BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF FOREIGN LANGUAGES
ÚSTAV JAZYKŮ

SHEDDING LIGHT ON THE DARK WEB
KONCEPCE A PROBLEMATIKA DARK WEBU

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR — **Jakub Horváth**
AUTOR PRÁCE

SUPERVISOR — **Mgr. Ing. Eva Ellederová**
VEDOUCÍ PRÁCE

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Angličtina v elektrotechnice a informatice** obor Angličtina v elektrotechnice a informatice Ústav jazyků

Student: Jakub Horváth ***ID:*** 203153

Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Koncepce a problematika Dark Webu

POKYNY PRO VYPRACOVÁNÍ:

Vymezte koncepci Dark Webu, jeho vznik, účely a způsoby k jeho přístupu. Diskutujte legální a etické aspekty používání Dark Webu.

DOPORUČENÁ LITERATURA:

1) Cody, J. (2017). Tor. Exactly how to remain invisible on the anonymous Deep Web. Kowloon: HHB. Solutions

2) Gehl, R. W. (2018). Weaving the Dark Web. Legitimacy on Freenet, Tor, and I2P. Cambridge: The MIT Press.

3) Norton, J. (2016). Tor and the Dark Net. Learn to avoid NSA spying and become anonymous online. Scotts Valley: CreateSpace Independent Publishing Platform.

Termín zadání: 6. 2. 2020 ***Termín odevzdání:*** 12.6. 2020

Vedoucí práce: Mgr. Ing. Eva Ellederová

doc. PhDr. Milena Krhutová, Ph.D.

předseda oborové rady

Abstract

This bachelor's thesis deals with the Dark Web and its use. Even though the Dark Web has been part of the Internet almost since its very beginning, it attracted the public attention only a few years ago. The main purpose of this work is to raise awareness about the topic to help the Internet users to protect themselves in the cyberspace. The thesis is a theoretical study based on the literature review of the available sources related to the topic of the Dark Web. It focuses on the levels into which the web is divided and its origins. It also explains how to access the Dark Web using the Tor browser, outlines the concept of cryptocurrency bitcoin and the marketplace Silkroad. Finally, it discusses content that can be found on the Dark Web, frames the concept of cybercrime and tries to predict the Dark Web's future.

Key words

Dark Web, anonymous, Tor, users, Silkroad, Bitcoin, illegal activities, drugs, trade

Abstrakt

Tato bakalářská práce pojednává o Temném webu a jeho využití. Přestože je Temný web součástí Internetu takřka od samotného vzniku Internetu, veřejnost mu začala věnovat svou pozornost teprve před pár lety. Hlavním cílem této práce je zvýšit povědomí uživatelů internetu o dané problematice Temného webu a tím jim pomoci chránit sebe a své osobní informace. Práce se zabývá vrstvami, do kterých je web rozdělen a jeho původem. Dále také vysvětluje, jak k Dark Webu získat přístup za použití prohlížeče Tor, popisuje kryptoměnu Bitcoin a tržiště Silkroad. Na závěr práce uvádí obsah, který lze na Dark Webu nalézt, definuje pojem počítačová kriminalita a předpovídá budoucnost Dark Webu.

Klíčová slova

Temný web, anonymní, Tor, uživatelé, Silkroad, Bitcoin, ilegální aktivity, drogy, obchod

Rozšířený abstrakt

Navzdory tomu, že Temný web je součástí internetu téměř od samotného začátku, do podvědomí běžných uživatelů internetu se dostal teprve před pár lety. Informace, které běžný internetový uživatel o Temném webu i samotném internetu má, jsou ovšem často mylné, zkreslené či nedostačující k tomu, aby se uživatelé dokázali bezpečně navigovat jak internetem, tak i Temným webem a zabránili tak možnosti stát se obětí útoku hackerů nebo přijít o cenné osobní informace. Dostáváme se do dob, kdy i samotná představa o osobním soukromí individuálních uživatelů zní jako utopie. Temný web je dodnes vnímán jako místo, kde lze narazit pouze na nelegální obsah, drogy, dětskou pornografii či nájemné vrahy. Technologie se ovšem mění a svět zároveň s ní. Ačkoli Temný web poskytuje spoustu výhod, které lze využít pro nelegální činnosti, může být zároveň odpovědí na otázku jak zůstat na webu anonymní, předejít útoku hackerů a ztrátě osobních informací a jak utéci cenzuře. Práce se zaměřuje na koncepci a problematiku Temného webu, jeho obsah a správné využití a jejím hlavním cílem je poskytnout dostatek informací pro bezpečnější navigování uživatelů jak Temným webem, tak i internetem samotným.

Práce je založena na literární rešerši dostupných výzkumů, literatury, blogů a fór na téma Temný web. Při hledání objektivních, nestranných informací, které uživatele zavedou do samotného jádra problematiky Temného webu, lze zjistit, že těchto informací není mnoho. Většina zdrojů, které se na toto téma odkazují, se zaměřují pouze na základní rozdělení úrovní Webu, často používají pojmy “Deep Web” a “Dark Web” chybně a poskytují pouze jednostranný pohled, který nasvědčuje tomu, že Temný web je pouze místo určené pro kriminalitu a běžný internetový uživatel by se mu měl vyvarovat. Vedle výzkumů a literatury se práce také odkazuje na sociální síť Quora založenou na principu otázek a odpovědí, kde většina odpovědí pochází od uživatelů, kteří mají nějaké osobní zkušenosti s Temným webem.

Výsledkem této literární rešerše je vytvoření jednoho dokumentu, který obsahuje dostatek informací, jejichž znalost pomůže uživatelům pochopit problematiku a koncepci Temného webu, usnadní navigaci a použití alternativního webového prohlížeče Temného webu Tor a tím zlepší schopnost uživatelů zůstat na webu anonymní a chránit tak své soukromí a

osobní údaje. Práce se zpočátku zabývá samotnými úrovněmi webu, jaký je mezi nimi rozdíl a co lze v každé z úrovní nalézt. Následně uvádí historii Temného webu a motivace, které vedly k jeho samotnému vzniku. Jako další téma, které práce uvádí, je způsob, jakým lze získat přístup k Temnému webu za pomoci speciálního softwaru Tor, výhody a nevýhody použití Toru, návod, jak za jeho pomoci zůstat anonymní a jeho potenciální uživatele. Dále se práce zabývá další nedílnou součástí Temného webu a to kryptoměnami, které umožňují anonymní transakce. Vysvětluje, co je to kryptoměna Bitcoin a jak funguje. Práce se také zmiňuje o online černém trhu Silkroad. Silkroad byl jeden z prvních a nejúspěšnějších tržišť Temného webu, který změnil pohled na Temný web a jeho využití dodnes. Práce také pojednává o nelegálním i legálním obsahu, na který lze na Temném webu narazit. Závěrem práce je problematika počítačové kriminality a předpověď budoucnosti Temného webu.

Temný web je často vnímán jako místo, které je pouze plné nelegálního obsahu jako drog, nelegální pornografie, pirátství, nájemných vrahů či hackerů a jiných podvodníků. Anonymita temného webu, která umožňuje tyto nelegální činnosti, zároveň také poskytuje možnosti jiného využití, jako například platformu pro nezávislé a vyšetřovací žurnalisty, podporuje svobodu projevu a politické diskuze bez vládní cenzury. Mnozí tvrdí, že i některé nelegální činnosti, jako nákup a prodej nelegálních látek, je spíše politické hnutí za svobodu a volný trh než o zboží jako takovém. Temný web dále poskytuje svobodu projevu pro ty, kteří se stali obětí jakéhokoliv druhu zneužívání a diskriminace a dává jim možnost anonymně sdílet svůj příběh a tím pomoci ostatním. Soukromí je jedním ze základních práv člověka. Jeho zachování je ovšem v dnešní době poměrně problematické.Závěrem práce je problematika počítačové kriminality a předpověď budoucnosti Temného webu.

Temný web je často vnímán jako místo, kde lze nalézt pouze nelegální obsah, jako obchod s drogami a zbraněmi, nelegální pornografii, nájemné vrahy, hackery a podobně. Temný web také všem zároveň poskytuje platformu pro nezávislé a investigativní žurnalisty, bojovníky za svobodu projevu a umožňuje diskuze bez cenzury z politických či komerčních důvodů.

Soukromí je jedním ze základních práv člověka, jeho udržení je ovšem v dnešní době spíše problematické. Podle předpovědí by se Temný web mohl stát více mainstream a tím umožnit uživatelům lépe chránit sebe a své soukromí na internetu. Otázka, kam Temný web směřuje do budoucna a jak se bude vyvíjet, zůstává ovšem stále nezodpovězena.

Horváth, J. (2019). *Shedding the light on the Dark Web.* Brno: Vysoké učení technické, Fakulta elektrotechniky a komunikačních technologií. 57 s.

Vedoucí bakalářské práce: Mgr. Ing. Eva Ellederová.

Prohlášení

Prohlašuji, že bakalářskou práci práci na téma *Koncepce a problematika Dark Webu* jsem vypracoval samostatně pod vedením vedoucí bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

Jakub Horváth

Table of Contents

Introduction

The Dark Web has been around since the beginning of the Internet itself. Nonetheless, it has been a topic of public concern for the last few years. Privacy is the basic human right. The goal of this thesis is to raise the awareness of the Dark Web to improve public understanding, which could possibly help them to surf the web anonymously, and therefore, prevent them from being hacked or robbed of their personal data.

This bachelor's thesis is divided into eight chapters. The first chapter deals with the differences between the Surface Web, the Deep Web and the Dark Web and gives examples of information accessible when navigating through these different levels. This knowledge is essential to understand how the web is structured. The second chapter outlines the brief history of the Dark Web, its origins and the original motivation for its creation. The third chapter addresses the problem of accessing the Dark Web. Since the Dark Web cannot be accessed through the commonly used web crawling browsers such as Google Chrome and Mozilla Firefox, it needs special software. The chapter frames the concept of the Tor browser which is free and open-source software for accessing the Dark Web. It describes the main function of Tor, how to use it in order to stay anonymous, its advantages and disadvantages, and characterises Tor users and their motives for using it.

The fourth chapter of the thesis focuses on cryptocurrencies, namely Bitcoin. Bitcoin is an essential part of the Dark Web since it allows for the transactions to happen anonymously. It explains what Bitcoin is, how it works and how it is used on the Dark Web. The fifth chapter examines the Silkroad, one of the first online marketplaces ever to exist. The Silkroad was very successful for numerous reasons, which has changed the way that modern technology is used today.

