Scientific Research Publishing

Journal of Computer and Communications, 2019, 7, 30-43
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review

Arbër S. Beshiri, Arsim Susuri

Faculty of Computer Sciences, University of Prizren "Ukshin Hoti", Prizren, Kosovo
Email: arber.beshiri@uni-prizren.com, arsim.susuri@uni-prizren.com

How to cite this paper: Beshiri, A.S. and Susuri, A. (2019) Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. *Journal of Computer and Communications*, **7**, 30-43.
https://doi.org/10.4236/jcc.2019.73004

Received: February 19, 2019
Accepted: March 17, 2019
Published: March 20, 2019

Abstract

The Internet as the whole is a network of multiple computer networks and their massive infrastructure. The web is made up of accessible websites through search engines such as Google, Firefox, etc. and it is known as the Surface Web. The Internet is segmented further in the Deep Web—the content that it is not indexed and cannot access by traditional search engines. Dark Web considers a segment of the Deep Web. It accesses through TOR. Actors within Dark Web websites are anonymous and hidden. Anonymity, privacy and the possibility of non-detection are three factors that are provided by special browser such as TOR and I2P. In this paper, we are going to discuss and provide results about the influence of the Dark Web in different spheres of society. It is given the number of daily anonymous users of the Dark Web (using TOR) in Kosovo as well as in the whole world for a period of time. The influence of hidden services websites is shown and results are gathered from Ahimia and Onion City Dark Web's search engines. The anonymity is not completely verified on the Dark Web. TOR dedicates to it and has intended to provide anonymous activities. Here are given results about reporting the number of users and in which place(s) they are. The calculation is based on IP addresses according to country codes from where comes the access to them and report numbers in aggregate form. In this way, indirect are represented the Dark Web users. The number of users in anonymous networks on the Dark Web is another key element that is resulted. In such networks, users are calculated through the client requests of directories (by TOR metrics) and the relay list is updated. Indirectly, the number of users is calculated for the anonymous networks.

Keywords

Dark Web, TOR, Privacy, Anonymity, I2P

1. Introduction

Many people think that the Internet and web are synonyms. In fact, they are two different terms with common elements. The Internet includes multiple networks and their massive infrastructure. It enables the connection of a million computers by creating a network in which any computer can communicate with other computers as long as they are connected to the Internet [1]. The web (a medium) provides access to information. In terms of conceptualization, the web is a content made up of accessible web sites through search engines such as Google, Firefox, etc. This content is known as "Surface Web" (**Figure 1**) [2] [3] [4] [5].

Another part of the Internet is the Deep Web (**Figure 1**), which is referred a class of its content where for different technical reasons, it is not indexed by search engines and we cannot access via traditional search engines. It includes information on the private networks and intranets (agencies, universities, companies, commercial databases, etc.), sites with queries content or searching forms. Deep Web is segmented further as the Dark Web (**Figure 1**). Its content is intentionally hidden and cannot be accessed by standard web browsers [2] [4].

The sites' publishers on the Dark Web are anonymous and hidden. Users are accessed on the Dark Web to share data with little risk and to be undetected (anonymous). The access of users anonymously is essential for the Dark Web, which recently it is supported by the encryption tunneling for monitoring protection. The Dark Web content is supported by the Onion Routing (TOR). It is anonymous network and access by the TOR browser. The TOR project was launched in 2002 by the US Naval Research laboratory to enable online anonymous

