Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 3000-3005

Research Article

Terrorism on Dark Web

Sara Alayda[a], Najd. A. ALmowaysher [a], Faeiz Alserhani[a], Mamoona Humayun[a,*]
College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia:

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract : Nowadays, everyone has access to a burst of data in Cyberspace. The classic Web or Clear web consists of all the sites Internet and pages that are indexed by search engines conventional research; however, it only represents 5% of the entire web. Despite the multiple Internet advantages, it can hide several threats for nations and people, such as blackmail, illegal drugs and arms sales and murder. This side is the dark side of Internet which includes illegal activities starting from bullying to terrorism. In this paper, we define the Dark Web (DW) and who are the users of this part of cyberspace. We define dark web and emphasize illegal activities related to it. Our study focuses on cyber terrorism activities. Additionally, we define what is cyber terrorism? Who are the responsible of it and why this phenomenon has been exacerbate in the last few years? Moreover, present efforts done by international and national organization to combat against this phenomenon

Keywords: Dark Web (DW), Cyberspace, Web, Cyber Terrorism, Cyberspace, illegal activities;

1. Introduction

In the late 1990s, two research organizations of the US Defense ministry spearheaded an initiative to build an encrypted and anonymous network which protects sensitive communications. Conventional Internet users would not be aware of this secret network and have no access to it. In this way, the Onion Router (Tor) was created [1]. Tor sits on the fringes of the Internet and is the underlying technology of the Dark Web (DW). The term "Dark Net" refers to the hidden face (dark) of the Internet (net). It is a lawless zone of cyberspace (net) in which only illegal (dark) activities would be committed. Before continuing, it is essential to clarify the definition of certain related terms: the deep web, the invisible web, and the hidden web. These terms are synonymous with each other and cover the part of the Internet accessible online but not indexed by conventional search engines (Google, Yahoo!, etc.). However, it should be careful, and make it clear that the invisible web is inaccessible to traditional search engines, because more and more specific search engines are developing. Thus the search engine Shodan [2], created in 2009, references all objects connected to the Internet, whatever their destination.

Unlike the Web, which uses a centralized architecture, the Dark Net uses an architecture called Peer-2-Peer (P2P). So there are several Dark Nets and they can vary depending on their infrastructure. For example, there are P2P networks, mix nets or both at the same time. Unlike a centralized network, P2P works without a main server. Indeed, P2P is intended as an exchange of data between users. The central problem with DW is that with no real control we can find everything and of course illegal activities as well.

For the paper organization, it is divided into four sections. The first section is an introduction that clarify the definition of dark web and how it different of normal web. The second section highlights the main research that was conducted in order to combat cybercrimes on dark web and cyber terrorism in particular. Illegal activities on DW are defined and explained in the third section. Section 4 introduces mechanisms and strategies conducted to combat the cyber terrorism on DW and different present efforts done by international and national organization. Finally, section 5concludes the paper and highlights future works.

2. Literature review

Many researchers, specialists, and scientists keep raising inquiries about how Internet, especially dark web, increases terrorism and violent extremism, and how to combat its danger. In this section we highlight some of these researches which focused on cybercrime in DW. The study presented in [3], authors suggest five different propositions to progress the knowledge on the role of the Internet in extremism and terrorism. According to their suggestions, data should be firstly collected across diverse populations. In addition, they propose to outreach beyond terrorism studies and to engage in interdisciplinary research. Finally, they suggest to connect online and offline worlds of violent extremists.

A classification of illegal activities in DW was presented in [4]. The Authors at first highlight challenges that complicate research on data classification on DW. Namely, training supervised classifiers, which is hard to gather training samples for some illegal categories such as the transportation of weapons. In addition, DW web pages are generally not categorized which makes the data labelling a very time-consuming task. Hence, in order to overcome these difficulties, the authors aims to design and built an easy-train and flexible framework adapted to classify illegal activities on DW. The main contribution of this work is the creation of a data set for DW containing sites categorized and labelled manually. They propose to use a smaller data set and provide a way for the detection and the monitoring new types of illegal activities on DW by network regulators.

