ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 12, Issue, 12, pp.15337-15341, December, 2020

DOI: https://doi.org/10.24941/ijcr.40274.12.2020

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

THE ROLE OF DARK WEB ON CYBERSPACE

***Asalah Altwairqi[1], Hatim Alsuwat[2] and Emad Alsuwat[1]**

[1] College of Computers and Information Technology, Taif University, Saudi Arabia
[2] College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia

ARTICLE INFO

Article History:
Received 10th September, 2020
Received in revised form
17th October, 2020
Accepted 05th November, 2020
Published online 30th December, 2020

Key Words:
Cybersecurity, Cybercrime,
Cyberterrorism, Cyberwarfare.

ABSTRACT

Although the Internet has played a significant role in our daily life, it has become a major threat. To meet this threat, we need to identify the most dangerous layer among the three layers of the Internet, which is the Dark Web. This paper focuses on the role of the dark web in some areas of cyberspace: cybercrime, cyber terrorism, cyber warfare, and cybersecurity

Citation: ***Asalah Altwairqi, Hatim Alsuwat and Emad Alsuwat.*** **2020.** "The Role of Dark Web on Cyberspace", *International Journal of Current Research,* 12, (12), 15337-15341.

INTRODUCTION

Based on the statistics of Internet users around the world published by *We Are Social* website for the year 2019, the number of users reached 4.39 (Kemp, 2019) billion users while reached in 2018 4,021 (Kemp, 2018) billion. We can note the tremendous rise in Internet users. With this rise and different user skills, the question remains, does the use of the Internet differ from a user to a user? The answer is yes, the use of the Internet differs from one user to another. There are ordinary users and they are the majority of Internet users, as they use traditional common browsers to search for information on standard websites. And there are professional users who are the users who have the ability to search information in an invisible and sophisticated way. The Internet is divided into three layers: Surface Web, Deep Web and Dark Web. In the first layer, sites are indexed and saved, where ordinary users can easily access them. For sites that are not indexed, they are stored in the second layer. The third layer is part of the second layer where professional users can access it using special tools (Finklea, 2015). The dark web which is what we focus on it in this paper can be used for legal purposes such as hiding military databases or illegal such as selling weapons and drugs. Where we will focus on the role of the dark web on some aspects of cyberspace, whether legitimate or notsuch as cybercrime. This paper is organized in the following format. In the second section, we explained what the dark web is and a simple summary of its history.

***Corresponding author: Asalah Altwairqi,**
College of Computers and Information Technology, Taif University, Saudi Arabia.

In Section Three we discussed cybercrime and the dark web's role in it. Section four reviews cyber terrorism and the dark web's role in it. In Section five, we learned about cyber warfare and does the Dark Web have a role in it. Section six clarify the importance of securing and monitoring the dark web. Finally, we summarized the paper rapidly.

What is the Dark Web: As we mentioned in the previous section, the Dark Web forms the third layer of the Internet. It is part of the deep web that was deliberately hidden and cannot be accessed using common internet browsers. It is known for its anonymous markets that sell illegal products such as drugs or weapons. We can say that it is the black market of the internet. The idea of an anonymous network of communications over the Internet extends to the sixties with creation of ARPANET. Also known as the Advanced Research Projects Agency network. It is an experimental computer network. ARPANET has been used by the government for years which making it more privatized. This make the ARPANET divide into MILNET and civilian version of ARPANET, MILNET used by defense agencies and military, the civilian version become later the internet (SOS). The 1990s was the start of the Internet boom. With this boom, illegal businesses began to appear, including illegally copying CDs and selling them on online platforms. Later, there was an increased demand for products sold over the Internet, as it was easy and convenient. At the same time Tor appeared. Where he was in its early stages as a private network to surf the Internet (SOS). In 2002 Tor was launched to the world, where it made a shift in the Internet through the ability to surf the Internet freely and anonymously.

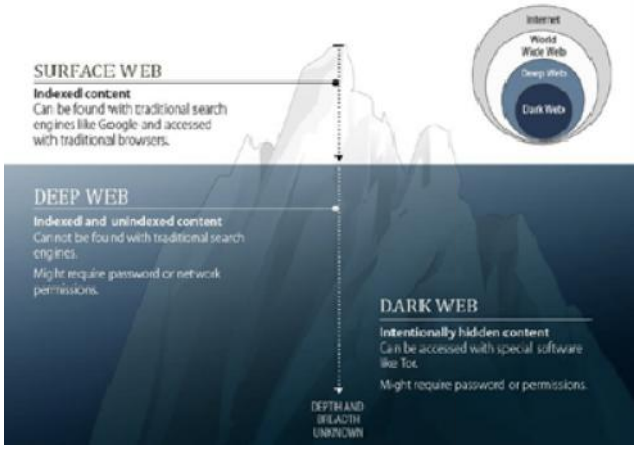

Figure 1. Layers of the Internet (Finklea, 2015)

With the spread of Tor, its users began to demand that they address censorship by the ability to spread ideas and accessing restricted websites freely. This motivated Tor's creators to develop a way for its network to overcome government firewalls. This increased the visibility of dark websites hosting illegal content. In 2009 cryptocurrencies, especially bitcoin, appeared, which is a form of digital currency that facilitates transactions anonymously. Previously, it was difficult to purchase from dark websites due to the fear of revealing identity. But with the emergence of bitcoin, this problem was solved. With the availability of dark websites hosting illegal content and the ability to deal with content from buying and selling and most importantly with a demand for illegal content, the dark web corner will exist (SOS).

