Dark and Deep Webs-Liberty or Abuse

Lev Topor, Bar Ilan University, Ramat Gan, Israel
https://orcid.org/0000-0002-1836-5150

ABSTRACT

While the Dark Web is the safest internet platform, it is also the most dangerous platform at the same time. While users can stay secure and almost totally anonymously, they can also be exploited by other users, hackers, cyber-criminals, and even foreign governments. The purpose of this article is to explore and discuss the tremendous benefits of anonymous networks while comparing them to the hazards and risks that are also found on those platforms. In order to open this dark portal and contribute to the discussion of cyber and politics, a comparative analysis of the dark and deep web to the commonly familiar surface web (World Wide Web) is made, aiming to find and describe both the advantages and disadvantages of the platforms.

KEYWORD

Cyber, DarkNet, Information, New Politics, Web, World Wide Web

INTRODUCTION

In June 2018, the United States Department of Justice uncovered its nationwide undercover operation in which it targeted dark web vendors. This operation resulted in 35 arrests and seizure of weapons, drugs, illegal erotica material and much more. In total, the U.S. Department of Justice seized more than 23.6$ Million.[1] In that same year, as in past years, the largest dark web platform, TOR (The Onion Router),[2] was sponsored almost exclusively by the U.S. government and other Western allies.[3] Thus, an important and even philosophical question is derived from this situation- Who is responsible for the illegal goods and cyber-crimes? Was it the criminal[s] that committed them or was it the facilitator and developer, the U.S. government?

The key advantages and disadvantages of the deep and dark web are discussed in this article with a constant comparison to the their commonly known sibling- the surface web. Moreover, this article explores the methods by which deep and dark web users can stay almost totally anonymous and secure. In contrast, these users can be maliciously exploited by hackers, money-launderers, drug dealers, human traffickers and other cyber-criminals, users can even be exploited by foreign governments and terror groups. On the one hand, these non-regulated platforms can facilitate many malicious, offensive and illegal activities. On the other, the anonymous platforms can provide anonymous and secure ways of communications for intelligence operatives but more importantly for oppressed regime oppositions and promoters of human rights in authoritarian states (Finklea, 2017; Gehl, 2016).

DOI: 10.4018/IJCWT.2019040101

As assumed and argued in this article, the deep and dark web is a double-edged sword, it enables free speech while spreading extremism. In this case, the scale and trends of the deep and dark web are worrisome. While our commonly known surface web holds tremendous amounts of web pages and data, the deep and dark webs are in fact estimated to be about 400-500 times larger than the surface world wide web (Rudesill, Caverlee & Sui, 2015). This fact raises the questions about deep and dark web activities, specifically malicious and criminal activities. If we all encounter concerning articles in our newspapers from time to time about terror cells or child pornography on the web, is that only the tip of the iceberg? Is there 400-500 times more crime and exploitation on the deep and dark web?

The simple arithmetical answer is no. The deep web is larger than the surface web, but it stores mostly private data such as personal and public undisclosed information; financial information, health documents, legal documents, governmental data assets and more. Everything not accessible to the public and password protected or restricted is in fact the deep web, even your (the reader's) bank account. However, the problem lies in another layer of the web- the dark web. The commonly used dark web (TOR) was designed by the U.S. Naval Research Laboratory to allow an anonymous and secure method of communication while avoiding monitoring, indexing and regulation. These military and intelligence benefits are exactly the social deficiencies, criminals, terrorists and other foreign states also use the anonymity and security for malicious and illegal activities. This argument is discussed throughout the article and the conclusion is derived from the combination of technical network aspects, social regulations and desirable norms.

DARK AND DEEP WEB: WHAT, WHY AND HOW

The deep web is every set of data that is not indexed or controlled in the public surface web and is not publicly accessible. The dark web is an alternative routing infrastructure that hosts web platforms and requires special software for use. Before the explanation and discussion regarding these platforms, it is important to understand when and why the internet, as we know it today, was established. The surface web internet originated from a U.S. Department of Defense project known by the name of ARPANET- Advanced Research Project Agency Network. In 1983 the ARPANET project switched from being a closed network, named Network Control Protocol (NCP) to an open one, the Transmission Control Protocol/ Internet Protocol (TCP/IP) (Hurlburt, 2015).

Effectively, this transition led to the expansion of protocols and communication types. The networks grew each month since the early beginning of the network project in the late 1960's and quickly expanded. As the number of networks and users grew, a classification of network types begun; National (Class A), Regional (Class B) and Local (Class C). Nowadays, governments and individuals can design and install their own networks (Hurlburt, 2015; Bradley & Currie, 2015). As illustrated in Figure 1 and Figure 2, early ARPANET networks designs connected only a few computers together, but these networks grew quickly. At the beginning, only a few nodes[4] (crossroads) were designed and used for the network. This design became tremendously complicated in the designs of the dark web, as described further on (Waldrop, 2008).

In 1989 the ARPANET project ended officially. However, it gave birth to the larger internet as we know it today. The public domain internet quickly expanded. In order to simplify the networks designs to the public the Internet Corporation for Assigned Names and Numbers (ICANN) begun designing the internet to be more accessible to the public. Just like looking in the Yellow Pages, sorting and finding whom one wants to call, ICANN assigned names, IPs and DNSs (Domain Name System) to a wide spread of computers in every government, industry, home, and now even to our mobile devices (Ciancaglini, Balduzzi, McArdle & Rösler, 2015). Thus, ICANN websites can be found easily; Instead of typing an IP address (192.0.32.7, ICANN), people can simply type "icann.org".[5] ICANN begun indexing almost every registered service, inviting big tech giants such as Alphabet's Google search engine[6] and others such as Bing, Yahoo, AOL, Yandex.ru and much more to sort, index and manipulate all of the registered DNSs and IPs.