In [5], the authors suggest an innovative method to recognize weapon procurement by groups of terrorists using the social media forums. They used classification techniques based on Machine Learning (ML) to categorize the labelled posts. More specifically, they used the analysis of text to detect the purchase of drones in DW. Hence,

they perform an extraction of the communicated messages between terrorist. Thus, they claim that their proposed model can automatically detects the procurement of weapons over DW.

The usage of cryptocurrencies to analyse DW data was conducted in [6]. Authors stressed that several challenges confront them in their study because of DW nature. Among these challenges, the collection of cryptocurrency data on DW should be preceded by the collection of DW data which is a hard task to do. Moreover, because of the pseudosymmetry in DW, it is difficult to identify the cryptocurrency user accounts. Hence, in order to discourse these challenges, the authors conceive a DW data analysis and collection platform. The proposed platform extracts address of dark website using DW indexing services, and then crawl them. Additionally, other dark websites can be also extracted from the crawled data.

3. Legality of dark web

Between data exchanged over networks, internet service providers, who record movements on the web, and some web security agencies, surveillance is ongoing. Hence, DW can prevent this global surveillance of Internet users around the world. Thanks to its access system and architecture, some dark networks make travel anonymous and untraceable. It should be noted that with an IP address generated by an internet provider, we are constantly geo-locatable; regularly and precisely. DW is subdivided into communities. Regularly presented as a place where criminals flourish, it opens up a vast space of exchange where political dissidents and activists, extremist groups and criminals coexist. Everything that constitutes illegal and criminal activities can be found on the DW: sale and exchange of confidential information, counterfeit articles, fundraising for the benefit of criminal organizations, Terrorist organizations, hired pirates and killers, arms and drug trafficking, etc. These very diverse profiles seek to erase their traces on the Internet, to conceal their real identities and their transactions. Consequently, a lot of what we find on a dark net is volatile. The lifespan of sites indexed by Tor would only be a few days to a few weeks. As for legal activities, if their authors consider it necessary to use a dark net, it is because they fear being listened to or tracked. Frequent change of dark net settings allows them to bypass the surveillance they want to guard against.

According to the statistics provided in [7], illegal activities constitute 25% of the global activities performed on Tor. In 2017, the Federal Bureau of Investigation shut down the biggest underground market on DW: Alphabay and Hansa [8]. Another issue with the DW is that it has become the central channel for trafficking illegal data. Therefore, it is necessary to have control and potential monitoring of illegal activities on DW [9].

4. Cyber terrorism: definition, actors and reasons

The term cyber terrorism was first defined by Dr. Barry Collin as a planned attack performed by terrorists on data and computer systems. Later, all the terrorist activities using Internet as a tool were included in this definition [10]. Beyond the sabotage of national infrastructure, terrorism on DW has several forms. Namely, announcing a warning on Internet that a public building includes a bomb is also considered as a terrorist act, this kind of activity aims to spread fear and provoke chaos. Hence, DW terrorism ranges from propaganda and psychological warfare to actions coordination and fundraising. On the public web, websites, forums and social media are supervised by agencies specialized on fighting cyber terrorism and illegal activities. Nevertheless, the nature of DW is advantageous for the terrorists need, such as: anonymity, obscurity and limited access. Thus, DW offers the ideal private communication to terrorists.

Cyber terrorist can belong to different categories. As Figure1 shows, we can divide them to four main categories. The first one is active terrorists; this category represent terrorists that are aware which specific web sites to attack or to change. They use computer network as a tool to lunch a cyber-attack, which they will use it as a weapon. The second category is terrorist sympathizers, they don't have a full knowledge but they participate in terrorist acts because they share the same idea of the terroristic group responsible of these acts. The third category is involved terrorists; this category includes states or nations that are involved in terrorist acts to develop certain capabilities of cyber warfare. The final category is joyriders; this category includes peers who use cyber-attacks and terrorisms to gain notoriety.