The sixth chapter deals with what types of different content is to be found while navigating through the Dark Web. The chapter is divided into two parts. The first part of the chapter describes the content with the illicit nature and discusses how various types of users use the Dark Web for the purposes such as drug dealing, arms trade, distribution of illegal pornography, hacking and doxxing of personal information and how terrorists use this

platform for propaganda, recruitment and organization of their attacks. The second part of the chapter then focuses on the legal ways in which the Dark Web is used, including investigative journalists, supporters of freedom of speech, activists, political discussions without the intervention of the government and whistleblowers.

What is cybercrime and how does one become a cybercriminal is a topic of the seventh chapter. The chapter provides different perspectives on the question what the cybercrime actually is, talks about the naivety of the Internet users and how cyber criminals exploit this naivety, weak points and little knowledge of the internet security of their victims.

The Dark Web evolves very rapidly and we are slowly entering the era in which it is almost impossible to protect the privacy of individual Internet users. The last, eighth chapter then tries to predict the possible future of the Dark Web based on the available data and existing predictions. The chapter discusses how the Dark Web may evolve and grow in the future and talks about the possibility of the Dark Web and Tor becoming more mainstream for the Internet users to stay anonymous and protect their private information.

1 Levels of the Web

Terms Deep Web and Dark Web are commonly confused with one another. Norton (2016) states that there is a substantial difference that separates the Deep Web from the Dark Web. He then further explains that "the reason why Deep and Dark are sometimes confused, is that the majority of users only use the 'surface web' – the most popular and heavily linked websites on the Internet" (p. 5).

Figure 1 illustrates the web levels that this chapter discusses. The web as it is known is layered into three levels; Surface Web, Deep Web and Dark Web, each of which has their own different purposes, users, reasons to be used and ways to be accessed. Even though the last two levels have been in a public eye only for the last decade, it seems that they have been around since the beginning of the Internet itself.

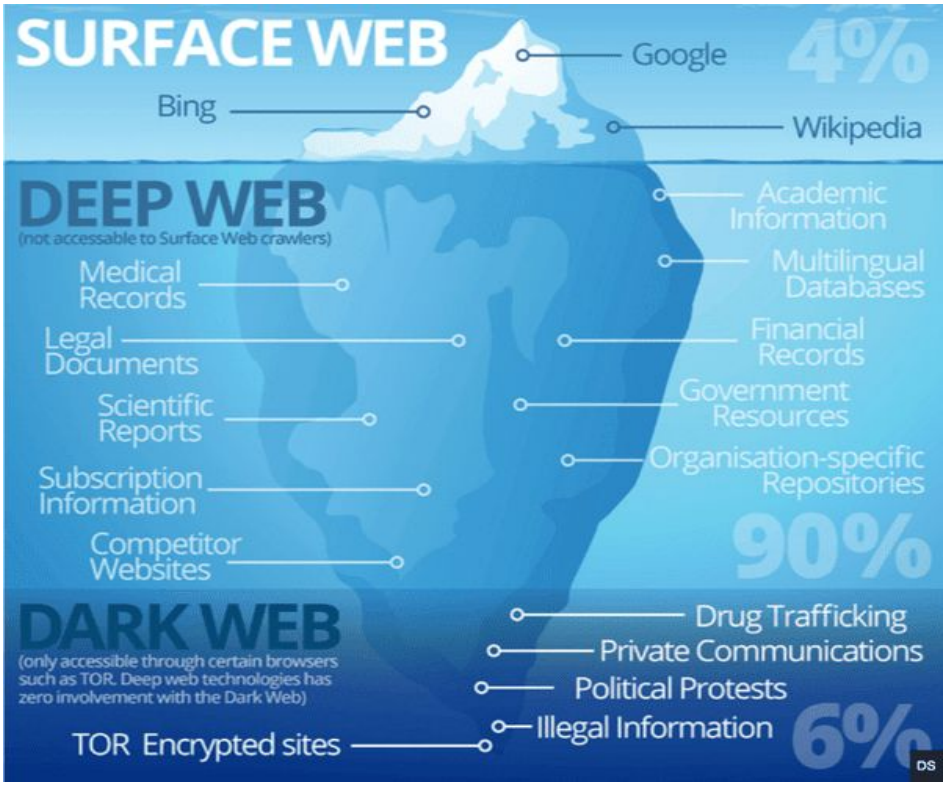

Figure 1. Levels of the Web. Reprinted from https://i1.wp.com/www.skyindya.com/wp-content/uploads/2017/01/surface-web-vs-deep-web-vs-dark-web-2.png?ssl=1

1.1 Surface Web

Even those who consider themselves active and frequent Internet users might have discovered only a fraction of the real content of the web. Awoyefa (2019) explains that the Surface Web is a term that describes a part of the Internet that can be found through the search engines such as Google and Bing. This part of the Internet is believed to contain just about 0.03 % of all the information on the web, leaving potentially almost an unlimited number of web pages that are owned privately. Norton (2016) debates the extreme limitations of the Surface Web.

Norton (2016) claims that "the easy answer is that the Surface Web is extremely limited in terms of providing information, and much in the same way as a TV network plans its schedule, there isn't much "exploring" to do on the Surface Web" (p. 7). Google, Bing and other web crawling search engines manipulate search results and whispers (finishing sentences while using search engines) for not so clear business purposes. It is also believed that the Surface Web only provides "mainstream" one-sided points of view to certain stories and controversies to support commercial sector and the government. To evade this, one may consider the Dark Web as a mean to access underground political views, alternative viewpoints, underground books, new and unexpected information or to avoid mass surveillance.

1.2 Deep Web

According to Drbola (2016), the Deep Web is a part of the Internet whose content cannot be simply accessed through a so called "web crawling browser" such as Google. In other words, it is not possible to click on a link to access a web page with universal content. A login (username and password), or even in some cases a universal link, will be required to access such content. Internet users might be familiar with this part of the Internet, too. The zone of the Deep Web is possible to enter by means of login to a Facebook account or online payment. Abdel (2017) further asserts that this hidden, non-indexed web is believed to be 400-550 times larger than the Surface Web, even though its actual size cannot be precisely measured since most information is locked and hidden. Content on the Deep Web can also differ from a state to state. Some authoritarian states might censure a certain web

pages for political reasons. These pages would then not appear while searching because they, for instance, include a specific blacklisted phrases or words.

1.3 Dark Web

Drbola (2016) additionally points out that "the Dark Web is a subdivision of the Deep Web". Similarly to the Deep Web, the Dark Web sites cannot be accessed through regular web crawling search engines, or through a regular web browser. When selecting this web browser, a user has an option to choose different types of software. This thesis will deal with software called Tor which is open source software[1] for anonymous communication between its users. Even though anonymity creates a space for free speech and political discussions without the government having knowledge of it, it can also be exploited. The Dark Web is notoriously known for its trade with drugs, guns, child pornography and other black-market transactions.

Moore and Rid (2016) carried out an analysis of the Dark Web to help classify its content. They chose an approach of "an in-depth, lengthy web-crawl of every web-based hidden service reasonably accessible by an individual seeking content within the Dark Net" (p. 19). This web-crawler[2] went through roughly 300,000 addresses inside the Tor network with hidden services which provided data from 205,000 unique pages. As a result of this scan, the Dark Web content can be divided into 12 different categories (see Figure 2). The program then classified scanned pages (5,205 live websites) into the categories with a high level of confidence (some pages were randomly inspected for potential errors) as shown in Figure 3.

[1] Open source software is software whose code is available to general public, typically created as a collaborative effort (Beal , 2014).

[2] "Web-crawler" is a program that follows links like a person surfing through the Dark Web would. The program was designed to go up to five levels deep into each site and scan a maximum of 100 pages within each site (Moore & Rid, 2016).

Category	Details
Arms	Trading of firearms and weapons
Drugs	Trade or manufacture of illegal drugs, including illegally obtained prescription medicine
Extremism	Content espousing extremist ideologies, including ideological texts, expressions of support for terrorist violence, militant how-to guides and extremist community forums
Finance	Money laundering, counterfeit bills, trade in stolen credit cards or accounts
Hacking	Hackers for hire, trade or distribution of malware or DDoS[45] capabilities
Illegitimate pornography	Pornographic material involving children, violence, animals or materials obtained without participants' consent
Nexus	Websites primarily focused on linking to other illicit websites and resources within the darknet
Other illicit	Materials that did not easily fit into the other categories but remain problematic, such as trade of other illegal goods and fake passports or IDs
Social	Online communities for sharing illicit material in the form of forums, social networks and other message boards
Violence	Hitmen for hire, and instructional material on conducting violent attacks
Other	Non-illicit content, such as ideological or political content, secure drop sites, information repositories, legitimate services
None	Websites which were either completely inaccessible or otherwise had no visible content, including websites which hosted only placeholder text, indicating that their operator had yet to generate indicative content

Figure 2. Categorization of content on the Dark Web. Reprinted from More and Rid (2016, p. 20)

Category	Websites
None	2,482
Other	1,021
Drugs	423
Finance	327
Other illicit	198
Unknown	155
Extremism	140
Illegitimate pornography	122
Nexus	118
Hacking	96
Social	64
Arms	42
Violence	17
Total	5,205
Total active	2,723
Total illicit	1,547

Figure 3. Classification. Reprinted from More and Rid (2016, p. 21).

Pages classified as the "None" category had a lack of content for proper classification and pages classified into the "Unknown" category were either illegal (as pages with illegal content were either skipped or immediately discarded) or it was too sparse to determine its nature. The results of the scan suggest that the use of Tor hidden web services is rather illegal, since more pages include the content such as illegal pornography (pornography that involves children, animals, violence or materials obtained without the individuals consent), trade with drugs and weapons, hacking and murders for hire.

2 The Origins and History of the Dark Web

2.1 Original Motivation Behind the Creation

Why does the Dark Web exist in the first place? It serves many purposes and their legality can be often rather questionable. However, even the most obvious ones, such as drug dealing, and similar illegal activities were not the motivation for this technological wonder to be born. The Dark Web accessing tool that this thesis will deal with, The Onion Router (henceforth Tor), was formerly developed by the United States government. According to Veaux (2019):

> The idea of an encrypted, anonymizing, onion-routed network came from DARPA, the Defense Advanced Research Projects Agency. The first onion routing software was developed at the Naval Research Laboratory. Initially, Tor was supported financially by the US State Department. Further financial support of Tor came from the National Science Foundation.

Hale (2019) further claims that the anonymous exchange of information was the main motivation behind the creation of the Dark Web. Tor was then released as open source software so government messages could be hidden among thousands of other messages of other users.