Figure 1. ARPANET map design, December 1967

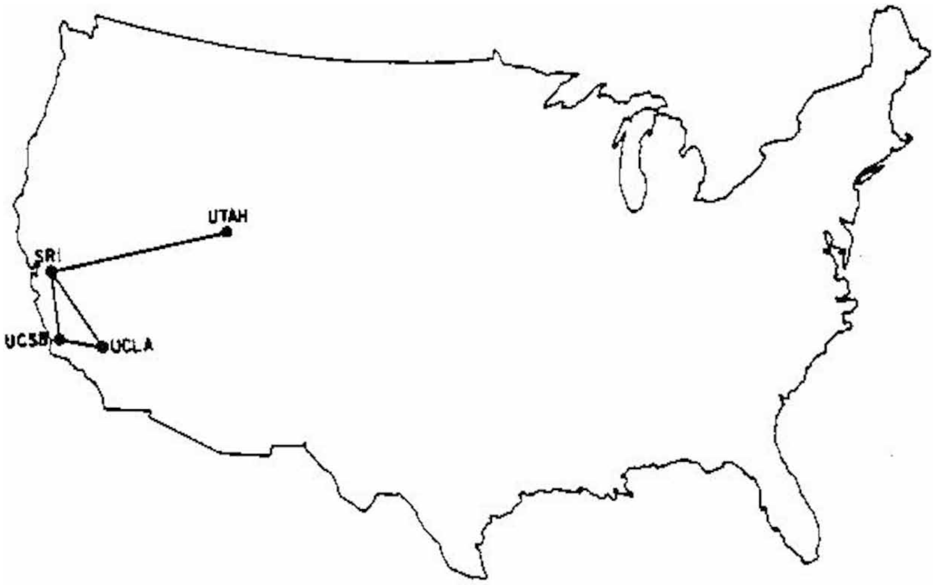
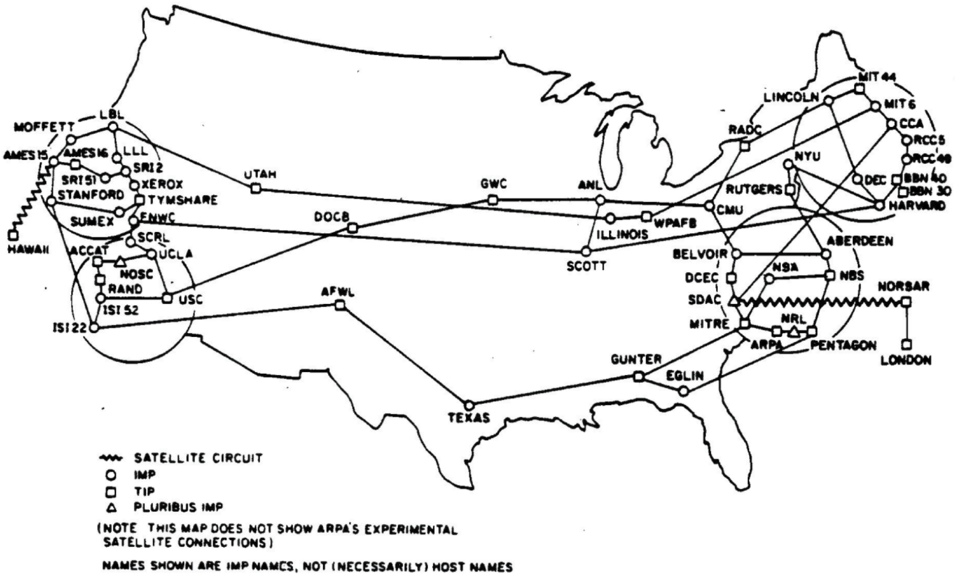


Figure 2. ARPANET logical map design, July 1977



The indexing process raises some significant questions and concerns. First, who gets to be on top of the index list, and why. Manipulation of the indexing process can be an effective political method to dominate the web. Second, if every address is indexed, it can be monitored by the government, commercial players and even malicious players. Effectively, this situation causes a biased web that can be manipulated to prevent free speech or spread of significant news, events and knowledge. Moreover, different states have different access to the web. For example, in 2018 China blocked the Australian Broadcast Corp sites in an attempt to stop the spread of certain coverages of events. An official at the Office of the Central Cyberspace Affairs Commission noted:

However, state cyber sovereignty rights shall be maintained towards some overseas websites violating China's laws and regulations, spreading rumours, pornographic information, gambling, violent terrorism and some other illegal harmful information which will endanger state security and damage national pride. (BBC, 2018)

Denying access to the internet is a violation of basic human rights. Moreover, oppressive countries use geo-located IP addresses to silence opposition simply by tracing it and arresting the ones involved (Vogt, 2017; Russon, 2017; Baharain Watch, 2013). Thus, in Michel Foucault's view, the hegemonic U.S. based Arpanet, internet and indexing systems, or the authoritarian North Korean or even Chinese internet manipulation systems can cause the exclusion of the weaker, un-indexed, or blocked, players. Hence the importance and popularity of the dark web (Foucault, 2003).

As was explained earlier in this article, networks can be national, wide and large and they can be narrow and small. While the small-scale surface web networks are quite wide, the large-scale deep web networks can be quite narrow. The deep web is everything that is not indexed by search engines and national and international regulators. The deep web mostly consists of dynamic web pages generated by requests, blocked sites that use authentication methods, unlinked sites which prevent an effective indexing process, Non-Scriptural or contextual content (Everything that is not based on HTML, HyperText Markup Language), limited access networks which are placed in non-public infrastructures, private web platforms which require a password or a payment for access. For example, our private bank account data or health information is access restricted. Most police and military networks are also restricted and even not connected to the public web systems because of information leak fear. Moreover, many large military bases have their own networks and protocols and act as an internal internet system (Hurlburt, 2015).

It is important to understand the role of search engines when comparing the deep web and the surface web. Currently, search engines systematically exclude, either by design or by accident, certain sites in favor of others. Nations and technology providers can manipulate and control the web. For instance, when they refuse to index a site or when they rank a certain site lower than another, so the lower ranked site is harder to find. Free speech is prevented by restricting access or manipulating the index process. Certain groups of people, legitimate or not, intentionally turn to the deep and dark web to avoid this kind of political bias (Introna & Nissenbaum, 2000; Hargittai, 2007).