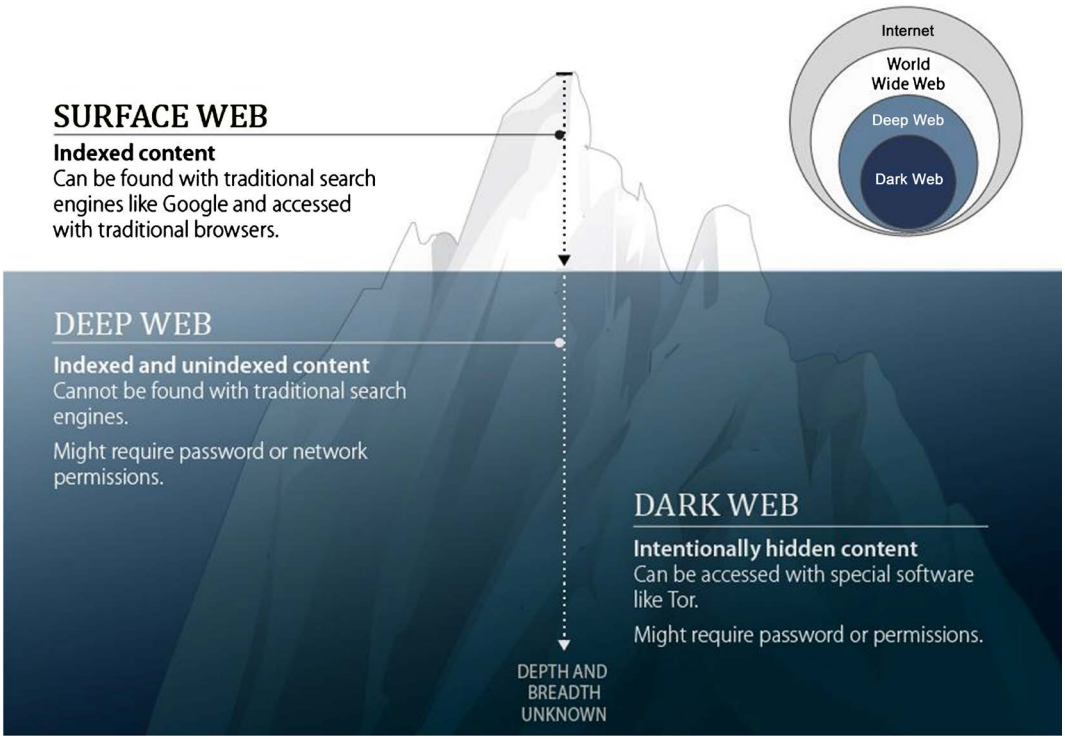

Figure 1. The Internet layers [2].

communication. Invisible Internet Project (I2P) is another network on the Internet with the traffic in its borders and it is used for anonymous communication, users' traffic encryption, etc. It provides more robust and reliability of the networked networks [1] [5]. In the Dark Web, the possibility of user detection is low and this has favored the development of legal and illegal activities among the traffic of this segment of the Internet [2].

Dark web can be achieved through anonymous and decentralized nodes of certain network groups (TOR or I2P). TOR has the software name that we install on the computer and the computer network that care and manage its connections. It enables users to access websites through virtual tunnels where people and organizations can distribute data through public networks without compromising their privacy. TOR enables users to route their traffic through "users' computers" so in order that traffic is not traced back to the originating users and conceal their identity. To pass the data from one layer to another layer, TOR has created "relays" on computers that carry information through its tunnels all over the world. The encrypted information is placed between the relays. TOR traffic as a whole goes through three relays and then it is forwarded to the final destination [2].

"Exit relay" is called the final relay. The IP address of this relay resembles with the TOR traffic source. With the use of TOR, software is possible to hide the addresses of the users. Browsing websites through TOR enables the display of the link for the given web page (in the background of it exists the IP address of the exit relay of TOR). To have more security, anonymity and privacy during the communication, individuals should use e-mails, web chats or similar communications' platforms hosted in TOR [2].

2. Related Work

There are an increasing number of research papers and projects related to the Dark Web. In terms of the related works, the importance and the essentiality of the project have been the focus of improving the surveillance regarding the state [6]. The exchange of the weapons and the occurrence of the child pornography are easily conducted with the help of the Dark Web. The distribution of the network analysis with the help of the TOR network, and the users can easily afford the anonymous anonymity of the process. Therefore, for the conduct of the in-depth analysis, the various works of literature provide for the enhancement of the research, and thereby the TOR routing with the other principles is providing with the help of the various US intelligence systems. It not only enables the Dark Web process for the licit purpose, but the illicit purpose also.

The privacy of the system with depicting the appropriate analysis of the trackers of the network is being easily depicted for the purpose of analyzing the fact and also the research is being continued by the help of the ISI research frameworks [7]. The conduct of the literature review is based on the detailed research on the various parts of the Dark Web which is being explained in an appropriate

way. The research also helps in depicting the appropriate facts regarding the research which was conducted by the researcher.

In another work of Barnett *et al.*, [8] the role of the spiders (defined as the software programs that are used to transverse the World Wide Web information) and the easy accessibility that can be achieved by the process of handling the registration and thereby the exact and the desired information about the various types can be easily collected, is studied.

The social network analysis (SNA) is a topic of interest in [9] and is being conducted for the purpose of obtaining the graph-based methods, and thereby the analysis of the network group becomes easier with depicting the group or the population strength. The impact of the social interactions is widely depicted by the usage of the social networks, and thereby the real world networks can be easily identified.

Different SNA techniques have developed for examining forum posting and website relationships. The main focus is on understanding the "dark networks" and their unique properties [10]. Detailed coding schemes have been developed to evaluate the extremist websites and terrorist contents.

The sentiment and affect analysis allow determining violent and radical sites that impose significant threats [11].

Terrorism informatics is referred to as the application of advanced information fusion, analysis techniques and methodologies to acquire process, integrate, manage and analyze the diversity of the information related to terrorism for international/national security applications. The technique is derived from the disciplines such as informatics, mathematics, science, statistics, social sciences, public policy, and linguistics. The research shows terrorism involves a huge amount of information from different sources, languages, data types, information fusion and analysis, such as text mining, data mining, language translation, data integration, video and image processing helps to detect and prevent terrorism [12].

The identification of fraud and theft are relevant at both the national and international level, since criminals may escape by using false identities, and the smugglers can also enter the country by holding fake visas or passports [13]. Internet fraud, network hacking, intrusion, illegal trading, hate crimes, virus spreading, cyber pornography, cyber privacy, theft of the confidential information and cyber terrorism, narcotics trafficking and terrorism have no boundaries and are a security concern globally.