2.2 Brief History

Many people might think that the Dark Web is something that has been developed quite recently. Nonetheless, the opposite is true. Breeding (2019) speculates that it has been around "since the beginning of the Internet" itself. The very first electronic message from one computer to another was sent on 29 October in 1969 by a student at the University of California, Los Angeles (henceforth UCLA), using the system called ARPANET[3]. Very shortly after non-indexed hidden websites ("Dark Nets") that used ARPANET's framework were established. Butler (2018) additionally comments that in the early 1970s, the very first item purchased on the Internet was marijuana, sold by UCLA students to Massachusetts Institute of Technology (MIT) students. At that time, Stanford students used ARPANET for drug dealing.

[3] ARPANET stands for the Advanced Research Projects Agency Network.

According to Butler (2018), "the Dark Web proper really got its start in March of 2000 with the release of Freenet[4]". He believes that this software is a "true implementation of the Dark Web" that made online illegal activities, such sharing pirated content or pornographic material, possible. However, since cryptocurrencies have not existed yet, it was rather challenging for ~~a~~ money exchange to happen anonymously. Butler (2016) also believes that:

> The most important Dark Web development of all time happened in 2002, with the release of Tor or *The Onion Router*. It was created by non-other than the US government, as a way to help their own operatives remain untraceable. It's no exaggeration to say that the Dark Web of today could not exist without this technology. Late in the 2000s came the advent of cryptocurrency in the form of Bitcoin. The final piece of the puzzle needed to make the Dark Web really click.

In February 2011, the Silkroad was founded and operated by Ross Ulbricht, also known as "Dread Pirate Roberts" (Summers, 2017). The Silk Road was a place where Tor and cryptocurrency together created the very first proper online black market. The foundation of this site was a reason for the Dark Web to rise to the surface, becoming a topic of public concern.

[4] Freenet Project (n.d.) describes its software as a "peer-to-peer platform for censorship-resistant communication and publishing".

3 Accessing the Dark Web

It has already been made clear that to access the Dark Web a special piece of software is required. Questions such as how to access the Dark Web, how to get Tor, how it works and how to remain anonymous will be dealt with in this chapter.

The world is getting smaller with new technologies. Due to the development of the Internet, one person might always be connected to the other seven billion people. We live in an era where a small piece of technological device, such as a smartphone, with the access to the Internet will give its user unlimited access to all the knowledge of the world. There are, nonetheless, disadvantages, too.

All the data of the Internet, including data of its users, are stored on servers. Summers (2017) explains that information exchange between the server and a client (any device connected to the server such as computer or smartphone) is a two-way affair because

> …at the same time that the individual receives a package of information from the server, a package of his or her own information is exchanged. This includes data on browsing habits and location. As it is transferred, this data can be visible to others (whether government or private enterprises) who can observe and keep track of an individual's Internet behaviour. (p. 7)

Cody (2017) further says that if the Internet user only used a regular web browser such as Google Chrome and a regular web searching engine, all their sensitive information would be disclosed to others including search preferences, cookies, search engine history, personal information, pictures, videos or even locations you frequently visit. This information can be abused in many ways. To protect the Internet users from cybercriminals and personal information leakage several software programs, such as Tor, that allow them to use the Internet services anonymously were developed

3.1. The Onion Router, Tor

When a connection between a server and its client is established, information flows both ways from one device to another, making them visible in the cyberspace and vulnerable to

abuse. To prevent this and protect the users from cybercrimes, tracking and surveillance, the non-profit organization named the Tor project with the funding help of the United States government developed an Internet browser Tor that lets the user browse the web anonymously. The Tor Project (n.d.) describes Tor as an anonymous browser that lets you "browse privately and explore freely". According to this website, Tor blocks trackers, defends against surveillance, resists fingerprinting and encrypts users' traffic into three different layers, making the user essentially anonymous and untraceable.

Geeks for Geeks (n.d.) describes onion routing as an encryption method that encapsulates a message into multiple different layers to establish anonymous communication across a computer network. Web browsers such as Chrome or Firefox establish a direct connection between a client (user) and a server that the user requires an information from so anyone monitoring the network (the Internet provider, government, etc.) has a knowledge of what is happening between these two entities. The onion routing aids this by encrypting the message and sending it through multiple nodes before it reaches its final destination. Each node then only has one part of the key required to decipher the message and address of the next node.

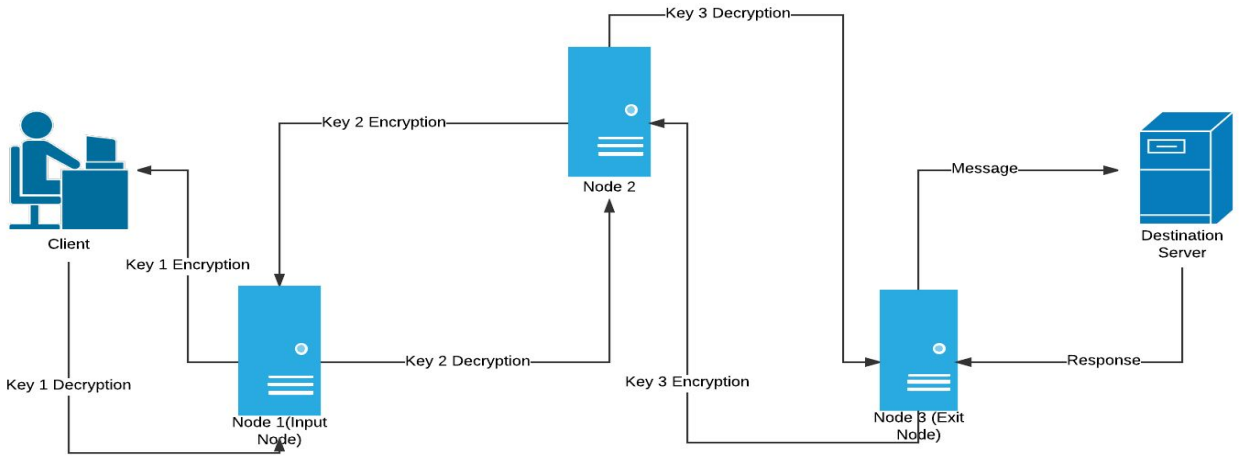

Figure 4. The onion routing.
Reprinted from https://www.geeksforgeeks.org/onion-routing/

Figure 4 illustrates the onion-routing based connection between a client and a destination server. The client that has access to all three keys (key 1, 2 and 3) encrypts the message into three different layers. Like the onion, layers of this message must be peeled one at the time (that is where the name "onion routing" comes from). A message (encrypted into three layers) is sent to a Node 1. Since the node only has the key 1 and the address of the next node (Node 2), it deciphers one layer of the message and then passes it to the next node (Node 2). This action repeats until the encrypted message reaches its final destination. The destination server then sends its response back through the same nodes to the client while each node adds a layer of encryption to the message. When the message (again three times encrypted through the nodes) reaches the client, it can be deciphered since the client has all three keys. To stay completely anonymous, nonetheless, the user needs to also follow a set of rules.

3.2 How to Remain Anonymous

The anonymity that Tor provides is, however, vulnerable to users' ignorance and inexperience. In other words, one little mistake can imperil the anonymity provided. This would cause the user to leave traces behind even when surfing the web via the onion router. In order to stay anonymous a set of rules must be followed, and a user might even rethink the way they surf on the web.

Luke (2018) suggests that users should not use their personal information while using the Tor browser, such as using the same usernames, their credit and debit cards and personal emails. Instead, he advises users to create an anonymous persona which they should stick to, transact in cryptocurrencies and use Tor-based temporary email services. Browser cookies should be either deleted or completely prevented. Cody (2016) additionally emphasizes that users should neither download (do not use peer-to-peer connections such as Torrents) nor open files through the Tor browser, since such doing is traceable for authorities and the Tor will not provide protection against it. This way the users only slow down the whole network for the other users. In order to stay anonymous, users must not use regular "web crawling" search engines such as Google and Java scripts and Flash and Java because they collect personal data about their users. Hussain (2016) adds that Google

should be especially avoided since it collects the data about the user in many ways such as through ads and search history, making it relatively easy to identify the user. Cody (2016) also suggests that users should

> Use HTTPS. The node exits from the Tor network are the most vulnerable points for your anonymity. Tor encrypts the information within its network and camouflages the source of your activity. However, the activity outside the network is exposed. What can you do about it? Make a consistent use of end-to-end encryption, such as SSL or TLS. (p. 33)

If a user really values their privacy and wants to remain anonymous, they should know and follow rules stated above. Tor's encryption techniques provide a great camouflage, but it is not completely bulletproof.

3.3 Advantages and Disadvantages of Using Tor

There are both advantages and disadvantages to the use of Tor. The user should be aware of them while making the use of it either to get the maximum benefits or to avoid potential problems.

The most important and obvious advantage of Tor is the anonymity it provides (as long as users' behaviour is not in conflict with the rules). According to Deep Web Sites (2019), the advantages of Tor are the software being open source, eliminating the potential occurrence of malicious backdoors, censorship circumvent, onion sites support, and IP address hiding. Another great advantage is availability, simplicity and easy set-up. Norton (2016, p. 12) points out that "the Tor web browser is actually modelled after Firefox and thus it's not too hard to figure out". Tor is also free of charge.

Klein (2015) claims that main disadvantage is the Tor's rather slow performance. Norton (2016) explains that the reason for that is all the Tor's traffic is shared with its users and data also must travel much greater distances. Klein (2015) further compares the Tor to "the red flag on the map" saying that the Tor may provide a user with a "false sense of security", while only giving the government a reason to monitor their traffic.

Tor will provide the users the anonymity for as long as they respect these rules. Do not use HTTP protocol, encrypt your data with suitable add-ons, disable Flash and Java scripts, do not establish peer-to-peer connections, delete cookies or use add-ons that prevent their collecting, do not use regular web crawling browser and do not use your real personal email address. And most importantly avoid illegal activity. Tor makes it significantly harder for authorities to reach the user who performs illegal activities, but not impossible. Users should remember that Tor is still in a development phase and is not bulletproof: it is only as safe as the user makes it.