Within the deep web lays the dark web. A dark web is part of the deep web but can only be accessed using a special software since it is based on a unique infrastructure. Dark webs and other alternative routing infrastructures are hosted on platforms that require a special software to reach them, such as a TOR browser. There are more dark web infrastructures such as the Freenet protocols, I2P, Riffle and more alternative domain roots (Hurlburt, 2015). Moreover, military and intelligence agencies can establish and maintain their own deep and dark webs. In order to access the dark web, one has to know the address, the content and the password (If there is any) so even terror groups use these platforms to communicate securely to plan and conspire terror attacks and acts (Weimann, 2016). Thus, while western nations use dark webs to influence on oppressive regimes and fight terrorists, the latter is acting in the same way, but with a different aim- terror.

The most commonly used dark web infrastructure is TOR. It was developed and designed by the U.S. Naval Research Laboratory and was introduced in 2002. Its aim was to allow military and governmental private and secure communication worldwide. TOR allows an anonymous method of communication between users (clients and servers) by using volunteer nodes. All routing is encrypted and while some nodes can be exposed, it is very difficult to retrieve all the access points and nodes from server to client. Effectively, if one were to enter a special address, the last node accessing this address could be found, even by a local ISP (Internet Service Provider) but not the original user. Unknown is un-indexed and search engines and governments can do very little to sort the dark web. Moreover, the TOR network uses a unique top-level[7] .onion domain names that are not accessible by regular surface web browsers. I2P sites also use a unique top-level domain; .i2p (Ciancaglini, Balduzzi, McArdle & Rösler, 2015; Jardine, 2015).

In most cases, network traffic analysis can detect these sorts of connections but not reach their content nor their end-users- the true server or client. This detection problem had to be overcome since U.S. agents and data sets would have been discovered by a simple deprivation methodology— every transaction of data that other governments can see is categorized as innocent and everything these governments cannot see, or reach, is foreign activity. The solution was quite simple. The U.S. flooded the TOR network and other dark webs so that their intelligence activities would not be discovered. Besides Western strategic goals, these dark webs also allow regime opposition in authoritarian states to contact the outside world without being monitored by the domestic intelligence services, thus, promoting human rights and freedom. Simultaneously, the wide spread proliferation of these platforms caused cyber-crime to spread (Ciancaglini, Balduzzi, McArdle & Rösler, 2015; Jardine, 2015).

Is the Dark Web Really That Anonymous?

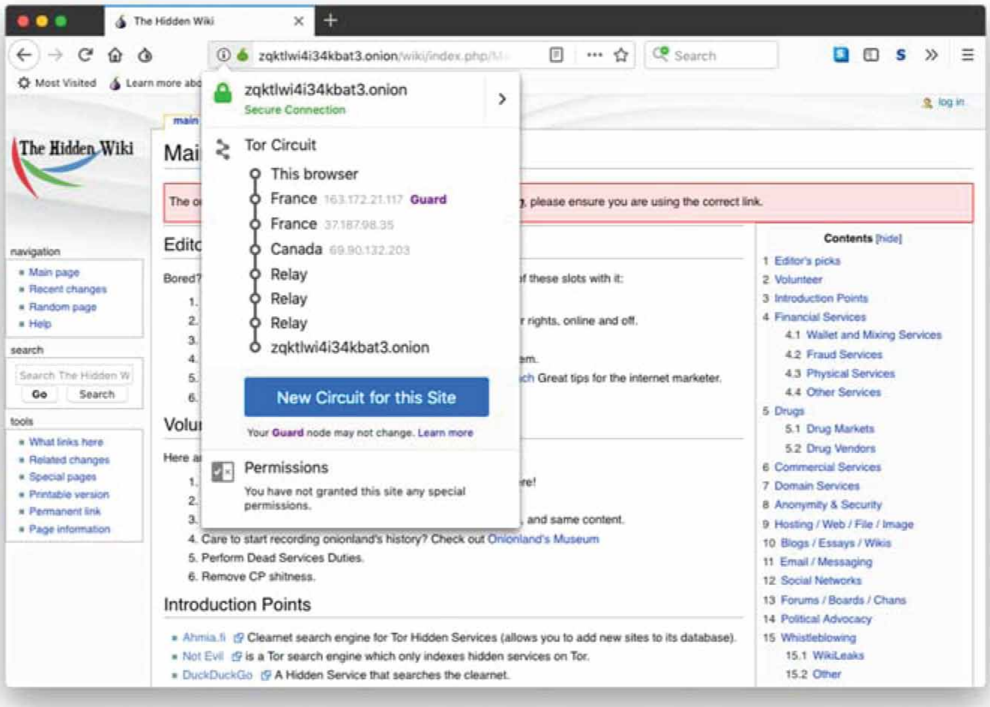
The dark web hosts vast amounts of illegal and malicious activities. Law enforcement worldwide are always looking into new methods to index and investigate the dark web. When entering the TOR browser, a set of proxies, nodes and relays are used to hide one's location and identity (See Figure 3). Data retrieving protocols are always disabled and blocked, such as the use of JavaScript, HTML 5 media, images, icons, symbols and much more. There protocols are blocked in order to protect one's cyber identity. For instance, location services, JavaScript or responsive website graphics can identify one's screen size, the Operation System (For instance whether it is a Windows based machine, a Mac or a Linux machine, etc.). Even one's private computer name can be discovered. Thus, allowing either law enforcement of malicious actors to locate and pinpoint the end-user.

This data can be extremely critical. For instance, if a malicious player wants to target wealthy victims, all he has to do is to design a fake web activity (Such as phishing sites and autonomous web scripts) that will sort all types of computer screens, processes and even location. Thus, he can than focus on users with high-end expensive computers, that live in wealth neighbourhoods. Interestingly, it can all be done without even breaking the law and hacking into somebody else's computer. Figure 3 presents a screenshot of the TOR browser and assigned route. A website user in the United States can pass through various nodes and relays all over the world before reaching his destination, making his location extremely difficult.

One way of surveillance is using exploited nodes or just distributing ones. Government-made nodes can be spread, thus, tracking users and their web routes to their real identity. For instance, if one enters a website through a short route, a local ISP can detect his first directions and nodes, the website this user visits also can detect the last node that requested access. Assuming this user used a government made node, law enforcement can then tract both the request for the use of their node and the next request for the destination. Thus, governments can retrieve data from website hosts, local ISPs and use their own nodes to complete the route-puzzle, allowing law enforcement to track a user. Another way of surveillance and dark web users' detection is to constantly monitor hidden services, map them (Though most illegal activists change their domains and designs constantly), and index information semi-manually in order to keep track of overlapping information (Chen, Chung, Qin, Reid, Sageman & Weimann, 2008; Ciancaglini, Balduzzi, McArdle & Rösler, 2015; Jardine, 2015).