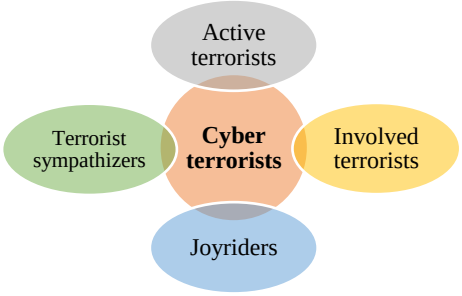

Figure 1.Cyber terrorist categories

After the definition of cyber terrorism and its supporters, it is necessary to understand what are its reasons and motivations. Either ideological, economic, or social, several reasons are launching terrorist activities on DW. However, the most important reason is political motivations. These motivations include regime dictatorship and the lack of political participation of citizens. Despite their differences, all of these reasons aim to violate security and spread fear and panic among individuals and to destabilize or destroy the information infrastructure of countries from a general perspective. In general, DW is used by terrorist for:

1. Communication: Terrorist use DW to coordinate and plan their operations taking advantage of it anonym and obscure aspect.
2. Promotion: Terrorists use DW to publish their statements, as well as to promote their ideologies, in addition to spreading false news and rumors to incite violence and terrorist acts.
3. Propaganda: with the purpose to attract many individuals and recruit them, especially minors, and to get support and financial resources.

5. combat against Dark web terrorism

DW opposes the authoritarian government's surveillance and facilitates the development of an underground market. The security report released by IBM in 2015 reveals the huge threat of DW cyber-attacks. The Dark Web is considered the main platform for criminal activities and terrorism. Hence, providing the essential tools to be developed to combat it is undoubtedly important. Cyber terrorism and is considered the modern form of terrorism, and it must be treated as any other type of war. Terrorism on DW can threaten any country's security and peace. Policies and legislation to combat dark web terrorism differ from one country to another, so each country differs according to its political, economic, and social nature, and that is at the national level, but despite these efforts made by each country separately, it is not sufficient and it requires international efforts in cooperation with some countries.

5.1. International efforts

Many international organizations are working on cooperating with their member states to combat terrorism in general. However, no treaties or international laws are dealing with cyber terrorism. Despite this, several organizations have studied terrorism and ways to combat it. Terrorism is a transnational threat that no government or organization can fight alone; to achieve this, concerted multilateral action at national, regional, and global levels is needed. The absence of an international treaty or arrangement on terrorism is sabotaging efforts to turn terrorists to justice. Thus, a universal agreement based on countries' cooperation during cyber terrorism should be considered. In the annual report released in 2015 [11], reporters stressed up the high importance of establishing practices to fight cyber terrorists and to prosecute their cases. Hence, they recommended that agencies responsible for the enforcement of law should cooperate with Internet service providers (ISP) to gather key evidence in cases of terrorism. International lawmaking made a lot of efforts to fight terrorism by underlining the intergovernmental and regional cooperation on three levels:

1. International organizations: such as the distinctive department created by the Interpol against terrorism (Interpol Counter-Terrorism Fusion Centre).

2. Multinational platforms: G8 efforts to prevent terrorism and protect information technology united with the work of the Organization-for-Economic-Cooperation and-Development (OECD), adopted strategies to secure information systems. They endorse information and computer network security to prevent cyber terrorism and hacking systems [12].

3. Regional action: such as the efforts done by The European Union to combat terrorism, by establishing The-Committee-of-experts-on-Cyber-terrorism (CODEXTER].

5.2. National efforts

Cyber terrorism is one of the most prominent problems facing Saudi society. It aims at destroying the security of the state and creating panic among individuals. Hence, the government has taken many measures and mechanisms, which can be addressed as follows.

A. Legal efforts:

To combat crimes, there must be a punitive legal structure that governs it, and there must be a judicial body that applies the penalty to those who commit it, and this is what has been done in combating the crime of cyber terrorism in Saudi Arabia, the Kingdom was able to create a special law to fight cybercrime. Additionally, it joined the Arab-convention to contesting cyber criminality, such as the Arab Convention to Combat Information Crimes. The KSA ratified the Arab-Convention-to-Combat Information-Technology- Crimes (ACCITC) [13], which includes many cybercrimes such as internet crimes and cyber-terrorism. The purpose of this agreement is to strengthen the Arab countries' cooperation to combat crimes in cyberspace. Moreover, it aims to highlight the property rights laws significance. Penalties are applied when standings and regulations of the agreement are violated.