3.4 Tor Users and the Reasons Why They Use Tor

As already stated above, the Dark Web has been a topic of a public concern since 2011 with the opening of the Silk Road and it is no surprise that opinions and attitudes are rather negative. However, there are users with intentions that are not necessarily bad or illegal. Very important is that the usage of Tor and the Dark Web itself is not an illegal act. Summers (2016, p. 7) claims that the Dark Web is a place where "journalists in countries which have repressive laws against freedom of Internet use" operate. Journalists can use the Dark Web as storage of sensitive information, a place where they can interview people that wish to stay anonymous, verify information and to publicize their articles without government's involvement and censorship. Summers (2016) further says that the Dark Web is also praised by academics and ordinary people who wish to embrace the freedom of speech, activists or people with political agendas. Winter (2015) compares the Dark Web to the bathroom door, explaining that closing it is not an unethical or illegal act. However, what is happening in the bathroom while the door is shut is a different thing. The Dark Web, due to its concept, provides a shelter for criminals. According to FindLaw (2019) "any type of crime with covert transactions, whether it involves drugs, money, or even human beings, can be committed on the Dark Web". The web page lists a few examples of frequent crimes on the Dark Web such as illegal drugs sale, illegal arms sale, murder for hire, blackmailing, terrorism, child pornography or even sex trafficking. FindLaw (2019) further claims that in Britain alone roughly 144,000 people used the Dark Web to gain access to child pornography.

Tor provides the Internet users with a basic human right, which is the right for privacy. How privacy could be kept, used or, in many cases, exploited, could be a problem. It is advised not only to follow the rules mentioned above in this chapter, but also to respect the law and ethics. The best way to remain anonymous is not to attract any attention.

4 Cryptocurrency, Bitcoin

Cryptocurrencies are the last piece of puzzle that made the Dark Web shape into its present form. Rosic (2016) describes cryptocurrency as "an Internet-based medium of exchange which uses cryptographical functions to conduct financial transactions". Cryptocurrencies work based on a so-called blockchain[5] technology, providing them immutability, transparency and decentralization, meaning that they are under no control of government or any other institution. However, similarly to a network for file sharing, cryptocurrencies work on a peer-to-peer principle or, in other words, on a direct connection between two users.

4.1 Bitcoin

The above-mentioned Moore's and Rid's analysis of the Dark Web content shows that many sites that were examined offer a "services for laundering money through Bitcoin" (p. 17). According to Ledger (2019), Bitcoin is the oldest and the most wide spread (mostly thanks to the Dark Web) cryptocurrency to this date. Concept of Bitcoin was first described in 2008 by the Bitcoin founder, Satoshi Nakamoto. Nakamoto published a white paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" in which he describes Bitcoin blockchain network. Nakamoto (2008, p. 2) describes Bitcoin as "a chain of digital signatures". Transaction is completed by an owner digitally signing a hash[6] of the previous transaction and the public key of the next owner, both pieces of information added to the end of the coin (see Figure 5).

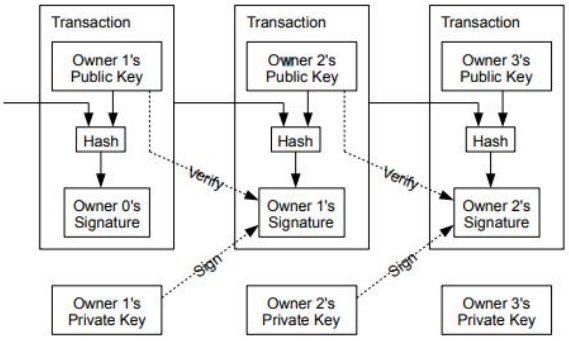

Figure 5. Bitcoin transaction. Reprinted from Nakamoto (2008, p. 2).

[5] Blockchain is referred to as a public record of transactions (Fortney, 2019).

[6] Hash is an essential part of the blockchain management in cryptocurrencies. It is a function that "converts an input of letters and numbers into an encrypted output of a fixed length" (Frankenfield, 2019).

The main problem with this scheme is that even though a creditor can through these signatures verify the chain of ownership, he cannot verify if one of the previous owners did or did not double-spend[7] the coin. This could be solved by running the currency through a trusted central authority or a mint that would check tokens for double-spending. That, however, introduces a problem of an authority or a mint to have a full control over the entire money system and, similarly to the bank, every transaction would have to go through them. Nakamoto proposes a solution to the problem starting with a timestamp server. The only way a user can prevent double-spending is that they need to be aware of all transactions. He claims that these transactions need to be made public and agreement of participants on a single history of the order in which transactions were received is needed as well. This should provide a proof for the creditor that at the time of each transaction, the higher number of nodes agreed the transaction was the first one to be received. Nakamoto (2008) says that

> The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

See the Figure 6 for the illustration of the solution to the above-mentioned problem.

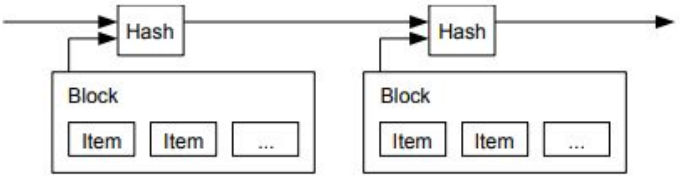

Figure 6. Timestamping. Reprinted from Nakamoto (2008, p. 2).

Since all transactions through Bitcoins are made public to ensure that the tokens are not being spent multiple times, users might be rather sceptical about the privacy and

[7] Double-spending is referred to as a potential fraud in a digital cash scheme. Cryptocurrencies consist of a digital file that can be either duplicated or falsified, meaning that one digital token could be spent multiple times (Frankenfield, 2019).

anonymity of transactions that they make. Transactions made through a common bank system are private due to the access to the information about the users and a third party being strictly limited. Manipulation with cryptocurrency may violate one's privacy and disclose any personal information. Drbola (2016) observes that "many different pieces of software were lately developed to help to solve the issue" (p. 29). They work on a basis of combining transactions, dividing them into smaller portions and then uniting them again. As an example, Bitcoin mixer 2.0. (n.d.), which is an Internet service using this method, replaces entrusted Bitcoins into verified coins from European, Asian and North American stock exchanges. This should provide a higher level of anonymity and reduce the risk of getting coins whose character is rather questionable. A commission fee is a dynamic value that can go up to 3.9 % of the total amount cleansed + 0.00015 BTC. Drbola (2016) points out that a birth of such services also made first frauds and thefts of cryptocurrencies possible, which significantly reduced a trust in them. Transactions made on the Dark Web that go through a good marketplace are usually automatically mixed, so users do not have to worry about the issues with privacy or risk the use of coins-mixing services.

Cryptocurrencies, namely Bitcoin, are essential part of the Dark Web and together with the Tor browser created an anonymous marketplace. The very first and arguably the most known marketplace, Silkroad, is to this date notorious for its large trade with illegal goods and services of all sorts. Although the former founder of Silkroad was arrested many years ago, that did not put the end to the Dark Web black markets.

5 Silkroad, the Notorious Dark Web Marketplace

Thanks to the invention of cryptocurrencies, mostly Bitcoin, a number of online black markets emerged. The notorious Silkroad was one of the first online marketplaces with illegal goods and services ever. Its large impact influenced the Dark Web on a great scale and changed it forever since.

According to Summers (2016), roughly 80,000 drug users from forty-three different countries went in 2014 through a survey that asked them where they get their drugs from (p. 9). The results showed that the number of people who are buying their drugs online is increasing. Most drug purchases made on one particular website, the Silkroad.

One of the earliest mentions about the Silkroad dates back to November 27, 2010 on the forum called "The Shroomery" (magic mushroom-related forum) by a user named "Altoid". Altoid posted a post asking other forum users whether they have heard about the Silkroad since he was considering using their anonymous services. Shortly after that, he posted a very similar post on bitcointalk.org providing links to a WordPress blog about the Silkroad. Few months after, in 2011, the Silkroad began to gain attention as more users were creating their accounts as vendors which inevitable brought more customers. By the May 2011, approximately 300 listings on the website had been created while most of them sold illegal drugs.

Summers (2016) suggests that the main reason why the Silkroad became so popular is that "it was infinitely more secure than the unstable and informal online deals users were used to partaking in, either interpersonally via forums or through less secure sites such as the Farmer's Market[8]" (p. 10). The website was professionally and formally designed and maintained, had a simple navigation layout, easily accessible links to customer services and a shopping cart with an account balance. The way to carry out transactions was strictly limited to cryptocurrencies only and the services were accessible only via the Tor browser. Summers (2016) adds that

[8] Farmer's Market is an illegal drugs-selling online service that appeared in early 2000s when such online services first expanded. They became a Tor hidden service in 2010. (Summers, 2016)

> All digital communications between users on the site were secured via PCP encryption, automatically erasing messages once they were read. A more secure forum was introduced in June 2011 to allow for easier contact between buyers and sellers on the website.

When Altoid became a member of the Silkroad's management team, he posted a post on bitcointalk.com where he announced that he was recruiting for the website's technical maintenance team. Technical maintenance team consisted of two to five people and their job was to help with customers' problems and to answer their questions. Via a private email system established on the website, they also made weekly reports to the main administrator of the website, Ross Ulbricht (also known as "Dread Pirate Roberts").

Gehl (2018, p. 99) describes the Silkroad marketplace as "Amazon" or "eBay" that sells illegal substances and works on the basis of a user-feedback system and agorism, meaning that it seeks to achieve free society and supports free market with use of non-state currencies and creates state-independent communities.

The Silkroad received commissions from all the transactions that were made through the website. According to Summers (2016), members of the technical maintenance team were making approximately $1,000 to $2,000 per week through those commissions (p. 11). By the July 2013 (two years into the website's existence), about 4,000 sellers and 150,000 customers together had created a black market through which roughly $1.2 billion passed, making it with no doubt the most successful illegal marketplace ever to exist.

The Silkroad's popularity did not stop growing and its name even made an appearance on popular websites on the Surface Web such as 4chan and Reddit. The FBI, however, had been working on taking the website down since 2011. The undercover FBI agents were posing as buyers on the website, closely monitoring the largest vendors and site administrators (including Ross Ulbricht). The main website administrator, Dread Pirate Roberts, was arrested on October 1, 2013. According to Nikolova (2019), he was accused and subsequently convicted of aiding and abetting distribution of drugs, continuing criminal enterprise, computer hacking, fraud with identification documents, money

laundering and now serves a life sentence in Metropolitan Correctional Center in New York.

Winter (2015) argues that the Silkroad was a political movement rather than anything and was more about the community of the like-minded people rather than the trade with illegal substances. Greenberg (2013) assembled Ulbricht's writings from the Silkroad's forums to found out his motives and ideologies. According to those writings, the Silkroad was founded and continued to be operated on libertarian principles. Since the market was out of the government's reach, it was fully regulated by supply and demand of the Silkroad's vendors and customers. Vendors could sell anything that causes no harm to other human beings such as counterfeit money, falsified tickets, child pornography or murders for hire. Any substance, as Ulbricht notes, does not violate that rule.