3. Techniques, Attributes, Accessing and Communication in the Dark Web

Anonymity [14] in the Dark Web derives from the Greek word "anonymia" that refers hiding of the personal identity from others. When we make any action on the web, our footprints deposited as data on the Internet. If the Internet Protocol address cannot be tracked, then we can say that anonymity is guaranteed. TOR

client via volunteer server networks route the Internet traffic over the world. This makes it to conceal user information and avoid any possibility of monitoring activities. Dark Web also has negative effects by allowing criminals to commit cybercrime and conceal their traces [15].

It is considered to be an adequate channel for governments to exchange secret documents, for journalists as a bypass for censorship and for dissidents as a possibility "to escape" from authoritarian regimes. The onion technique[1] enables anonymous communications through a network of computers. Messages are sent encrypted (using the asymmetric encryption) then they are sent through some nodes of networks known as onion routers. When the message is sent to the onion routers, each onion router deletes the encryption layer in the same way as remove the onion peeling to not discover the routing instructions, so a message is sent to the other router and this process is repeated until it is sent to a specific destination (**Figure 2**). This technique protects the intermediate nodes form "being informed" about the source, destination and message content [1] [14] [16].

4. Online Privacy in the Dark Web

TOR is used to enable private, anonymous and secure communications and activities for specific purposes [2] [14]. In the following are given some examples that they are related to above mentioned elements:

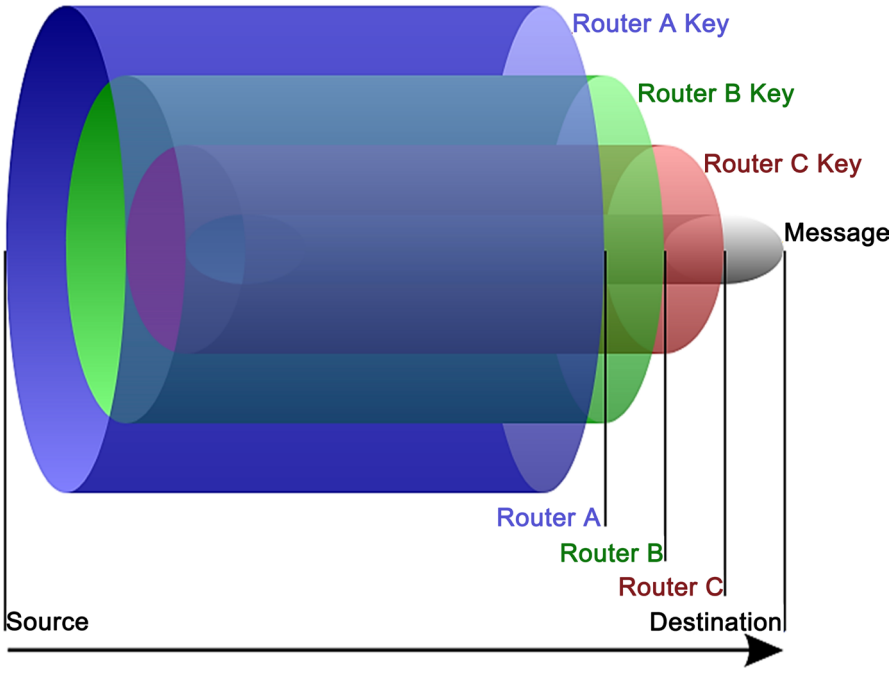

Figure 2. The message routing by using the onion technique[2].

[1]This is available at: Rola, I., Balzarotti, D. and Santos, I. (2017) The Onions Have Eyes: A Comprehensive Structure and Privacy Analysis of Tor Hidden Services. *Proceedings of the 26th International Conference on World Wide Web*, ACM, Perth, Australia, 1251-1260. https://doi.org/10.1145/3038912.3052657

[2]The onion routing is available at: https://en.wikipedia.org/wiki/Onion_routing.

- **Anti-censorship and political activities.** To avoid censorship and to reach certain destinations or contents that they are blocked in one or another way, TOR considers as an adequate tool. It enables individuals to access contents that may be blocked in certain parts of the world. To stop it, some governments have established rules for using TOR, or blocking access to TOR for the specific time periods. TOR is also used by political dissidents to secure and maintain their anonymous communications and locations. Such a case is the movements of dissidents in Iran and Egypt [2].
- **Sensitive communications.** If the individuals want to access in chat rooms or forums and they like to do the sensitive communications for personal or business purposes, this is enabled by TOR. It is used to protect children online (the Internet browsing) to avoid them from abuse activities (by hidden IP addresses of their devices). This tool can be used by businesses to protect their projects and to fence spies from their competitors [2] [17] [18].
- **Leaked information.** TOR can be used from journalists to communicate securely with informers and dissidents [2] [18]. Individuals have the possibility to communicate and share documents anonymity with publishers thought TOR, e.g., the New Yorker's Strongbox. Edward Snowden has used Tail (an operating system for anonymity) that runs in TOR. He has reported and communicated to journalists for disclosing the classified documents about defense programs of the USA. Snowden disclosed a top secret document which described how the National Security Agency (NSA) tried to use the TOR browser to de-anonymized users [2].

