and terrorist sites, and should be treated as a global phenomenon [18]. The Black Internet is a "cybernetic underground" where there is freedom and anonymity that allows users to share often uncensored content and illegal goods or services. Anonymity threatens security and increases the propensity for inappropriate behavior, especially when the user is convinced of the absence of legal sanctions [19].

In the TOR network you can find websites specialising in trafficking in illegal goods such as arms, drugs, stolen goods and illegal services, child pornography forums, torrent services, oppositionist and political heist websites. The most popular service that introduced hidden platforms of the TOR network to international economic markets was the aforementioned Silk Road. The best-known drug market operated on a similar basis to eBay or Amazon, allowing anonymous contact between sellers and those interested in buying banned substances of all kinds: cocaine, cannabis, heroin, psychotropic substances, LSD. Several factors contributed to the unprecedented success of the service. First of all, very high quality of drugs that were sold at affordable prices and a friendly, simple system for using the website. However, the decisive factor could also be the attitude of the creator and administrator of the site Ross Ulbricht, whose technological, organizational and ideological solutions became an example for the subsequent websites emerging in the TOR network.

Ulbricht moderated the Silk Road in great detail and immediately reacted to any attempts to deceive customers and transactions that could harm them. As he described the service himself: "It's a great idea and an excellent, practical system. Not a utopia. It's governed by the laws of the market, not some central authority". After the website was closed, new ones were created in its place, including the most popular Alpha Bay and Hansa, whose operations were also terminated by law enforcement in 2017. However, the growing market needs mean that instead of closed websites, new ones are created, which take over both technologies, as well as suppliers and customers of previous points rendering illegal services. Trading activity in the TOR network after 2017 moved to the Russian-language website "Hydra" and the equally popular "Dream Market" and "Wall Street Market".

In the Tor network, services dedicated to hacking services such as HeLLForum, Hacker Place or Rent-A-Hacker are very active. Much of the communication of hacking communities is closed to the public, and access to individual forums is conditioned by invitation. The websites offer exploits, Trojan horses, ransomware generators or Cybercrime as a Service. There are also numerous paid offers to carry out DDoS attacks. Underground markets also offer services of theft of personal data, in particular any documents that are carriers of personal data, which can be used as a second form of authentication, such as passports, social security numbers and even utility bills. There is a growing interest and demand for training tutorials containing instructions for hackers and criminals as well as guides for the organisation of spam and phishing campaigns. The TOR network is also a place where you can indulge in online gambling, which is illegal in some countries, including Poland.

Pornographic websites, especially those containing violent child pornography, are considered by both opponents and supporters of

the TOR network as its darkest and morally unacceptable place. Unfortunately, it is this darkness that creates psychological security and fosters the creation of a community of the worst kind of deviation. There are discussions on the age at which it is best to rape a child, from which country and how to get it, descriptions of how to desecrate the bodies of the dead, links to films containing bestial rapes on women, children and animals. One of the most brutal and popular websites was "Hurt2theCore", which was divided into numerous forums and categories including: "Cruelty", "Sexturistics and prostitution", "Hurtcore – how to make him scream". Forums with pictures and video materials were divided into subgroups: men, women, newborns, infants, small children, teenagers and adults. Whereas in pornographic and paedophile websites or those providing instructions and indications for sexual deviation, the content is made available free of charge or the original materials obtained in the course of the committed criminal act are billed. This exacerbates the difficulties in detecting individual users of these portals by law enforcement authorities. An officer who would like to penetrate such a service would have to commit a criminal act alone.

New technologies generate new threats, the consequences of which often reach the world of politics. This can be through the criminal world and may affect the stability of the balance of political forces in the world and could destabilise the balance of political power globally. At the beginning of 2018, the wave of deepfakes increased, which can be considered a new serious threat to many areas of security. Deepfakes are differently manipulated audiovisual materials that were created as a result of a combination of so-called deep learning – i.e. deep, thorough learning (including facial expressions or intonation of the voice) and pipes or false internet information. The technology based on artificial intelligence created by an anonymous user with the pseudonym "deepfakes" allows replace your face from a video to any other, i.e. to create or modify the content of audiovisual works.