Silkroad was arguably the largest as well as the most successful online black market with illegal substances and other goods to ever exist. Even though it was banned almost seven years ago by the FBI, it had an enormous impact on the way the technology, the Internet and the Dark Web are used today.

6 The Major Uses of the Dark Web and Tor

The anonymity promised by the Tor browser while navigating through the Dark Web can attract numerous groups of users with very different intentions. Excluding drug and weapon sellers and other cybercriminals, a not negligible number of civilians use the Dark Web for legal actions, such as seeking protection from corporations, that might collect and possibly leak users' personal information, avoid censorship and gain access and ability to intervene in sensitive topics without being targeted (politics and controversies).

Nonetheless, this promise of anonymity also attracts users with intentions performing illegal activities. According to the already mentioned Moore's and Rid's analysis of the Dark Web content, most of the Dark Web webpages host a kind of illicit content.

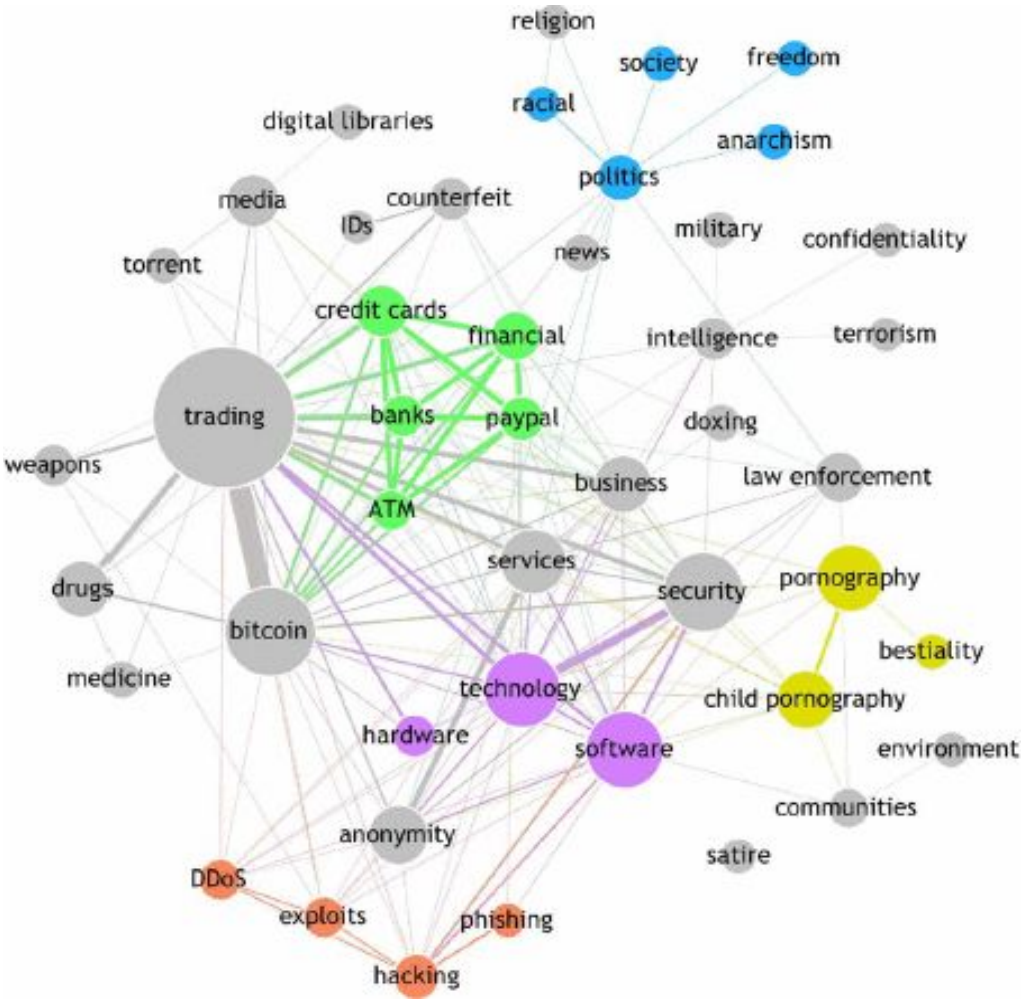

Figure 7. Taxonomy of the Tor's hidden services.
Reprinted from Splitters, Verbruggen, Staalduinen (2014).

Figure 7 illustrates the representation of the various topics and content that can be found on the Dark Web through the Tor browser. The size of each node represents the degree of presence of each topic and the thickness of the connection lines between nodes illustrates the relatedness of different topics to each other. Nodes with the same colour then belong to the same topic group (green = financial, purple = technology, orange = hacking, yellow = pornography, blue = politics). According to Splitters, Verbruggen and Staalduinen (2014), about 59 % of the Dark Web hidden services include at least some form of trading. Most trading include drugs, arms, counterfeit money and documents, hacked accounts, and stolen credit cards. 20–25 % is then software and security, 10–15 % child pornography and drugs and 2–5 % weapons, anarchy and doxing.

6.1 Illicit Hidden Services

6.1.1 Terrorism

Weimann (n. d.) points out that terrorists and extremists have been active on various platforms since the 1980s. Taking into account the traceability of events that are happening on the Surface Web, using the Surface Web for illicit actions of any sort is very risky on the users' part. In order to remain anonymous and not get tracked down, terrorists use the Dark Web for various purposes, such as passing information to other terrorists, planning attacks, recruiting new members and supporters, spreading propaganda, raising funds and purchasing of weapons via anonymous cryptocurrencies.

In the past, terrorists had to rely on attacks being large enough to attract the attention of television producers, radio broadcasters and print publishers. Stacey (2018, p. 18) reports that fatalities caused by terrorists in 2000s claim ten times more victims in a comparison to fatalities that happened in 1980s. This was achieved by the terrorists' use of more sophisticated weaponry and attack coordination via new communication technologies such as Tor. Jihad, unlike Al Qaeda, is much more opportunistic in spreading their message. Jihad makes its social media activity that involves violence purposely public to individuals that have no actual ties to it. Whenever a terrorist organisation recruited more fighters and supporters, those fighters and supporters had to cross borders to access the training in the

Middle East. The digital era, however, with all its communication technology that enables users to stay anonymous eliminated this complication and radicalization has become a matter of a couple clicks on the right website.

Edwards (2019) asked a security expert Michael Osborn a question "how do terrorists recruit people on the anonymous corner of the Internet known as the Dark Web?". Michael Osborn deals with some of the issues related to the topic of the European project called "PROTON" to get better understanding of criminals' behaviour online. This project focuses on the terrorism recruitment and cybercrime to find out what influences criminal behaviour on the larger scale to inform a policy response. This includes searching through not only the Dark Web, but also popular social media platforms. Osbron (2019) remarks that "it's all about modelling the journey into recruitment". To achieve that, the establishment of a generic profile of the Internet user that may be susceptible to become involved with cybercrime and terrorism online is a key step. Osborn compares this method to the approach chosen by the police when looking for a criminal suspect. This method in both cases helps to reduce the possible suspects.

In November 2015, after terrorist attacks in Paris, the terrorist organisation ISIS (The Islamic State of Iraq and al-Shams – Greater Syria) used the Dark Web to spread news and propaganda. They tried to keep the identities of the group supporters secret and protect their content from the hackers, since hundreds of websites including some form of content related to the ISIS were taken down as a part of the so called "Operation Paris" launched by the notorious group of hackers Anonymous.

After attacks on Britain in 2017, the government decided to spend more time and funds to combat terrorism online, especially paying attention to the Dark Net, where terrorists try to hide their actions and intention.

6.1.2 Pornography

Pornography with illicit content, such as child pornography, bestiality, videos taken without the consent, extreme violence or even rape followed by a murder are an integral part of everyday trading on the Dark Web. According to the above-mentioned Splitters's, Verbruggen's, Staalduinen's research, child pornography itself creates about 10–15 % of the Dark Web content, which is an enormous amount of data considering the actual size of the Dark Web.

According to Dredge (2014), a study, carried out by a researcher Dr Gareth Owen, revealed that more than 80 % of the traffic on the Dark Web is generated by visits to websites that are dedicated to a child pornography content. Despite the fact that paedophile materials estimated only 2 % of 45.000 analysed Tor hidden web services, "they account for 83 % of visits to these sites once automated "botnet" traffic is removed from calculations". The study also found out that when the study began in March, only 17 % of websites were still online in September, meaning that a lifespan of sites offering such content is rather short.

Farivar and Blankstein (2019) point out that "Federal prosecutors have filed multiple charges against a 23-year-old South Korean man accused of running what they call the world's largest Dark Web child porn marketplace." In March 2018, probably the largest Dark Web child pornography marketplace was taken down by the U.S. government after it was three years in service. Roughly 8 terabytes of data (more than 200.000 unique videos) were to be found on a hidden service called "Welcome to Video" through which about 7.300 bitcoin transactions were processed, forming together more than $730,000. The main person behind the marketplace, 23-year-old South Korea citizen, together with other 337 suspects from all around the world, were tracked down and arrested. When the site was seized, the United States authorities posted there a warning (Figure 8).

Figure 8. Warning posted by United States authorities. Reprinted from Farivar and Blankstein (2019).

6.1.3 Arms Trade

Even though there are serious attempts to regulate the arms trade, there are a few ways that let illegal gun sellers bypass them and use hidden services on the Dark Web together with a cryptocurrency as one of them. Trading with weapons is estimated to form around 2–5 % of the Dark Web content, although it should be noted that the actual size of these markets is not clear.

RAND (n. d.) proposes that the public became more concerned and aware of the issue after the Munich shooting in 2016, where a single terrorist used weapons that were purchased on the Dark Web. RAND Europe together with the University of Manchester carried out a

study, commissioned by the ESRC (Economic and Social Research Council), in which they focused on the Dark Web impact on contributing and enabling arms trade.

This project focused on seven main issues:

- methods of buying and selling weapons and related goods;
- viability of the online markets with weapons and likeliness of vendors attempting to scam the buyer;
- size and scope of markets, number of markets listing weapons and related goods;
- value of weapons and related goods;
- shipping techniques and routes;
- overall impact on the arms trade;
- law enforcement agencies and policy markets on the issue.