5. Dark Web in the Government, Military and Intelligence

Because of the anonymity provided by Tor and other software such as I2P, the Dark Web can be a playground for nefarious actors online. As noted, however, there are a number of areas in which the study and use of the Dark Web may provide benefits. This is true not only for citizens and businesses seeking online privacy, but also for certain government sectors—namely the law enforcement, military, and intelligence communities.

Anonymity on the Dark Web can be used to shield military command and control systems in the field for identification and hacking by adversaries. The military may use the Dark Web to study the environment in which it is operating as well as to discover activities that present an operational risk to troops. For instance, evidence suggests that the Islamic State (IS) and supporting groups seek to use the Dark Web's anonymity for activities beyond information sharing, recruitment, and propaganda dissemination, using Bitcoin to raise money for their operations. In its battle against IS, the Department of Defense (DOD) can monitor these activities and employ a variety of tactics to foil terrorist plots [19].

TOR software can be used by the military to conduct a clandestine or covert computer network operation such as taking down a website or a denial of service attack, or to intercept and inhibit enemy communications. Another use could be

a military deception or psychological operation, where the military uses the Dark Web to plant disinformation about troop movements and targets, for counterintelligence, or to spread information to discredit the insurgents' narrative. These activities may be conducted either in support of an ongoing military operation or on a stand-alone basis [20].

DOD's Defense Advanced Research Projects Agency (DARPA) is conducting a research project, called Memex, to develop a new search engine that can uncover patterns and relationships in online data to help law enforcement and other stakeholders track illegal activity. Commercial search engines such as Google and Bing use algorithms to present search results by popularity and ranking, and are only able to capture approximately 5% of the Internet [20]. By sweeping websites that are often ignored by commercial search engines, and capturing thousands of hidden sites on the Dark Web, the Memex project ultimately aims to build a more comprehensive map of Internet content. Specifically, the project is currently developing technologies to "find signals associated with trafficking in prostitution ads on popular websites" [21]. This is intended to help law enforcement target their human trafficking investigations [21].

Similar to the military's use of the Dark Web, the Intelligence Community's (IC's) use of it as a source of open intelligence is not a secret, though many associated details are classified. According to Admiral Mike Rogers, Director of the National Security Agency (NSA) and Commander of U.S. Cyber Command, they "spend a lot of time looking for people who don't want to be found" [22]. Reportedly, an investigation into the NSA's XKeyscore program—one of the programs revealed by Edward Snowden's disclosure of classified information—demonstrated that any user attempting to download TOR was automatically fingerprinted electronically, allowing the agency to conceivably identify users who believe themselves to be untraceable [23].

While specific IC activities associated with the Deep Web and Dark Web may be classified, at least one program associated with Intelligence Advanced Research Projects Activity (IARPA) may be related to searching data stored on the Deep Web [24]. Reportedly, conventional tools such as signature-based detection don't allow researchers to anticipate cyber threats; as such, officials are responding to rather than anticipating and mitigating these attacks [25]. The Cyber-attack Automated Unconventional Sensor Environment (CAUSE) program seeks to develop and test "new automated methods that forecast and detect cyber-attacks significantly earlier than existing methods." [26]. It could use factors such as actor behavior models and black market sales to help forecast and detect cyber events [26].

6. Payment on the Dark Web

Bitcoin is the currency often used in transactions on the Dark Web [27]. It is a decentralized digital currency that uses anonymous, peer-to-peer transactions [28]. Individuals generally obtain bitcoins by accepting them as payment, ex-

changing them for traditional currency, or "mining" them [29].

When a bitcoin is used in a financial transaction, the transaction is recorded in a public ledger, called the block chain. The information recorded in the block chain is the bitcoin addresses of the sender and recipient. An address does not uniquely identify any particular bitcoin; rather, the address merely identifies a particular transaction [30].

Users' addresses are associated with and stored in a wallet [31]. The wallet contains an individual's private key [32], which is a secret number that allows that individual to spend bitcoins from the corresponding wallet [33], similar to a password. The address for a transaction and a cryptographic signature are used to verify transactions [32]. The wallet and private key are not recorded in the public ledger; this is where bitcoin usage has heightened privacy. Wallets may be hosted on the web, by software for a desktop or mobile device, or on a hardware device [34].

7. Results and Discussion

Results are derived based on research questions (RQ) mainly focused on TOR metrics information and different reliable Dark Web privacy (anonymity) reports and information. Through of them are given arguments about anonymity and privacy for different cases. We have given eight RQ as follows:

(*RQ*1) *How many users use TOR software in Kosovo*?

Based on data that we have generated from the TOR metrics, we find that the daily users of TOR software in Kosovo during January to December 2018 have been near 90. This cipher is increased and decreased during this period of time (**Figure 3**).

(*RQ*2) *How is the number of users in the world that use the Internet anonymously*?