Other methods of surveillance and detection are the use of Artificial Intelligence (AI) and autonomous web scripts to retrieve data. A good example is DARPA's AI software MEMEX (Combination of 'memory' and 'index'). Instead of using pre-programmed and predesigned software as most of the search engines do, MEMEX uses AI to explore and sort these places like a human analyst (Fox-Brewster, 2015). Another way to monitor the dark web is based on geo-locating large number of users (Crowds) who use the dark web. This method allows the analysis and the comparison of populations in certain locations with regular web activities, but it is harder to locate specific users and information this way (Morgia, Mei, Raponi & Stefa, 2018). There are more monitoring and

Figure 3. A route of nodes and relays in the TOR browser



zqktlwi4i34kbat3.onion
Secure Connection

Tor Circuit

- This browser
- France 163.172.21.117 Guard
- France 37.187.98.35
- Canada 69.90.132.203
- Relay
- Relay
- Relay
- zqktlwi4i34kbat3.onion

New Circuit for this Site

Your Guard node may not change. Learn more

Permissions

You have not granted this site any special permissions.

Mai

The o ... , please ensure you are using the correct link.

Edito

Bored? ... f these slots with it:

1\.
2. ... r rights, online and off.
3\.
4. ... em.
5. ... ch Great tips for the internet marketer.
6\.

Volu

Here a

1. ... re!
2\.
3. ... , and same content.
4. Care to start recording onionland's history? Check out Onionland's Museum
5. Perform Dead Services Duties.
6. Remove CP shitness.

Introduction Points

- Ahmia.fi Clearnet search engine for Tor Hidden Services (allows you to add new sites to its database).
- Not Evil is a Tor search engine which only indexes hidden services on Tor.
- DuckDuckGo A Hidden Service that searches the clearnet.

Contents [hide]

1 Editor's picks
2 Volunteer
3 Introduction Points
4 Financial Services
4.1 Wallet and Mixing Services
4.2 Fraud Services
4.3 Physical Services
4.4 Other Services
5 Drugs
5.1 Drug Markets
5.2 Drug Vendors
6 Commercial Services
7 Domain Services
8 Anonymity & Security
9 Hosting / Web / File / Image
10 Blogs / Essays / Wikis
11 Email / Messaging
12 Social Networks
13 Forums / Boards / Chans
14 Political Advocacy
15 Whistleblowing
15.1 WikiLeaks
15.2 Other

mapping methods available mostly to state security services such as phishing methods, impersonation, frequency sweeping and screening and others. These methods and others are not discussed in this article in order to keep them under confidential and affective.

EMPIRICAL DISCUSSION: LIBERTY OR ABUSE

In this section, the question whether the dark web promotes liberty or promotes abuse is discussed. Moreover, the discussion is accompanied with empirical up-to-date examples of dark web activities. As argued in the beginning of the article, the dark web can be a double-edged sword. Assuming that freedom of expression, freedom of press, and the general access to knowledge are all part of a normative set of human rights, the initial deep and dark web development by the U.S. has been a significant act of promotion of human rights (UN, 1948). Moreover, in a 2015 report by the Human Rights Watch organization TOR and the general use of privacy and anonymity tools were endorsed. As China, Russia, Turkey, Ethiopia and other countries tried to interfere with TOR services in order to keep track of the population trends (Human Rights Watch, 2015). It is worth mentioning that Edward Snowden's leaks in 2013 had a major impact on the dark webs popularity and TOR's usage had tremendously increased since the Snowden affair (Hampson & Jardine, 2017, pp. 81-90).

The dark web is very similar to the regular surface web. It hosts websites such as social media sites, blogs, forums, boards, market places and secure chats. Assuming an oppressed and politically persecuted person can install dark web browsers or proxies such as TOR or I2P, or presumably an anonymous and amnesiac operating system such as TAILS[8], he can then publish insights and information to others. This publication and expression can be done by running a hidden blog, sending a dark web email, posting on social media platforms, providing information in online chats and even leaking information in platforms such as WikiLeaks or SecureDrop.[9] A significant example is the 'We Fight Censorship' (WeFC) project which is promoted by Reporters Without Borders organization. This service is designated to publish content that has been censored, banned or has led to reprisals against its creator. The WeFC project serves as a critical information access tool, allowing oppressed populations to find out about events which their governments are trying to keep confidential. For instance, censored and forbidden content is presented on the WeFC dark web site, mainly regarding Iran, China, Syria, Jordan, Turkey, Venezuela and a few other countries.[10]

An important example is that WeFC discovered and published in its dark web site that the Jordanian government had blocked 291 news websites in 2013, following a royal decree from September 2012. The Jordanian government requested its local ISPs to block the sites. First, DNS blocking was preformed, blocking all assigned domains for the unwanted sites. Afterwards, it is believed that a rigid method of blocking was used- IP blocking. Effectively, Jordanian citizens could not enter blocked sites when typing their domain address. Further, these sites were blocked even when Jordanian citizens typed the sites' exact IP address.[11] Thus, Jordanian citizens that wanted to gain access to the blocked content could have used Virtual Private Networks (VPNs)[12] or use the TOR browser to overpass the governmental restriction.

Another example of dark web utilization for the promotion of human rights is the Russian dark web site *РосПравосудие* ('RusJustice') which claims to host more than 50 million juristic documents and some private information on Russian prosecutors, judges and lawyers.[13] As claimed in this dark web site, it is a non-political site that aims to disclose all legal aspects regarding Russian law. Thus, Russian civilian justice promoters can host legal documents, specifically those regarding controversial political and legal cases, review them and act to seek justice. Private and anonymous boards over the dark web are another good way to express opinions and share information without the fear of persecution. For instance, on 8chan one can write freely; An anonymous user wrote about the Pakistani-Indian recent conflict, numbered the death tolls, described weapons used and analysed some strategic goals of both sides. Moreover, Pakistani and Indian citizens then shared information that at least some of it was censored.[14] This information exchange is not unusual and happens on the surface web all the time, however, it is private and anonymous and cannot be censored easily by a local governmental decree.