Several research methods were developed by the project team to get answers for these questions:

- a review of relevant literature from multiple sources, such as peer-reviewed academic literature, grey literature from trustworthy sources and web-sourced materials from appreciated commentators and researchers in the Dark Web community;
- a review of the materials from the Dark Web community found on the Surface Web, including websites that are used to classify marketplaces and cater information and comments on how cryptomarkets are currently developing;
- a review of the Dark Web community discussions on forums about the issue of scamming of firearms sellers;
- the analysis of cryptomarkets to classify the portion of them selling weapons;
- the analysis of the digital traces left after marketplace transactions;
- individual interviews and expert workshops with policy and law enforcement experts.

The study found out that the Dark Web was a great tool for selling and circulation of illegal weapons with a potential to be a source of diversion for weapons that are owned legally. The Dark Web provides a source from which more performant weapons can be bought for the same or even lower price than on the black market on the streets. As it seems, roughly 60 % of the products originate from the United States, however, market in the Europe is the largest illegal firearm market with revenues almost five times greater than the United States. The most found listings on the Dark Web appeared to be listings with weapons, constituting 42 % of the all listings found on the Dark Web, followed by the listings with guns-related digital products (27 %) and ammunition (22 %). Weapons sold the most are hand pistols (84 %) followed by rifles (10 %) and sub-machine guns (6 %). Arms-related digital products are guides and tutorials for a variety of illegal behaviour, such as conversion of replicas into fully functioning weapons, manufacture of home-made guns and explosives and 3D printing of real firearms.

Because of the anonymity provided by the Dark Web marketplaces, law enforcements agencies and national governments face additional challenges attempting to regulate the firearms trade worldwide. Even though the Dark Web trade with weapons is not large enough to supply conflicts, it is a potential platform of choice for so-called “lone-wolves terrorists” or gangs to obtain weapons and ammunition anonymously. Some listings of weapon vendors were also observed to be fake, nonetheless, it seems to be almost impossible to determine the extent in which buyers are being cheated.

To summarize the results of the study, the Dark Web introduces a completely new way of acquiring weapons anonymously and brings forth several challenges for policy and law enforcement agencies that attempt to ban the illegal trade. Except providing a guides and tutorials to manufacture homemade guns and explosives, the Dark Web does not create new weapons, it rather acts as a means for their trafficking.

6.1.4 Hacking and Doxxing[9]

The role of hackers has significantly changed as the time passes and they are no longer known just as criminals who try to hijack bank accounts, emails or social media accounts. Nowadays, companies and firms are even paying hackers to try to penetrate their security systems. This way companies, firms and other institutions can truly put their security features through a real test and possibly improve them if hackers get through.

However, that does by no means eliminate the possibility of being specifically or mass targeted by a hacker. Hacking services, ranging from hijacking social media accounts to taking down entire websites, are sought commodities on the Dark Web.

Product	Price
Hacking	
Hacking web server (vps or hosting)	USD 120 (0.49 BTC at the time I'm writing)
Hacking personal computer	USD 80 (0.49 BTC at the time I'm writing)
Security Audit	
Web Server security Audit	USD 150 (0.62 BTC at the time I'm writing)
Social media account take-over	
Social media (FB, Twitter, etc.) - account hacking	USD 50 (0.21 BTC at the time I'm writing)
Spyware and Device Tracking	
Spyware development	USD 180 (0.74 BTC at the time I'm writing)
Device Tracking	USD 60 (0.25 BTC at the time I'm writing)
Intelligence and Investigation	
Intelligent report - locate people	USD 140 (0.58 BTC at the time I'm writing)
Intelligent report - background checks	USD 120 (0.49 BTC at the time I'm writing)
Fraud Track - Find your Scammer	USD 120 (0.49 BTC at the time I'm writing)
Cyber extortion	**To be agreed prior contact**

Figure 9. Hacking services on the Tor website called "Hell". Reprinted from Paganini (2019).

[9] Gonimah (2019) explains that doxxing means breaching into someone's personal computer/cloud storage and making their personal data public.

As Paganini (2019) points out, there are several websites that you can choose from while looking for hacking services, such as Rent-A-Hacker, Hacker for Hire and Hell. Figure 9 illustrates what services can be purchased for what prizes on the Tor website called "Hell". This website is divided into different sections that relate to hacking tools, hacking tutorials and hackers offering their services. Websites such as this one offer not only a protection of both hacker and a client, but also the possibility of validation of hacker's reputation or qualification. Hell offers various hacking services ranging in price from $50 to $180.

Product	Price
Hacking	
Hacking web server (vps or hosting)	USD 250 (1,04 BTC at the time I'm writing)
Hacking personal computer	USD 200 (0,83 BTC at the time I'm writing)
Hacking Social Media Account (Facebook, Twitter)	USD 300 (1,25 BTC at the time I'm writing)
Gmail Account Take over	USD 300 (1,25 BTC at the time I'm writing)
Security Audit	
Web Server security Audit	USD 400 (1,66 BTC at the time I'm writing)
Malware	
Remote Access Trojan	USD 150 - 400 (0,62 - 1,66 BTC at the time I'm writing)
Banking Malware Customization (Zeus source code)	USD 900 (3,75 BTC at the time I'm writing)
DDoS attack	
Rent a botnet for DDoS attack (24 hours)	USD 150 - 500 (2,08 - 1,66 BTC at the time I'm writing)

Figure 10. Hacking services on the Tor website called "TheRealDeal". Reprinted from Paganini (2019).

Paganini (2019) decided to contact a few hackers on the website TheRealDeal who offered their services there. The result of his research confirms the possibility of hiring a hacker to

gain unauthorized access to numerous spaces, such as websites, personal computers, social media accounts or rent a botnet that executes DDoS[10] attacks.

The hacking communities and forums are usually specialized in specific topics, such as hacking social media accounts, malware and exploits, DDoS attacks and others. Since the general public (almost always) does not have access to such forums and communities, one must request an invitation to be able to join the discussion.

6.1.5 Drugs and Other Illegal Substances

The Dark Web is notorious for its trade with illegal substances. Trade creates roughly 60 % of the Dark Web content and illicit substances have a great contribution to that. Authorities not once claimed victory over the online black markets, it did not take too long though for them to rise again.

Since the shutdown on the Silkroad in 2013, the online black market with illegal substances has grown even larger. RAND (2016) claims that regardless on the law enforcement's effort to prevent this, the number of transactions has tripled, and revenues doubled as of 2016 (see Figure 11).

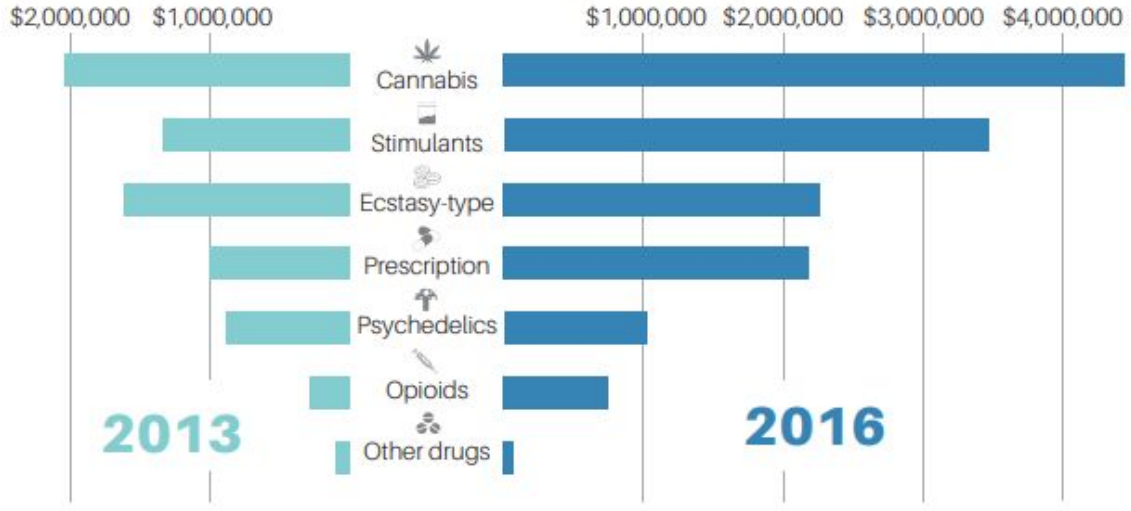

Figure 11. Yearly revenue by a drug type.
Reprinted from RAND (2016).

[10] Weisman (n. d.) describes DDoS attacks as "one of the most powerful weapons on the Internet". DDoSing a server means flooding a server with too much traffic to make the server crash.

During January 2016, drug-related cryptomarkets (excluding sales of prescription drugs, tobacco and alcohol) generated revenues between $12.0 and $21.1 million. This number is, nonetheless, only a small fraction of the market. According to the report made by European Monitoring Centre for Drugs and Drug Addiction (henceforth EMCDDA) in 2016, "offline" market outside the Dark Web poses a bigger threat, generating $2.3 billion on average per month in Europe alone.

Cannabis, contributing roughly 37 % to the total revenue, appears to be the most sold drug amongst the other substances. The next most purchased substances are stimulants (cocaine and amphetamines; 29 %) and ecstasy-type drugs (19 %). RAND (2016) compares these numbers to the EMCDDA statement about the offline drug market. The only difference seems to be that ecstasy-type drugs create only 3 % of the total European retail drug market and heroin 28 % of the total European drug market, whereas only 6 % on the Dark Web. RAND (2016) proposes that the reason for this difference might be that online cryptomarkets may not suit the daily users of heroin, because "cryptomarkets purchases typically require an element of planning", since the majority of drugs sold online are recreational or so-called "party drugs".

Figure 12. Monthly revenues from cryptomarkets by country.
Reprinted from RAND (2016).

As Figure 12 shows, the country with the most operating vendors selling drugs online appears to be the United States, generating 35.9 % of the total drug revenues, followed by the United Kingdom (16.1 %), Australia (10.6 %), Germany (8.4 %) and the Netherlands (7.1 %).

RAND (2016), based on the research, put together a profile of vendors and buyers on the Dark Web. Both vendors and buyers are mostly young, well-educated, entrepreneurial males with strong IT skills from English-speaking or Western European countries. Vendors are usually a mix of professional drug dealers who are also closely tied to the drug production. They only consider the Dark Web to be an additional stream of revenues. Over time, shipping practices have been adjusted and single-vendor markets (websites operated by a single vendor) have emerged. Buyers select between vendors based on the prices, availability, product details, reputation of a specific vendor and feedback and recommendations from other buyers.

Terrorism, arms trade, drug deals, pornography and hacking create most of the illicit content on the Dark Web. Nonetheless, many more frightening and disturbing things can be found there. The darkest corners of the Dark Web hide various abominations, such as human trafficking, murder for hire, human experiments or live feeds of torturing, sexual abuse and murders.