Based on the TOR metrics, the daily users in the world that they have used the Internet anonymously during January to December 2018 was above 4 million in the two first months of 2018 and this cipher has fallen off after second month of the same year (**Figure 4**).

(*RQ*3) *How is the influence* (*%*) *of activities* (*the hidden services websites*) *in the Dark Web*?

According to the study of University of Portsmouth results that researchers have worked with 40 relays (computers) that ran on TOR network and they have collected above 45.000 TOR hidden services web sites. Researchers concluded that 2% of them were for children abuse and 83% of visitors have visited these sites. Another study is realized by King's College London about the TOR hidden services web sites via search engines like Ahmia and Onion City (for the Dark Web). Researchers have identified 5.205 websites live. 1.557 of them is identified by illicit content. According to TOR project estimated that the traffic of hidden services is 3.4%. In March 2016 to March 2017 have existed between 50.000 - 60.000 daily hidden services (unique and with the onion addresses) [2] [3].

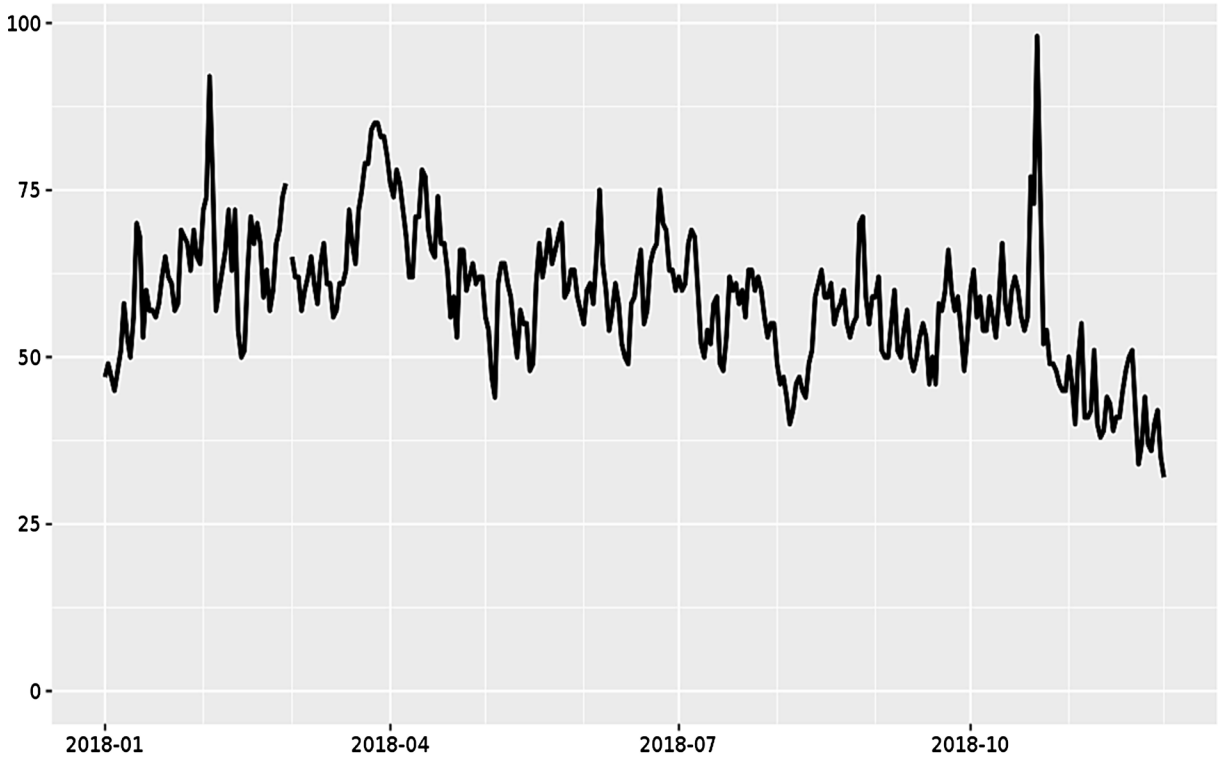

Figure 3. The TOR daily users in Kosovo during January to December 2018[3].