In contrast to the examples above and to the fact that the dark web can be utilized to promote human rights and the freedom of information, it can also be exploited by malicious users to promote terror, hate and other negative and illegal acts and goods. As mentioned in the introduction of this article, the U.S. Department of Justice had published and uncovered its nationwide covert operation in which vendors from the dark web were targeted and arrested. The operation resulted in 35 arrests and seizure of weapons, drugs and other illegal material. The Department of Justice also foreclosed 23.6$ Million. The most known dark web market place was the Silk Road marketplace. Though versions and attempts of recreation still exist, the original dark web site was founded in 2011 and sold over 200$ Million worth of drugs and other illegal material. The founder of the Silk Road marketplace, Ross William Ulbricht, was arrested by the Federal Bureau of Investigation (FBI) in October 2013 in a San Francisco public library. Ulbricht was charged in computer hacking, narcotics trafficking and money laundering (Hume, 2013). Ulbricht was convicted in February 2015 in the state of New York under the charges of conspiracy to commit drug trafficking, money laundering and computer hacking (BBC, 2015).

Once inside the dark web's most commonly known repository of links, *The Hidden Wiki*, one can find a large number of sites that offer all sorts of illegal material; Stolen and cloned credit cards, bank accounts, PayPal accounts, drugs, weapons, stolen or fake identification cards and passports, illegal pornography and even hacking services or hired assassins.[15] Most drug, weapons, pornography and even assassination vendors require that payments would be made using cryptocurrency such as bitcoins. Though there are a lot of vendors, some of them scam and exploit customers. They trick them into paying for products or services but do not deliver them. Though hired assassins do exist, one would probably encounter an undercover law enforcement agent, looking to stop potential future murders by arresting those who are trying to hire those assassins. For example, a 58-year-old woman was arrested in Denmark in March 2017 and was later sentenced to six years in prison for an attempt to arrange the murder of her boyfriend (Fox News, 2017).

Apart from selling and buying illegal material or services, racist hate groups also flourish on the unregulated deep and dark webs. Mainly, neo-Nazi bloggers, activists or organized groups find shelter in the dark web if hate-speeches and incitements are illegal in their home countries. A well-known example is the case of the Charlottesville rallies in recent years. The rallies are titled 'Unit the Right' but a site named the *Daily Stormer* organizes them. In August 2017, Heather Heyer, 32, was killed when a white supremacist drove a car into a demonstration against the alt-right 'Unit the Right' (Katz & Stockman, 2018). After the incident, the Google and GoDaddy companies refused to service the neo-Nazi site and the *Daily Stormer* found shelter in the dark web. The site managers started serving a site on the dark web[16]. A few month later, when they found a way to get back to the regular surface web, they issued a statement that if their site is taken off, supporters should go to their dark web site (Robertson, 2017).

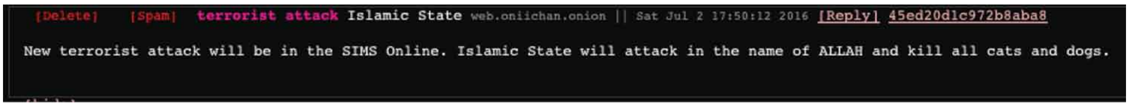
Terrorist are also making use of the anonymous and private infrastructures. Terrorists and other extremists find shelter on the dark web to plot attacks, raise funds, recruit new followers and spread their propaganda. They hide from the intelligence agencies which are constantly trying to find them and act against them. While terrorists can plot attacks in private meetings or with their own coded language, it has become harder for them to act. For this reason, they often seek shelter in the dark web where they can communicate securely and privately. Moreover, even if the intelligence agencies do encounter their conversations, it will be more difficult to locate these terrorists. These extremists also use cryptocurrencies to avoid surveillance on their bank accounts. Many wealthy supporters of terror make bitcoin donations to terror groups since it is nearly impossible to trace these transactions. Extreme propaganda is also used in the dark web. As was mentioned in this section, incitement is illegal in most Western countries and those who do want to incite do it securely and anonymously (Weimann, 2016; Malik, 2018).

As can be seen in the figure below (Figure 4), an anonymous message was put in a dark web board, stating that an attack is likely to come in the name of Allah. As was analysed in the board by other users, "SIMS" means a city, "online" means a metropolitan or a modern city, "cats and dogs" means Jews and Christians, which means this attack is intended to take place in a non-Muslim country.[17]

Countries also use the dark web to spread their own mis-information, leak information that they do not want to publish in conventional and formal ways of communication. They also buy and sell all kind of material for their own benefits. For instance, a former senior official from one of the British intelligence agencies had told me that the British government made several purchases on the dark web; They tried to buy stolen passports and identification cards and even stolen credit and debit cards in order to make untraceable purchases in their future clandestine operations. Moreover, the official admitted that the 'all-mighty' intelligence agencies fell for several scams and that the British tax-payers lost several bitcoins on the dark web. As for law-enforcement, the senior official noted that agencies frequently upload dummy guides and files about homemade drugs or even bombs and firearms- the dummy files are infected with malware and spyware to track the ones who looked for these guides.[18]

Law-enforcement agencies play a curtail role in the eradication of cyber-crime, both on the dark web and on the regular surface web. While it is difficult to track dark web users, honey traps and psychological pressure can do what technology still cannot; undercover police officers frequently impersonate themselves as young children and wait for potential pedophiles to make contact, an adapted technique which was initially used by intelligence agencies worldwide to seduce their target with genuine bonds of affection in order to get a hold on the targets information (Tickle, 2012; Mijalković, 2014). As for the use of psychological pressure, in 2014 the FBI tricked a child abuser into playing

Figure 4. An anonymous terror threat on the CHANGOLIA board in July, 2016



[Delete] [Spam] terrorist attack Islamic State web.oniichan.onion || Sat Jul 2 17:50:12 2016 [Reply] 45ed20d1c972b8aba8

New terrorist attack will be in the SIMS Online. Islamic State will attack in the name of ALLAH and kill all cats and dogs.

what was presented to be a child pornography video. Once the video loaded up, it automatically opened another network connection which was monitored by the FBI and the true IP address of the one who tried to watch the video was captured and recorded (Sulleyman, 2017).