B. Executive efforts:

Laws are useless without a parallel institutional framework to implement them; ministries and various government agencies are the ones responsible for combating the crime of cyber terrorism. The following is a review of the efforts of some concerned ministries to combat this crime in Saudi Arabia:

- The Saudi Ministry of Communications and Information: it is the authority authorized to propose draft regulations related to communications and information technology and submit them to the Council of Ministers. The Ministry has issued many decisions regulating electronic transactions which included setting up a plan to provide government services and transactions.
- Ministry of Interior: responsible for monitoring internal security affairs, and in this regard the ministry seeks to address cybercrime, conducts meetings to talk over its arrangements to start receiving reports of cybercrime, digital evidence security technique, digital criminals' identification, and checking the cyberspace for purposes.
- Ministry of Justice: responsible for supervising the KSA judicial system. At the same time, it is in charge to ensure that workers fulfill the requests of combating the finance of terrorists and the laundering of money. Courts in KSA have perceived a tremendous growth in deciding on the preparation of cybercrime cases.

To be noted that, the combat against terrorism does not include only the aforementioned ministries, yet there are numerous efforts made by other ministries and organizations, Also, the Kingdom started a media campaign to denouncing terrorism, using text messages, Internet, programs and interviews on TV and advertisements, to propagate counter-extremism visions. Electronic terrorism activities have gained a wide reaction from the government; this last has taken serious measures and make this phenomenon a priority. Hence, the government has adopted strategies and policies aiming to put an end to this crime.

5.3. Scientists' efforts

Lately, scientists have been working to combat terroristic activities on DW and cyberspace. They used innovative techniques, such as link analysis, Web networking, analysis of content, and authorship. Consequently, experts can discover, index, and analyse the activities of extremists. Namely, the Whiteprint technique is established for Dark Web to extracts features to define creators of online anonymous content. Additionally, scientists use Web Spiders software to hunt discussions where terrorist activities are taking place. As we presented in the related works section, efforts have been done by researchers in several works [14] to combat cybercrime and cyber terrorism on the dark web [15].

5.4. Personal efforts

On a personal level, every one of us should be aware of cybercrime risks and the severity of terrorism on DW. Hence, attention should be taken when sharing information or using it. Besides, it is recommended to avoid dealing with unknown accounts or persons online. Moreover, it is preferable to avoid things that make our profiles easy to exposure, such as hashtags. Furthermore, misinformation should be reported, and news should be double-checked. We need to be aware from different intrusion detection approaches [16], ransomware approaches, phishing emails [17] as well to keep ourselves secure. Our self-awareness, and training will protect us from several attacks [18], since attackers have strong criminal networks [19], they are dealt mainly using the personal efforts effectively. Terrorism on dark web uses several approaches to bring the several adversaries to the users, IoT and other smart and light weight applications [20] becomes easy source to approach them. The use several approaches to hard the user data, including ransomware [21]. Blockchain and other related secure mechanisms can further help the users [22] to manage their data.

6. Conclusion

The dark web is a neutral private network, in the sense that it is not substantially harmful. This neutrality should not, however, encourage naivety; it is therefore advised to venture there only with full knowledge of the facts,

without any guarantee of the veracity of the information found. DW can be assimilated, in their illegal part, to a territory run by a gang or a criminal organization: only guests enter and only because something is expected. Simple prudence then advises not to venture there, even on behalf of the company: it is not sure that its quest will be crowned with a certain result, and the risks of compromising the equipment used are proven. Ultimately, it will be interesting to see how legal doctrine views the dark web. Everything that constitutes illegal and criminal activities can be found on the DW. Terrorism on the dark web is considered one of the most dangerous cybercrimes. It can be as harmful as regular terrorism. Therefore, a punitive legal structure must be created and laws should be defined to combat this dangerous phenomenon. As future work, because scientific works on DW have been minimally conducted to date, efforts must be increased to find ways to combat this phenomenon, such as using new technologies, strategies, smart solutions, and operative use of computational analysis to counter cyber terroristic activities on DW.