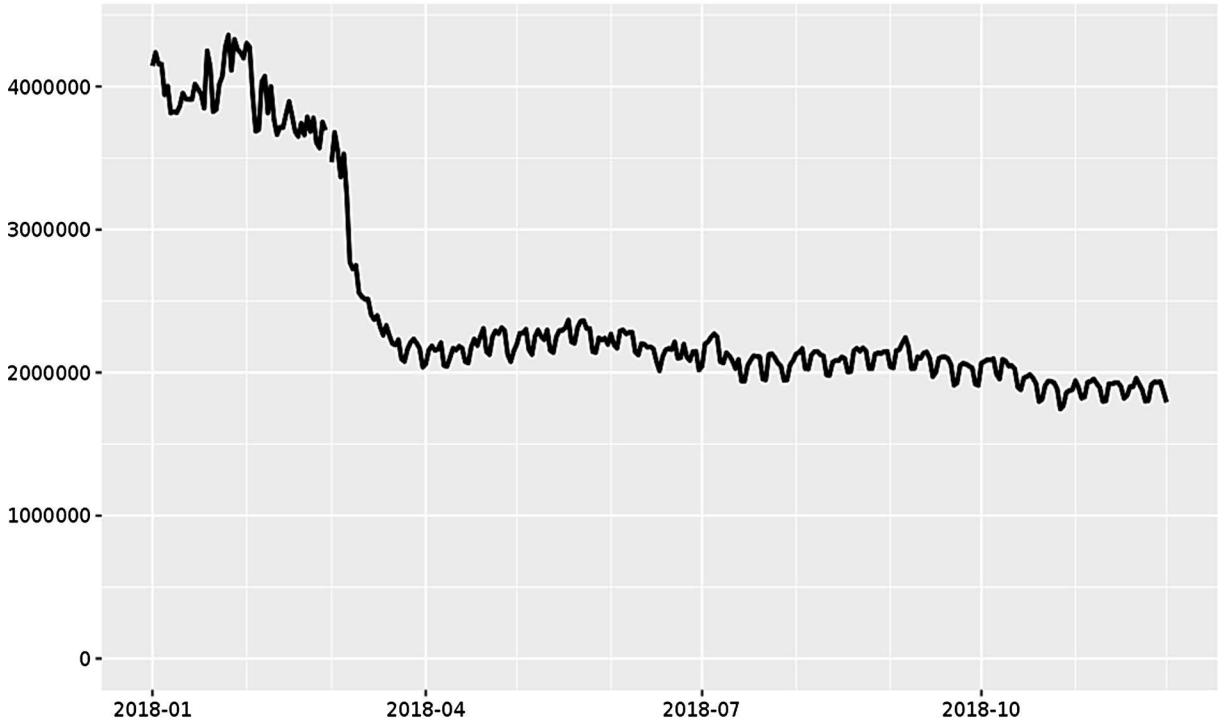

Figure 4. The TOR daily users in the world that they have used the Internet anonymously during January to December 2018[4].

[3]The daily users of TOR software in Kosovo based on the TOR metrics is available at:
https://metrics.torproject.org/userstats-relay-country.html?start=2018-01-01&end=2018-12-01&country=xk&events=off
[4]It is available at:
https://metrics.torproject.org/userstats-relay-country.html?start=2018-01-01&end=2018-12-01&country=all&events=off

(*RQ*4) *Can anonymity be verified in the Dark Web and can we say that it is the anonymous content*?

We cannot say that anonymity is completely verified on the Dark Web. TOR has purposed to enable anonymous activities, but researchers and security experts are continually working to develop tools through which they can identify individuals or hidden services and de-anonymize them. There are many cases (examples) about anonymity, but to elaborate this research question are considered two of them:

1) The Federal Bureau of Investigation (FBI) took in control the Freedom Hosting[5] in 2013, even why many years ago, it had infected that with a malware designed to identify visitors. FBI, since 2002, has used "a computer and internet protocol address verifier" [2] that was a malware in the Freedom Hosting web hosting service, though of which it had identified and verified suspects and their location using a proxy server or anonymous services such as TOR.

2) Hackers who are part of Anonymous, in 2017 have reactivated and controlled the Freedom Hosting II, the web hosting service on the Dark Web and the predecessor of the Freedom Hosting. They claimed that over 50% of the Freedom Hosting content was related to sensitive content. Users who placed these data on the Freedom Hosting could easily be identified. Security experts have concluded that the Freedom Hosting II hosted 1500 - 2000 hidden services (near 15% - 20% of them were rated as active sites) [2].

(*RQ*5) *How the number of users is retrieved from the directory requests through TOR and in what way does their calculation become*?

There are mechanisms in the TOR that make assumptions that clients make on average ten requests per day. A TOR client, if it is connected to the Internet 24/7, can make approximately fifteen requests per day, but not all clients stay connected to the Internet 24/7, so it takes into consideration average ten requests per client. The total number of directories' requests that come from users divide by ten and it is found the number of users. Another way to calculate users is the assumption that each request represents a client who is on the Internet for 1/10 of a day (or 2 hours and 24 minutes).

(*RQ*6) *How do we know from which countries are the Dark Web users and in what way does their reporting become*?

The directories disassemble IP addresses according to country codes from where comes the access to them and report numbers in aggregate form. These numbers indirectly represent the Dark Web users. Since reporting is made in such form, it is considered a reason why TOR ships related to GeoIP database.

(*RQ*7) *How can censorship events be identified/calculated through TOR*?

There is an anomaly-based censorship detection system[6] that calculates the number of users over a series of days and predicts how many users may be in the next few days. If the current number of users estimated to the above system is

[5]For more information please refers at: https://en.wikipedia.org/wiki/Freedom_Hosting.
[6]The anomaly-based censorship detection system is available at: https://dl.acm.org/citation.cfm?id=3201093

high, it can be concluded that there are possible censorship events, otherwise no. For more details about this issue please refer to the relevant report[7].