Initially deep fakes were used mainly in the pornographic industry, but quickly became attractive for all kinds of political activities. The obvious threats to the authenticity of the transmitted content, ethical aspects and fear of abuse on an unprecedented scale of the image of a person have resulted in deepfakes being banned by websites and portals where they were published so far. Following the bans deepfakes have moved to the TOR network and their creators are working on refining the imposed images through increasingly better technological solutions [20]. Threats arising from this crime occur both in criminal, civil and commercial law. The victims, by changing their faces, become the main protagonists of pornographic films, and can be the subject of fraudulent extortion of money and confidential information. Deepfakes are also a potential weapon that can be used to undermine the credibility of a person who is a moral authority. In the case of disclosure of offensive content, personal rights and the image of the company are violated, which may determine its further economic development. In addition, deepfakes seem to be an ideal tool for creating false evidence for use in court proceedings. After all, they pose a serious threat to national security, democracy and privacy.

Conclusions

The Internet is a virtual reflection of the society, including its positive and negative sides. Considerable anonymity provided by the TOR often triggers what is worst in people and leads to the most gruesome crimes. Such actions refer both to the security of private and public stakeholders in social and political dimension, as well as in virtual settings. It should be remembered that criminal activity is like communicating vessels. Increased criminal activity in one segment automatically generates a chain of criminal links, which will continue to grow proportionately to the size of the original crime. Darknet may be a chance and a hope for some people, while the author of this paper believes it is also a threat. This is why we need to be aware of potential crimes, so that it remains only a new source of information, and the TOR should be an innovative tool, which is reasonably used in everyday life and work, to support national security.

References

1. Mazur M. *Historia naturalna polskiego naukowca*, PIW, Warsaw 1970, pp. 5-13.
2. Cezary Banasiński (scientific supervision), Marcin Rojszczak (scientific supervision), *Cyberbezpieczeństwo*, Wolters Kluwer, Warsaw 2020, pp.338-339.
3. Cook J., *Tor Director Claims Some Government Agents Are Secretly Helping Him, Undermining Intelligence Operations*, [w:] Buinsessinsider.com, 2014.
4. *Russia offers $110,000 to crack Tor anonymous network,* BBC.com, 2014.
5. Callanan C., Dries -Ziekenheiner H.,Escudero-Pascual A., Guerra R., *Lepaing Over the Firwall: A Review of Censorship Circumvention Tools'*, freedom House, 2011.
6. Wilde.O, *The Critics as Artiists*, 1981.
7. M. Bergman, *The Deep Web: Surfacing Hidden Value*, *Journal of Electronic Publishing*. 2001.
8. Devine J., Egger-Sider F. *Beyond Google: The Invisible Web in the Academic Library*, *The Journal of Academic Librarianship*. 2004, vol. 30.
9. https://2019.www.torproject.org/about/overview.html.en#stayinganonymous
10. http://brasshorncommunications.uk/projects/Onion3G/
11. *Silk Road, największy sklep z narkotykami w Internecie zamknięty. FBI namierzyło i aresztowało jego twórcę*, Niebezpiecznik. pl, 2013.
12. https://blog.chainalysis.com/2019-cryptocrime-reviewhttps://uploads
13. https://www.coindesk.com/tor-project-takes-cryptos-after-donors-request-new-options
14. Lewin K. *Froniter in Group Dynamics*, Human Relations 1947, vol. 1, no.2.
15. Halavis A. *Wyszukiwarki internetowe a społeczeństwo*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 81.
16. SecDev Foundation, Syrian Regime Tightens Access to Secure Online Communications, new.secdev-foundation.org, 2015.
17. https://www.fsf.org/news/2010-free-software-awards-announced
18. Bartlett, J. *The Dark Net: Inside the Digital Underworld,* 2014.
19. Leukfeldt E. R., Stol W. *Cyber Safety: An Intruduction*, Eleven International Publishing Hague 2012.
20. Roose K., *Here Come The Fake Videos, Too*, Nytimes.com, 2018.