References

1. Monk, B. M. (2017). Tor, what is it good for? How crime predicts domain failure on the darkweb (Doctoral dissertation, Arts & Social Sciences: School of Criminology).
2. Chen, Y., Lian, X., Yu, D., Lv, S., Hao, S., & Ma, Y. (2020). Exploring Shodan From the Perspective of Industrial Control Systems. IEEE Access, 8, 75359-75369.
3. Scrivens, R., Gill, P., & Conway, M. (2020). The role of the internet in facilitating violent extremism and terrorism: suggestions for progressing research. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 1417-1435.
4. He, S., He, Y., & Li, M. (2019, March). Classification of illegal activities on the dark web. In Proceedings of the 2019 2nd International Conference on Information Science and Systems (pp. 73-78).
5. Saini, J. K., & Bansal, D. (2019). A comparative study and automated detection of illegal weapon procurement over dark web. Cybernetics and Systems, 50(5), 405-416.
6. Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., ... & Shin, S. (2019, February). Cybercriminal minds: an investigative study of cryptocurrency abuses in the dark web. In Network and Distributed System Security Symposium (pp. 1-15). Internet Society.
7. Al Nabki, M. W., Fidalgo, E., Alegre, E., & de Paz, I. (2017). Classifying illegal activities on TOR network based on web textual contents. In Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 1, Long Papers (Vol. 1, pp. 35-43).
8. Afilipoaie, A., & Shortis, P. (2018). Crypto-Market Enforcement-New Strategy and Tactics1. Policy, 54, 87-98.
9. He, S., He, Y., & Li, M. (2019, March). Classification of illegal activities on the dark web. In Proceedings of the 2019 2nd International Conference on Information Science and Systems (pp. 73-78).
10. Chunying Wu and Juan Wang. (2019). Analysis of Cyberterrorism and Online Social Media. In 4th International Conference on Modern Management, Education Technology and Social Science (MMETSS 2019).
11. UNODC Annual Report. (2015). Retrieved February 02, 2017 from http://www.unodc.org/documents/AnnualReport2015/Annual_Report_2 016_WEB.pdf
12. Vilić, V. M. (2017). Dark web, cyber terrorism and cyber warfare: Dark side of the cyberspace. Balkan Social Science Review, 10(10), 7-25.
13. The Arab Convention to Combat Information Technology Crimes: http://www.moj.gov.jo/EchoBusV3.0/SystemAssets/27adcb7a-5539-4b36-9d9a- 8b91f578bac.pdf.
14. Al-Suwaidi, N.A. and Nobanee, H. (2020), "Anti-money laundering and anti-terrorism financing: a survey of the existing literature and a future research agenda", Journal of Money Laundering Control, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JMLC-03-2020-0029.
15. Gabriel Weimann (2015): Going Dark: Terrorism on the Dark Web, Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2015.1119546.
16. Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). A Review of Intrusion Detection System using Machine Learning Approach. International Journal of Engineering Research and Technology, 12(1), 8-15.
17. Ubing, A. A., Jasmi, S. K. B., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Phishing Website detection: An improved accuracy through feature selection and ensemble learning. International Journal Of Advanced Computer Science And Applications, 10(1), 252-257.
18. K. Hussain, S. J. Hussain, N. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-4, doi: 10.1109/ICCISci.2019.8716416.
19. Lim M, Abdullah A, Jhanjhi N, Supramaniam M. Hidden Link Prediction in Criminal Networks Using the Deep Reinforcement Learning Technique. Computers. 2019; 8(1):8

20. A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020, doi: 10.1109/ACCESS.2020.2983117.
21. Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers, 8(4), 79.
22. Alamri, M., Jhanjhi, N. Z., & Humayun, M. (2019). Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. Int. J. Comput. Sci. Netw. Secur, 19, 244-258.