(*RQ*8) *How can users be numbered in an anonymous network in the Dark Web* (*according to the TOR Metrics*)?

According to the TOR metrics[8], the number of users is not directly calculated, but the requests of directories are numbered frequently for the clients and in this case the relay list is updated. Therefore, based on the above elements, indirectly counts the number of users in an anonymous network.

8. Conclusions

The Dark Web networks such as TOR have provided many possibilities for malicious actors to exchange legal and illegal "goods" anonymously. Dark Web is a growing asset, especially in terms of the illicit services and activities. Security mechanisms should be vigilant to these problems and take measures to eliminate them. The evolving technology with encryption (security) and anonymity (like the Dark Web and its special software) has put law enforcement and policymakers in challenge to effectively struggle harmful actors who are operating in the cyberspace.

In this paper, it is discussed for the impact of the Dark Web, respectively privacy and anonymity of it and through the results, it is shown the anonymous users daily number of this Internet segment for the Kosovo region as well as whole world and how much the impact of hidden services websites on the Dark Web is. The results of this part are gathered from Ahimia and Onion City search engines (for the Dark Web). We have concluded that anonymity is not completely verifiable on the Dark Web even through TOR is dedicated to this network segment which it has purposed to provide anonymous activities. Here is also retrieved the reporting aspect of users from which country they are. In this case, the directories disassemble IP addresses according to country codes from where comes the access to them and report numbers in aggregate form. These numbers indirectly represent the Dark Web users. The number of users in anonymous networks of the Dark Web is not directly calculated. This calculation is made through the TOR metrics where the client requests of directories are calculated an in this case the relay list is updated. Indirectly, the number of users in the anonymous network is calculated as a case is given through results in this paper.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Chertoff, M. and Simon, T. (2015) The Impact of the Dark Web on Internet Gover-

[7]This report is available at: https://research.torproject.org/techreports/detector-2011-09-09.pdf.
[8]The TOR metrics information is available at: https://metrics.torproject.org/reproducible-metrics.html.

nance and Cyber Security. *Centre for International Governance Innovation and Chatham House*, **6**, 1-18.
https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

[2] Finklea, K. (2017) Dark Web. *Congressional Research Service*, Washington DC, 10 March 2017, 1-19. https://fas.org/sgp/crs/misc/R44101.pdf

[3] Ilou, C., Kalpakis, G., Tsikrika, T., Vrochidis, S. and Kompatsiaris, I. (2016) Hybrid Focused Crawling for Homemade Explosives Discovery on Surface and Dark Web. *Proceedings of the* 11*th IEEE International Conference on Availability, Reliability and Security*, Salzburg, Austria, 15 December 2016, 1-6.
https://doi.org/10.1109/ARES.2016.66

[4] Park, A., Beck, B., Fletche, D., Lam, P. and Tsang, H. (2016) Temporal Analysis of Radical Dark Web Forum Users. *Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (*ASONAM*), San Francisco, CA, USA, 880-883. https://doi.org/10.1109/ASONAM.2016.7752341

[5] Berghel, H. (2017) Which Is More Dangerous—The Dark Web or the Deep State? *Computer*, *IEEE Computer Society,* **50**, 86-91. https://doi.org/10.1109/MC.2017.215

[6] Arora, M., Kanjilal, U. and Varshney, D. (2012) An Intelligent Information Retrieval: A Social Network Analysis. *International Journal of Web Based Communities*, **8**, 213-222. https://doi.org/10.1504/IJWBC.2012.046263

[7] Wu, P. and Li, S. (2011) Layout Algorithm Suitable for Structural Analysis and Visualization of Social Network. *Journal of Software*, **22**, 2467-2475.
http://pub.chinasciencejournal.com/JournalofSoftware/18611.jhtml
https://doi.org/10.3724/SP.J.1001.2011.03896

[8] Barnett, G. and Jiang, K. (2016) Resilience of the World Wide Web: A Longitudinal Two-Mode Network Analysis. *Social Network Analysis and Mining*, **6**, 1-105.

[9] Egoryan, L. (2015) New Fields for Web-Analysis: Social Network and Blogs. *Auditor*, **1**, 43-48.

[10] Davies, P. (2008) Information Technology. Oxford University Press, Oxford.
https://www.worldcat.org/title/information-technology/oclc/374881000

[11] Clifton, B. (2012) Advanced Web Metrics with Google Analytics. Wiley, Hoboken, NJ.
https://www.wiley.com/en-us/Advanced+Web+Metrics+with+Google+Analytics%2C+3rd+Edition-p-9781118168448

[12] Chen, H. and Yang, C. (2008) Intelligence and Security Informatics. Vol. 135, Springer, Berlin and Heidelberg, 1-460.
https://www.springer.com/gp/book/9783540692072
https://doi.org/10.1007/978-3-540-69209-6

[13] Yang, C., Mao, W., Zheng, X. and Wang, H. (2013) Intelligent Systems for Security Informatics. Academic Press, Cambridge, Massachusetts, United States, 1-250.
https://www.elsevier.com/books/intelligent-systems-for-security-informatics/yang/978-0-12-404702-0

[14] Jardine, E. (2015) The Dark Web Dilemma: Tor, Anonymity and Online Policing. *Centre for International Governance Innovation and Chatham House*, **20**, 1-24.
https://www.cigionline.org/sites/default/files/no.21.pdf

[15] Baravalle, A., Lopez, M.S. and Lee, S.W. (2016) Mining the Dark Web—Drugs and Fake IDs. *Proceedings of the* 16*th IEEE International Conference on Data Mining Workshops*, *IEEE*, Barcelona, 12-15 December 2016, 350-356.
https://doi.org/10.1109/ICDMW.2016.0056

[16] Chen, H. (2012) Dark Web—Exploring and Data Mining the Dark Side of the Web.