ANALYSIS AND RECOMMENDATIONS

There are a few methods and patterns which derive from the empirical examples of the last section. Interestingly, promoters of human rights, governments, extremists and criminals all utilize the deep and dark web in a similar way for their own benefits. Initially, a necessity must be required for the utilization of anonymous and more secure communications otherwise users would not need anonymity. The main reason for the use of dark webs is restriction and illegality. While it is easy to understand the reason drug dealers or terrorists use dark webs- they want to avoid legal persecution, it is more complicated to understand why intelligence operatives, regime opposers and human rights promoters use dark webs. Intelligence operatives and regime opposers also act in illegal ways; They break the law of the authoritarian and oppressive regimes, endangering themselves in order to share important information. Moreover, laws and penalties against espionage and even against regime opposition are far stricter than laws and penalties against drug dealing or money laundering in many countries. Promoters of human rights also break the domestic law while trying to expose human rights violations.

As noted, all the mentioned above use the dark web in order to leak sensitive information, gain sensitive information, make financial transactions, gain the opportunity to speak freely as well as combine dark web publications with a larger disinformation operation. A method used by intelligence agencies, law enforcement, regime opposers and criminals alike is nicknamed a “Honey Trap”. This method can be divided into two sub-methods. First, honey traps are used to lure and trap a user into a relationship with a human operative or with an IT network such as a trusted blog or a site. Once the user is lured, the ones behind the honey trap can gain sensitive information from that user and even hold it against him later on. This method is similar to the “Sex Espionage” methods of some of the intelligence agencies where a woman or a man would lure someone with sensitive information and create genuine bonds of affection to build up trust (Mijalković, 2014). Intelligence operatives or law enforcement officers can utilize the dark web in order to attract people who want to leak information. Once they establish a relationship with them, even present themselves as journalists looking for leaks, they can mine information which eventually can be used to track down those leakers. Thus, making the anonymity and security of the technological infrastructures useless. Many dark web money launders or drug dealers lure those who seek to buy drugs in order to benefit from people’s addictions or lusts.

The second sub-method is an infrastructural variation of the classical honey traps. It is known within the intelligence communities as “Honey Nets”. A honey net is an inviting infrastructure which lures users who seek to act in illegal ways. For example, intelligence agencies often create sites, blogs, email systems, social networks in order to gain access to the ones who sign-in (Yasinsac & Manzano, 2002). A law enforcement agency could publish a drug selling site on the dark web, making it look anonymous and private. Once drug dealers and consumers sign-in, the law enforcement agency can start gathering information about nicknames, emails, transactions, patterns, ways of distribution and will eventually gain enough information to track down and arrest those involved. The same example is also valid with the example of terror activists. The dark web honey nets are used to lure users which seek to break the law and then to gather forensic data. Even your local ISP or your popular social network can be described as a honey net since it gathers all the information above, which eventually can be used for persecution but in most innocent cases this data is used for marketing leads. As mentioned in the empirical discussion, one would probably encounter an undercover law enforcement agent while looking for hired assassins on the dark web sites which claim to provide these services. This honeynet method is also valid for the regular surface web. Moreover, a theoretical, but worrisome question must be asked after this paragraph; What if the email providers which promise rigorous security such as

Proton Mail[19] are actually espionage infrastructures aimed to build up trust and invite users to send sensitive and private information, which can later be used against them.

Another example of a honey net is the creation of a private deep web network which can be easily manipulated and accessed by others such as intelligence agencies or criminal cyber-hacker but at the same time has the ability to collect data about the attacks. Once this network is attacked and access is illegally gained, those who established the network can learn about the attackers and eventually track them and arrest them. A good example of this kind of a honey net occurred in London in recent years, according to the former senior official from the British intelligence which was mentioned earlier. An undisclosed embassy, located in the famous 'embassy avenue' in Kensington Palace Gardens, suffered an attack by a foreign intelligence team which was from a country hostile to the mentioned embassy's origin country. The embassy had prior information about this kind attack. Thus, it established a Wi-Fi and an internal network which could be hacked easily but were also monitored, physically and technologically. Eventually, the embassy found out who was behind the attack and how they executed it.

As presented above, intelligence operatives, regime opposers and human rights promoters as well as criminals and terrorists use honey traps and psychological pressure to overcome the anonymous and private characterizes of the dark web. In addition, they also utilize the dark web, which appears to be private and secure for most users, for disinformation and propaganda operations. Intelligence agencies can publish anonymous posts and information leaks which might appear legitimate, thus, providing other users and other enemy intelligence agencies with disinformation. Further, they can share information which cannot be published with an official national affiliation with journalists which then publish it (After a strict verification in most cases). For example, some of the military air strikes on terror operatives or illegal weapons distributions in Syria during the recent years were made by Israel, which did not take responsibility for those actions in most cases. Some strikes were even made by American, British and French forces. While official national affiliation to those strikes could be problematic, leaks on the dark web and even direct leaks to some journalist can solve this issue, thus, making the dark web a perfect infrastructure for leaks (Hubbard & Halbfinger, 2018).

The analysis above yields some important recommendations for law enforcement and counter intelligence agencies worldwide. In order to track down a terrorist or a pedophile, psychological pressure of desire or lust must be achieved; The terrorist may want to broaden his terror cell or collect funds while the pedophile might lust for certain videos or pictures. The dark web can provide them with high anonymity and privacy, even security, but once they lust to get a hold on something, it can be utilized against them. The FBI video trick mentioned in the end of the empirical discussion strongly proves this insight. Taking one step further, law enforcement agencies can establish whole sites or social networks in order to attract criminal users to their honey nets. Once the criminal users sign-in, provide financial and distributary information, forensic methods can be utilized to gather information and track those criminals down, eventually causing the eradication of crime and terror. The same concepts of conduct apply for intelligence and counter intelligence agencies worldwide. As mentioned earlier, the U.S. flooded the TOR network and other dark webs so that their intelligence activities would not be discovered. Now, law enforcement and intelligence agencies hold the means to flood the dark web with honey traps and honey nets which will eventually attract terrorists and criminals to seek illegal products and services. Once they are trapped inside the honey traps, information can be collected so that the terrorists and criminals would be eventually captures and persecuted.