6.2 Use of the Dark Web for Other Purposes

The anonymity provided by the correct use of the Tor browser and the Dark Web itself can be used in many ways and not all of them are necessarily illicit or harmful. Summers (2016, p. 7) suggests that users from countries that have suppressive laws against freedom of Internet use (or freedom of speech) might find Tor attractive.

While browsing on the surface level of the Internet, it is relatively easy to identify where the website is hosted and who runs it. This gives authorities and law enforcement ability to contact the host and ban the website if it hosts illicit or inappropriate content. Countries such as China, Syria or Iran not only monitor the Internet users' traffic, but also modify or even ban websites with a specific content. According to Harrison (2015), other countries in the west are adopting this approach to prevent privacy, hate speech, radical and extremist views and protect children.

According to Lewis (2016), the Dark Web and Tor in particular can be also used by the following groups:

- Whistleblowers[11] subject to retaliation – Strongbox, a Tor website ran by The New Yorker (American magazine), was a secure website were whistleblowers could leave their messages and other documents. Another Dark Web service called Dead Man Zero works on a basis of leaking whistleblower's information if they did not log into the site for some time. This way, secrets saved there by the whistleblower will be published in case they were jailed or murdered for the secrets they possess. One example of a whistleblower could be an ex-soldier sharing videos of a war crimes committed in the war zone.
- Victims of abuse and discriminations – On the Dark Web, sites created directly for transsexual people, rape victims, domestic violence victims or racial discrimination victims exist so individuals can share their personal stories there anonymously to help and inform other users.
- Corporations and Governments – Since the Dark Web is relatively safe place to where sensitive information can be kept with a limited access to them, company records and political intelligence can be stored there. Law enforcement uses the Dark Web to remain anonymous and to bait criminals with their own fake websites.
- Fighters for freedom – the Dark Web is used by the supporters of a freedom of speech and other activists. Individuals may express their political views and opinions anonymously with no fear. The escape from surveillance and censorship

[11] Economic Times (n. d.) describes a whistleblower as a person who exposes secret information that are illegal, unethical or wrong within a public or private organization

also helps investigative journalists and journalists in general, since they can research and publish information without being censored or monitored and they can interview other people there that want to speak up on a specific topic but wish to remain anonymous.

The Dark Web with its enormous size and great number of users with different intentions is truly a place where anything imaginable (and unimaginable) can be found, bought or sold. Although it is partly a place where people can fight for freedom of speech, express their political opinions, share their personal stories and experiences with discrimination, the dominance of illicit content and black markets is undeniable and grows in strength despite the efforts of authorities and law enforcement to stop it. As the time passes with new technologies, privacy in the future might be just a utopian fantasy. Perhaps the Dark Web might be the solution for those who want to keep their privacy. To make this happen, a new way of how to make this cyberspace safer must be found.

7 Different Paths That Lead to Cybercrime

Technology of the contemporary world has opened up a new dimension to social interactions and enables people to conceal their real-life identities to escape the punishment for embarrassing or illegal activity. Richet (2018, p. 51) observes that the fact that a "virtual presence need not to be true to the actual persona of its created in the physical world" has a great impact on the negative behavior in cyberspace especially of the young people who abuse the anonymity provided to involve in cybercrime and hacking. The number of teenagers who get involved in criminal behaviour in the cyberspace rises as an increasing number of scholars proclaim that the Internet offers different opportunities for such behaviour in comparison to the real world.

Crime or offense has its own definition, limits, forms of interaction, rules and roles in the cyberspace. "Anyone who is computer literate can become a cybercriminal" (Richet 2018, p. 52). The lack of time and space barriers, the anonymity and the inter-connection of billions of people has provided a space for new kinds of illegal activities. According to Richet (2018, p. 52), although many criminal law scholars are working to establish a legal framework, "there is still no clear definition of cybercrime" since "cybercrime" could refer to the traditional offense that was accomplished through modern technology or to a technology-related type of crime such as DDoS attacks.

Committing cybercrime has several advantages in comparison to traditional crime. Perhaps the most motivating reason could be that the psychological cost of committing crime is much lower due to the frequent difficulty of identifying the cybercrime victims. When a cyber criminal takes part in a mass scamming campaign, such as sending an overwhelming amount of emails or spreading malicious software through the Internet to obtain credit card numbers, they never have to physically interact with their victims. Richet (2018, p. 57) reports that many cyber criminals see cyber criminal behaviour as an unethical act that could help them to become successful and somehow benefit them while some do not view

it as unethical at all. Another, perhaps even more obvious, reason for cyber criminals to engage in an illegal activity is that their chances to be caught and prosecuted are much less likely in comparison to traditional crime. According to Richet (2018, p. 57), only about 5% of cybercriminals are actually caught.

Ignorance towards computer security and careless behaviour on the Internet are the weak points of cybercrime victims that cyber criminals are very well aware of. In 2004, the National Cyber Security Alliance, a non-profitable group that tries to raise public awareness of cyber security issues, stated that even though 20 % of personal computers were infected with a virus or worm and 80 % of systems were infected with a sort of spying software, users were unaware of it and they thought that they are exposed to no threat whatsoever.

Another weakness that cyber criminals take advantage of is user's fear. Richet (2018, p. 57) points out that several businesses have become victims of so-called ransomware. Ransomware is computer malicious software that instead of destroying personal data, it encrypts it. The author of the ransomware is then the only person that has the knowledge of the private decryption key that is necessary in order for the data to be released. Data are held hostage and ransom is demanded for their restoration. Businesses then often prefer to redeem the data rather then losing them. Extortion is also one of the frequent cybercrimes occurring on the Internet. Federal prosecutors and child safety experts have both agreed on the fact that the Internet is experiencing the rise in online sexual extortion, called “sextortion”. According to Richet (2018, p. 57), in 2010, an eighteen-year-old student from Wisconsin was sentenced to 15 years in prison for extortion. Prosecutors reported that Anthony Stancl pretended to be a girl to obtain nude photos of his classmates that he used to blackmail them.

8 What the Future Holds

Fifty years ago, nobody could imagine that the technology like the Internet or, for the sake of the argument, the Dark Web would exist and be available to almost anyone, anywhere and at any time. The Internet has become a reliable, fast and comfortable source of information, entertainment, new jobs, learning materials and means of communication. The Dark Web has created a space where a lot of positives can happen, such as anonymously connecting like-minded people, embracing freedom of speech and political expression or providing victims of various crimes and oppression with a space where they can preach and share their stories. However, since most of the content and services there have rather illicit nature, the question which direction is the future of the Dark Web pointing is unclear. One thing is certain, it is here to stay in one shape of form or another.

Thomas Frey, a Google's top-rated futurist speaker, wrote an article, discussing critical points that might change the Dark Web in the future. Frey (2019) suggests that the Dark Web is "destined to become far more mainstream" as well as even darker. The Dark Web websites operate in rather complicated conditions, which pushes their operators into being innovative. Just like any other market, online black markets are constantly coming up with new ways of being customer-friendly, which also includes getting more decentralized, becoming more resistant towards censorship and avoiding detection by law enforcement agencies and authorities.

Whenever security of a company is breached by hackers, the company is forced to improve its security measures. The same thing occurs when the Dark Web flaw is exposed, the website is banned or when users are deanonymized and traced down. This "global cat and mouse game" constantly pushes the protection of anonymity to higher levels. Frey (2019) goes as far as saying that in the future, we might see insurance companies offering insurance to protect the users' anonymity.

In the past, it was rather difficult to navigate through the online black markets on the Dark Web due to their poor user interface, load times, simplicity of the menu and not so clear navigation schemes. With a goal of becoming more customer-friendly and efficient, markets are improving their UI/UX (User Interface and User Experience). This way, navigating through them would not remind a user of looking for a needle in a haystack.

In Chapter 4, the two main problems with Bitcoin were discussed. The total amount of Bitcoin that can ever exist is limited due to the cryptocurrency's design, which could possibly cause a rapid increase of its price in the future once all the bitcoins are mined. Even more problems, nonetheless, could be caused by the fact that all Bitcoin transactions are made public to avoid double-spending of each token. This gives users with high IT skills a chance to find out who is behind those transactions. According to Gola (2020), cryptocurrency named Ethereum is already beating Bitcoin as the market enters February 2020. Ethereum, which is a "second-largest blockchain asset by market valuation" experienced asset increase by 51.75 % in one year with Bitcoin reaching 34.81 %.

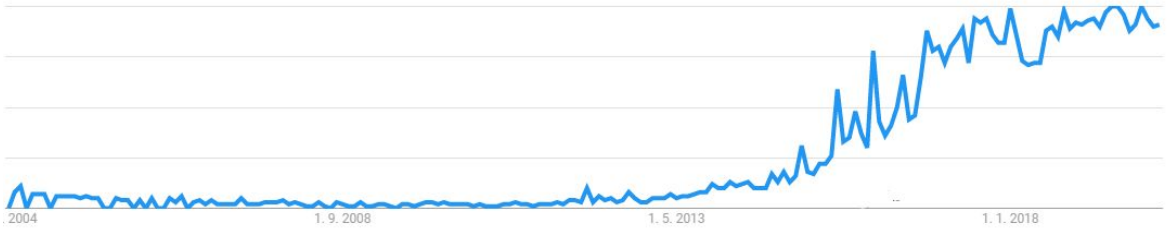

Figure 13. Term "Dark Web" searched through Google search engine over time. Print screen from Google Trends (2020).

Frey (2020) claims that the general public's interest in the Dark Web topic is dramatically increasing over time with the number of articles, TV shows and documentaries. The Figure 13 shows the increase of number of searches of a term "Dark Web" through Google search engine since 2004. The fact that more people are enthusiastically joining the world of the Dark Web might mean that the Internet users are feeling safer about the use of browsers such as Tor due to the recommendations of the other Internet users or they are starting to realize how important their privacy is.

While the number of users worldwide is increasing, the Dark Web marketplaces are expanding to meet the customer demand. When the Silkroad was banned by the FBI in 2013, roughly $1.2 billion dollars was already made by the site in transactions in twenty months' time. Frey (2020) speculates that the end of such lucrative business site inspires thousands of business-focused opportunists to create an alternative for a large number of existing consumers. This fact suggests that the Dark Web marketplaces will only grow, which could also possibly lead to the emergence of private delivery services that guarantee "untraceable, secure and anonymous delivery" (Frey, 2020).