Springer, New York, Vol. 30, 1-454.
https://www.springer.com/us/book/9781461415565

[17] Yang, L., Liu, F., Kizza, J. and Ege, R. (2009) Discovering Topics from Dark Websites. *Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security*, Nashville, 1-5.

[18] Zhang, Y., Zeng, S., Huang, C.N., Fan, L., Yu, X., Dang, Y., Larson, C., Denning, D., Roberts, N. and Chen, H. (2010) Developing a Dark Web Collection and Infrastructure for Computational and Social Sciences. *Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, Vancouver, 23-26 May 2010, 1-6.

[19] Tucker, P. (2015) How the Military Will Fight ISIS on the Dark Web, Defense One. 24 February 2015.
https://www.defenseone.com/technology/2015/02/how-military-will-fight-isis-dark-web/105948/

[20] Zetter, K. (2015) DARPA Is Developing a Search Engine or the Dark Web. Wired.com, 10 February 2015.
https://www.wired.com/2015/02/darpa-memex-dark-web/

[21] Pellerin, Ch. (2017) DARPA Program Helps to Fight Human Trafficking. Department of Defense, 24 January 2017.
https://dod.defense.gov/News/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/

[22] Sciutto, J. (2015) Interview of Admiral Michael S. Rogers (Responding to a Question Concerning the IC's Use of the Dark Web). *New America Foundation Conference on Cybersecurity*, Washington DC, 23 February 2015.
https://www.nsa.gov/news-features/speeches-testimonies/Article/1619291/remarks-at-the-new-america-foundation-conference-on-cybersecurity/

[23] Tucker, P. (2014) If You Do This, the NSA Will Spy on You. Defense One, 7 July 2014.
https://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/

[24] The Intelligence Advanced Research Projects Activity (IARPA). IARPA Invests in "High-Risk, High-Payoff" Research Programs. IARPA and Office of the Director of National Intelligence.
https://www.iarpa.gov/index.php/research-programs/hfc/38-about-iarpa

[25] Homeland Security News Wire (2015) Cyber Researchers Need to Predict, Not Merely Respond to, Cyberattacks: U.S. Intelligence. Homeland Security News Wire, 9 March 2015.
http://www.homelandsecuritynewswire.com/dr20150309-cyber-researchers-need-to-predict-not-merely-respond-to-cyberattacks-u-s-intelligence

[26] The Intelligence Advanced Research Projects Activity (IARPA) (2015) Broad Agency Announcement: Cyber-Attack Automated Unconventional Sensor Environment (CAUSE). IARPA-BAA-15-06, 0-2, 17 July 2015.
https://www.scribd.com/document/257104389/IARPA-Cyber-Attack-Automated-Unconventional-Sensor-Environment-CAUSE

[27] Paganini, P. (2012) What Is the Deep Web? A First Trip into the Abyss. Security Affairs, 24 May 2012.
https://securityaffairs.co/wordpress/5650/cyber-crime/what-is-the-deep-web-a-first-trip-into-the-abyss.html

[28] Murphy, E.V., Murphy, M.M. and Seitzinger, M.V. (2015) Bitcoin: Questions, Answers, and Analysis of Legal Issues. Congressional Research Service, 1-36, 13 Octo-

ber 2015. https://fas.org/sgp/crs/misc/R43339.pdf

[29] Bitcoin. Frequently Asked Questions—Find Answers to Recurring Questions and Myths about Bitcoin. https://bitcoin.org/en/faq#what-if-someone-bought-up-all-the-existing-bitcoins

[30] Bitcoin. Protect Your Privacy. Bitcoin. https://bitcoin.org/en/protect-your-privacy

[31] Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S. (2013) Evaluating User Privacy in Bitcoin. In: Sadeghi, A.R., Ed., *Financial Cryptography and Data Security*, *FC* 2013, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, Vol. 7859, 34-51. https://doi.org/10.1007/978-3-642-39884-1_4

[32] Bitcoin. Some Bitcoin Words You Might Hear. Bitcoin. https://bitcoin.org/en/vocabulary

[33] Bitcoin Wiki. Elliptical Curve Digital Signature Algorithm. Bitcoin Wiki. https://en.bitcoinwiki.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

[34] Bitcoin. Choose Your Bitcoin Wallet. Bitcoin. https://bitcoin.org/en/choose-your-wallet