CONCLUSION

This article dealt with the characteristics of the deep and dark web; whether these anonymous and private platforms benefit liberty and human rights or are these platforms actually abused and used for the spreading of terror, hate and exploitation. As was argued throughout this article, the dark web can provide anonymous and secure ways of communications for oppressed regime opposers and promoters of human rights in authoritarian states as well as law enforcement and intelligence agencies worldwide. In contrast, these non-regulated platforms can facilitate many malicious, offensive and illegal activities such as terror, drug and weapons, human trafficking, illegal pornography and other sorts of criminal activities. Effectively, the dark web is a double-edged sword- it enables liberty and freedom while spreading extremism.

Moreover, the fact that the U.S. developed the dark web platforms for its own use and then made it public, and that it is also TOR's largest donator, makes this discussion even more problematic; For instance, who is responsible for the spread of hate, drugs and terror? The criminals and terrorists or the U.S. government and military? One can argue that extremists would have acted the same in a world without these anonymous and private platforms. This argument is also valid for regime oppositions and promoters of human rights. Opposers from North Korea or Iran would have found other ways to oppose their authoritarian regimes. Both arguments are correct and valid in a way, deep and dark webs allow these groups to maximize their efficiency and effectiveness.

However, there is a way to resolve this problematic argument. In fact, one does outweigh the other; While extremists and terrorists do maximize their efficiency with the deep and dark web as well, the actors who are promoting [Western and liberal] human rights also use the deep and dark web to fight extremists, terror and other illegalities. Law enforcement and intelligence agencies use honey traps and psychological pressure to overcome the anonymous and private characterizes of the dark web, making the technological benefits almost useless. As were recommended, law enforcement and intelligence agencies should flood the dark web with honey traps and honey nets in order to attract and reveal criminal users. Thus, the benefits of the deep and dark webs outweigh their shortcomings. The creation, promotion and utilization of these anonymous and secure methods of communication are far too important to be disregarded because of some flaws or misuse. In addition, the empirical examples of this research shed light on the methods by which human rights promoters, extremists and governments make use of. The anonymous platforms are almost identical to the regular surface web and they host similar types of sites- the key differences are in anonymity, security and privacy.

REFERENCES

Baharain Watch Members. (2013). The IP Spy Files- How Bahrain's Government Silences Anonymous Online Dissent. *Bahrain Watch*. Retrieved from https://bahrainwatch.org/ipspy/viewreport.php

BBC. (2015, May 30). Silk Road drug website founder Ross Ulbricht jailed. Retrieved from https://www.bbc.com/news/world-us-canada-32941060

BBC. (2018, September 3). China blocks access to Australian Broadcasting Corp sites. Retrieved from https://www.bbc.com/news/world-australia-45392570

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the Dark Web: A Case Study of Jihad on the Web. *Journal of the American Society for Information Science and Technology*, *59*(8), 1347–1359. doi:10.1002/asi.20838

Ciancaglini, V., Balduzzi, M., McArdle, R., & Rösler, M. (2015). *The Deep Web*. Trend Micro. Retrieved from http://www.trendmicro.nl/media/wp/below-the-surface-whitepaper-en.pdf

Fidler, B., & Currie, M. (2015). The Production and Interpretation of ARPANET Maps. *IEEE Annals of the History of Computing*, *37*(1), 44–55. doi:10.1109/MAHC.2015.16

Finklea, K. M. (2017). *Dark web*. Congressional Research Service.

Foucault, M. (2003). *Society Must Be Defended": Lectures at the Collège de France, 1975-1976* (D. Macey, Trans.) (pp. 43–62). New York: Picador.

Fox-Brewster, T. (2015, April 10). Memex In Action: Watch DARPA Artificial Intelligence Search for Crime on the 'Dark Web.' *Forbes*. Retrieved from https://www.forbes.com/sites/thomasbrewster/2015/04/10/darpa-memex-search-going-open-source-check-it-out/

Fox News. (2017, December 17). Woman Who Paid Hit Man in Bitcoin Gets 6 Years in Prison. Retrieved from https://www.foxnews.com/world/woman-who-paid-hit-man-in-bitcoin-gets-6-years-in-prison

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, *18*(7), 1219–1235. doi:10.1177/1461444814554900

Hampson, F. O., & Jardine, E. (2017). *Look Who's Watching: Surveillance, Treachery and Trust Online*. McGill-Queen's Press-MQUP.

Hargittai, E. (2007). The Social, Political, Economic, and Cultural Dimensions of Search Engines: An introduction. *Journal of Computer-Mediated Communication*, *12*(3), 769–777. doi:10.1111/j.1083-6101.2007.00349.x

Hubbard, B., & Halbfinger, D. M. (2018, April 9). Iran-Israel Conflict Escalates in Shadow of Syrian Civil War. *The New York Times*. Retrieved from https://www.nytimes.com/2018/04/09/world/middleeast/syria-russia-israel-air-base.html

Human Rights Watch. (February 2015). On the Use of Encryption and Anonymity in Digital Communications. In *Comments Submitted to the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression*. Retrieved from https://www.hrw.org/sites/default/files/related_material/EncryptionandAnonymity_Feb1015.pdf

Hume, T. (2013, October 5). How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road. *CNN*. Retrieved from https://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html

Hurlburt, G. F. (2017). Shining Light on the Dark Web. *IEEE Computer*, *50*(4), 100–105. doi:10.1109/MC.2017.110

Introna, L. D., & Nissenbaum, H. (2000). Shaping the Web: Why the Politics of Search Engines Matters. *The Information Society*, *16*(3), 169–185. doi:10.1080/01972240050133634

Jardine, E. (2015). *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Global Commission on Internet Governance and Chatham House. Retrieved from https://www.cigionline.org/sites/default/files/no.21_1.pdf/

Katz, J. M., & Stockman, F. (2018, December 7). James Fields Guilty of First-Degree Murder in Death of Heather Heyer. *The New York Times*. Retrieved from https://www.nytimes.com/2018/12/07/us/james-fields-trial-charlottesville-verdict.html