The Dark Web appeared in 2011 with the birth of the notorious online black market Silkroad and has been the topic of public concern ever since. It has been rapidly changing and evolving for last two decades and it is still very difficult to predict its future. Data makes it clear that illicit activities happening on the Dark Web, including arms and drug trades, distribution of illegal pornography or terrorism propaganda, are here to stay. The Dark Web, nonetheless, also serves many positive purposes. It provides a space where investigative journalists can publish their work or interview people, activists can push their agenda and victims of various crimes and discrimination can share their stories. The anonymity provided by the Tor browser encourages freedom of speech and enables political discussions. We have already entered the era where the concept of privacy seems absurd. Perhaps the Tor browser (and the Dark Web itself) will become the mainstream for those who value their privacy.

Conclusion

The main goal of the thesis was to provide the Internet users with enough information about the topic so they can surf the web anonymously and prevent being hacked or robbed of their personal data. My aim was to adopt an objective approach to the issue of the Dark Web and to discuss the legal and ethical aspects of its use.

This thesis framed the concept of the Dark Web, compared different levels of the web (the Surface Web, the Deep Web and the Dark Web) and gave examples of the content that could be found in each of these levels. The Dark Web has been the part of the Internet since the beginning of the Internet itself. At that time, together with the Tor browser, it was created to serve governmental and military purposes to provide anonymous exchange of information. However, it did not take too long for this technology to be used for illegal purposes. Since the user cannot gain access to the Dark Web via web browsers such as Google Chrome, a special piece of software is required. Tor is one of the most popular Dark Web accessing tools. It provides the users with anonymity as long as they follow the rules.

The very last means to make the Dark Web what it is now are the cryptocurrencies. The thesis described the most common cryptocurrency on the Dark Web, Bitcoin. Bitcoin is a transparent, peer-to-peer, decentralized currency that makes it possible for transactions to happen anonymously. Cryptocurrencies and Tor have been united to create one of the first and most successful online illegal marketplaces ever. The Silkroad, an online black market controlled purely by market forces, where almost anything could be sold and bought anonymously, was banned by the FBI and the main administrator was caught and arrested.

Although most of the content found while navigating through the Dark Web is rather of illicit nature, it is also used for various legal and positive purposes. The thesis discussed how different users use the platform for various purposes, such as hacking and doxxing of personal information, drug dealing and trade with other illegal substances, trade with weapons, distribution of illegal child pornography, terrorists spreading their propaganda, recruiting new fighters and supporters, but also investigative journalists who wish to

publish their work and want to avoid censorship or the intervention of the government, interview guests that wish to remain anonymous, whistleblowers, fighters for freedom and supporters of the freedom of speech, activists who wish to push their agenda and people who want to anonymously engage in political discussions.

This work also provided different perspectives on what could be described as cybercrime, what motivates users to commit cybercrime, the comparison of cybercrime to traditional crime and how cyber criminals exploit weak points of their victims.

The way in which the technology and the Dark Web are used has significantly changed and keeps changing every day. The thesis, based on the data and already existing predictions, tried to predict the possible future of the Dark Web, the growth of the anonymous online markets and possibility of the Dark Web and the Tor browser becoming mainstream, since the privacy of the Internet users seems to be in danger.

List of Figures

List of References

Abdel, T. (2019). How big is the Deep Web? Retrieved from https://www.quora.com/How-big-is-the-deep-web

Awoyefa, T. (2019). What is the difference between the Dark Web and the Deep Web? Retrieved from https://www.quora.com/What-is-the-difference-between-the-dark-web-and-the-deep-web

Beal, V. (2014) What is Open Source Software? Retrieved from https://www.webopedia.com/DidYouKnow/Computer_Science/open_source.asp

Breeding, J. (n.d.). The origin and history of the Dark Web. Retrieved from https://www.ranker.com/list/history-of-the-dark-web/jordan-breeding

Bitcoin Mixer 2.0. (n.d.). Bitcoin Mixer. Retrieved from https://www.btcshaker.com/

Butler, S. (2018). Dark Web history: Where did it come from? Retrieved from https://www.technadu.com/dark-web-history/52017/

Cody, J. (2017). *Tor. Exactly how to remain invisible on the anonymous Deep Web*. Kowloon: HHB Solutions.

Deep Web Sites. (2019). Deep Web Sites 2019 | Dark Web | Deep Web Links | Hidden Wiki. Retrieved from https://www.deepweb-sites.com/

Drbola, V. (2016). *Darknet: Mýtus a realita kybernetického prostoru.* (Bakalářská diplomová práce). Brno: Masarykova Univerzita.

Dredge, S. (2014). Study claims more than 80 % of Dark Net traffic is to child abuse sites. Retrieved https://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites

Edwards, S. (2019). Terrorism recruitment on the Dark Web. Retrieved from http://www.youris.com/society/safety_and_security/terrorism-recruitment-on-the-dark-web.kl

Farivar, C., & Blankstein, A. (2019) Feds take down the world's "largest Dark Web child porn marketplace". Retrieved from

https://www.nbcnews.com/news/crime-courts/feds-take-down-world-s-largest-dark-web-child-porn-n1066511

Freenet Project. (n.d.). What is Freenet?
Retrieved from https://freenetproject.org/author/freenet-project-inc.html

Frankenfield, J. (2019). Double-spending.
Retrieved from https://www.investopedia.com/terms/d/doublespending.asp

Frey, T. (2019). Future of The Darknet: 9 critically important predictions
Retrieved from www.futuristspeaker.com/business-trends/the-future-of-the-Dark Net-9-critically-important-predictions/

FindLaw. (2019). Dark Web crimes.
Retrieved from https://criminal.findlaw.com/criminal-charges/dark-web-crimes.html

Fortney, L. (2019). Bitcoin Mining, explained.
Retrieved from https://www.investopedia.com/terms/b/bitcoin-mining.asp

Geeks for Geeks (n.d.). Onion Routing.
Retrieved from https://www.geeksforgeeks.org/onion-routing/

Gehl, R. (2018). *Weaving The Dark Web, Legitimacy on Freenet, Tor and I2P*.
Cambridge: The MIT press

Greenberg, A. (2013). Collected quotations of the Dread Pirate Roberts, founder of underground drug site Silk Road and radical libertarian.
Retrieved from https://www.forbes.com/sites/andygreenberg/2013/04/29/collected-quotations-of-the-dread-pirate-roberts-founder-of-the-drug-site-silk-road-and-radical-libertarian/#3d039d091b0c

Gola, Y. (2020). Why Ethereum is beating Bitcoin so far in 2020 and why it may continue.
Retrieved from https://www.newsbtc.com/2020/02/03/why-ethereum-is-beating-bitcoin-so-far-in-2020-and-why-it-may-continue/

Gonimah, D. (2019). What is Doxxing?
Retrieved from https://storyful.com/resources/blog/what-is-doxing/

Hale, J. (2019). Hidden web. What is the Dark Web? From drugs and guns to the Chloe Ayling kidnapping, a look inside the encrypted network.

Retrieved from https://www.thesun.co.uk/tech/2054243/dark-web-kidnap-chloe-ayling-encrypted-network-black-death/

Harrison, J. (2015). The Dark Web: Guidance for journalists. Retrieved from https://www.talkunafraid.co.uk/2015/08/the-dark-web-guidance-for-journalists/

Hussain, D. (2016). What is Tor & How to use it properly. Retrieved from https://www.ubergizmo.com/articles/tor/

Klen, A (2015). What are the pros and cons of using the Tor browser in Deep Web? Retrieved from https://www.quora.com/What-are-the-pros-and-cons-of-using-the-Tor-Browser-in-deep-web

Norton, J. (2016). *Tor and the Dark Net. Learn to avoid NSA spying and become anonymous online.* Scotts Valley: CreateSpace Independent Publishing Platform.

Ledger (2019). A brief history on Bitcoin & Cryptocurrencies Retrieved from: https://www.ledger.com/academy/crypto/a-brief-history-on-bitcoin-cryptocurrencies/

Lewis, M. (2016). What is the Dark Web – Who uses it, dangers and precautions to take. Retrieved from https://www.moneycrashers.com/dark-web/

Luke, J (2018). 7 Tips for using the Tor browser safely. Retrieved from https://www.makeuseof.com/tag/tor-browser-safety-tips/

Moore, D., & Rid, T. (2016). Cryptopolitic and the Darknet. *Survival, 58*(1), 7–38. Retrieved from https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

Nakamoto, S. (2008). Bitcoin: Peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Nikolova, M. (2019). Silk roads mastermind Ross Ulbricht challenges sentence. Retrieved from https://financefeeds.com/silk-roads-mastermind-ross-ulbricht-challenges-sentence/

Paganini, P. (2019). Hacking communities in the Deep Web.

Retrieved from https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/#gref

RAND. (n. d.). International arms trade on the Dark Web. Retrieved from https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html

RAND. (2016). The role of the Dark Web in the trade of illicit drugs. Retrieved from https://www.rand.org/pubs/research_briefs/RB9925.html

Rosic, A. (2016). What is cryptocurrency? [Everything you need to know!]. Retrieved from https://blockgeeks.com/guides/what-is-cryptocurrency/

Richet, J. (2018). *The Dark Web Breakthroughs in Research and Practice.* United States: Information Resources Management Association

Sparapani, T. (2016). The Dark Web is still a huge, difficult problem. Retrieved from https://www.forbes.com/sites/timsparapani/2016/06/28/the-dark-web-is-still-a-huge-difficult-problem/#379c662a65b1

Splitters, M. Verbruggen, S. Staalduinen, M. (2014). Towards a comprehensive insight into the thematic organization of the Tor hidden services. In Technische Universiteit Delft, *IEEE Joint Intelligence and Security Informatics Conference* (pp. 220–223). Los Alamitos: Conference Publishing Services, IEEE Computer Society.

Stacey, E. (2018). *The Dark Web Breakthroughs in Research and Practice.* United States: Information Resources Management Association

Summers, G. (2017). *Tor and the Dark Net. The lowdown on the Deep Web staying anonymous online, evading NSA spying, and organizing social revolution.* Scotts Valley: CreateSpace Independent Publishing.

Tor Project. (n.d.). The Tor project: Privacy & freedom online. Retrieved from https://www.torproject.org/

Veaux, F. (2019). Who invented the Dark Web? Retrieved from https://www.quora.com/Who-invented-the-dark-web

Weimann, G. (n. d.). Going Darker? The challenge of Dark Net terrorism. Public Policy Fellow at the Woodrow Wilson Center, Washington, DC, USA

Weisman, S. (n. d.). What is a DDoS attack?
Retrieved from
https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html
Winter, A. (2015). Joe Rogan Experience #633 – Alex Winter.
Retrieved from https://www.youtube.com/watch?v=BJMjGLcdtOA&t=213s