La Morgia, M., Mei, A., Raponi, S., & Stefa, J. (2018, July). Time-Zone Geolocation of Crowds in the Dark Web. In *Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems* (pp. 445-455). IEEE. doi:10.1109/ICDCS.2018.00051

Malik, N. (2018). *Terror in the Dark- How Terrorists Use Encryption, the Darknet, and Cryptocurrencies*. Centre for the Response to Radicalization and Terrorism. Retrieved from http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

Mijalković, S. (2014). ‘Sex-espionage’ as a method of intelligence and security agencies. *Bezbednost, Beograd*, *56*(1), 5–22. doi:10.5937/bezbednost1401005M

Robertson, A. (2017, August 15). Neo-Nazi site Moves to Dark Web After GoDaddy and Google Bans. *The Verge*. Retrieved from https://www.theverge.com/2017/8/15/16150668/daily-stormer-alt-right-dark-web-site-godaddy-google-ban/

Rudesill, D. S., Caverlee, J., & Sui, D. (2015). *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*. Woodrow Wilson International Centre for Scholars. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676615

Russon, M. A. (2017, April 21). Won't let your citizens access the internet? Fine, no more IP addresses for you. *International Business Times*. Retrieved from https://www.ibtimes.co.uk/wont-let-your-citizens-access-internet-fine-no-more-ip-addresses-you-1618040/

Sulleyman, A. (2017, May 5). Paedophile Caught After Police Video Trick Lures Him Out of Dark. *Independent*. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/paedophile-website-19-roy-harvender-jr-dark-web-police-video-trick-ip-address-delaware-new-castle-a7719976.html

Tickle, L. (2012, August 22). How police investigators are catching paedophiles online. *The Guardian*. Retrieved from https://www.theguardian.com/social-care-network/2012/aug/22/police-investigators-catching-paedophiles-online

United Nations. (1948). The Universal Declaration of Human Rights. Retrieved from http://www.un.org/en/universal-declaration-human-rights/

Vogt, S. D. (2017). The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. *Santa Clara Journal of International Law*, *15*, 104–125.

Waldrop, M. (2008). *DARPA and the Internet Revolution: 50 Years of Bridging the Gap*. Defense Advanced Research Projects Agency. Retrieved from https://www.darpa.mil/attachments/(2O15)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf

Weimann, G. (2016). Going dark: Terrorism on the Dark Web. *Studies in Conflict and Terrorism*, *39*(3), 195–206. doi:10.1080/1057610X.2015.1119546

Yasinsac, A., & Manzano, Y. (2002). Honeytraps, a network forensic tool. In Proceedings of the Sixth Multi-Conference on Systemics, Cybernetics and Informatics.

ENDNOTES

[1] United States Department of Justice, “First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More Than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More Than $23.6 Million,” June 26, 2018: https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35

[2] TOR- The Onion Router, explained and available free: https://www.torproject.org

[3] The TOR sponsors since it's establishment from 2001 until 2019: https://www.torproject.org/about/sponsors.html.en

[4] A Network Node is a connection point which can receive, send, store and create data along the network route.

[5] ICANN: https://www.icann.org/

[6] About Google Services: https://www.google.com/about/our-company/

[7] A Top-Level Domain (TLD) is a part of a hierarchical Domain Name System. These mostly include generic domains such as .GOV, .COM, .ORG, .MIL, .EDU as well country codes such as .AR for Argentina or .RU for Russia. In other cases, TLD also assigned and handled by other companies or groups, apart from ICANN. For instance, OpenNIC (Open Network Information System) also assigns TLD such as .FREE or .BBS. In the case of TOR, a .ONION special TLD is not an actual domain but a suffix that is designed to be accessible through proxies with a special software, such as the TOR browser. For more information on DNSs and TLDs visit the ICANN website (www.icann.org) or see Postel, Jon. “Domain name system structure and delegation.” (1994).

[8] The Amnesic Incognito Live System- TAILS, is a live operating system with tor browser in it, and can be started from almost any computer from a USB stick or a DVD disk, aiming to preserve privacy and anonymity.

[9] WikiLeaks and SecureDrop are information submission system, aimed to allow secure and anonymous leakage of confidential information.

[10] The ‘We Fight Censorship’ project is promoted by the Reporters Without Borders organization and funded by the European Union via the European Instrument for Democracy and Human Rights. It is also promoted by the city of Paris, France. For further information see WeFC dark web site: http://3kyl4i7bfdgwelmf.onion/

[11] WeFC, (n.d.), “Local News Sites Blocked”: http://3kyl4i7bfdgwelmf.onion/censored/local-news-sites-blockedhtml.html

[12] VPN- A Virtual Private Network is used to extend a private network across a public network. Effectively, a VPN user can explore the web from a virtual network IP address and not his own physical IP address.

[13] *РосПравосудие* (‘RusJustice’) dark web site: http://rospravjmnxyxlu3.onion/

[14] “Politically Incorrect”, on 8chan dark web site: http://oxwugzccvk3dk6tj.onion/pol/res/12851783.html

[15] The Hidden Wiki: http://zqktlwi4fecvo6ri.onion/wiki/Main_Page

[16] The Daily Stormer’s new dark web site: https://dstormer6em3i4km.onion.link

[17] An anonymous terror threat on the *CHANGOLIA* board in July 2016: http://beepedjhffvat3uwij5fxny72vlj7ugqb67ippjebise6adxf73y3uqd.onion/t/45ed20d1c972b8aba849abb109e919678f7cbfaf/

[18] An interview with a former senior official from one of the British intelligence agencies was made September 2018 in London. The former official asked (Firmly required) to stay anonymous.

[19] Proton Mail is one of the world’s largest secure email services, developed by CERN and MIT scientists. Besides its technological innovations, its servers are based in Switzerland in order to avoid U.S. and E.U. jurisdiction. For more on Proton Mail: https://protonmail.com

Lev Topor is a strategic consultant and the executive director of OTB Intelligence Ltd. Lev wrote his PhD in the Bar Ilan University in Israel. Lev also holds a master’s degree from the prestigious Diplomacy Studies program from Tel Aviv University. Lev’s main research interests include cyber and politics, racism and extremism online.