Dark Web and Cybercrime: In this section we will start by defining cybercrimes, what they mean. After that we will mention the most important cybercrimes that occur inside the dark web. Finally, we will analyze the reason for using the cybercrimes for dark web. There is still no approved definition of cybercrime. Definitions differed from expert to another. But it is possible to define cybercrime based on the attempts of many academic works as committing illegal actions with a criminal motive through electronic operations that target individuals or group of individuals (Ramírez, 2017; Viano, 2017).now let's figure out the most important cybercrimes inside the dark web (Balduzzi, 2015):

Passports and IDs: Passports and IDs are among the important documents used to identify a person, whether inside or outside the country. Not only identification, but also used to open bank accounts, buy property, and much more. Therefore, the sale of fake passports and IDs is of great importance in the dark web and at high prices. Certainly, the price varies from country to country and from seller to seller.

Stolen accounts: This type of cybercrime is not only limited to the Dark Web, but it is also found on the Surface Web. The most types of accounts that are sold: credit cards, banking, online auction sites and gaming accounts. The price is determined based on the quality and type of account, for example PayPal accounts are highly priced. One type of account that cannot be easily found on the Surface Web is actual physical credit cards. But it is very easy to find in the dark web.

Assassination services: It is one of the most worrying cybercrimes that the Dark Web offers. The Dark Web contains private websites where you rent someone for the purpose of killing someone. These websites do not provide the previous killings operations of a killer if they are successful or not in order to preserve privacy. Of course, to get the agreed price, the killer will provide proof of the killing operation.

Bitcoin and money laundry: Although Bitcoin are basically anonymous. However, it can be tracked as it travels through the system due to the Bitcoin blockchain setup (every transaction is fully public).Therefore, a service was provided that add more anonymity, which makes tracking e-currency more difficult through "mixing" your bitcoin. Bitcoin laundry service was used to Hide the identity of moneyin the bitcoin systems. Later, some users want to extract their money from the system and convert it into a traditional payment method such as cache. The dark web has a lot of anonymous services performing this purpose.

Leaked details Government, Law Enforcement and Celebrities: The Dark Web provides websites that publish leaked information about politicians, celebrities, governments and other people. Of course, it is very difficult to know whether this information is true or false. But the harm of information remains very strong. Where this information can be used for other criminal purposes such as blackmailing.

Drugs: Certainly, selling drugs is an essential part of the dark web. There are websites that sell drugs of various kinds, such as contraband Tobacco, Cannabis, Cocaine and so on. there are also websites that offer live information of Cannabis grow showing temperature, moisture of the growing plants over time.

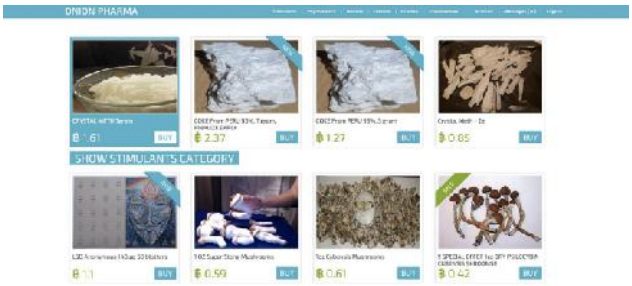

Figure 1. Drugs in Dark Web(7)

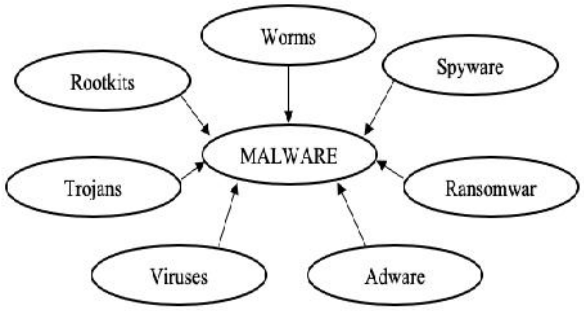

Figure 3. Malware Types

Malware: The best malware environment is the dark web. Because of the provided privacy, which is what every attacker wants.

So, it is difficult when spread a malicious program from the Dark Web to examine the IP address of the server, check the details of registration...etc. For example, Crypto Locker is a malware that uses the Dark Web which is a ransomware that directs the victims to the payment site so that they can regain control of the blocked system / encrypted file. After we learned about the most important electronic crimes that happen in the dark web, and although some of them can happen on the surface web and with knowledge of the services provided by the dark web, we can note that all dark web users want to keep their identity anonymous. In addition, the payment method in the dark web is Bitcoin, which is an anonymous currency. Let us take the third type of cybercrime as an example, which is the most worrying. Let us assume that the killing operation failed, and the hired killer was caught. Can the killer identify the tenant? No. Here the tenant ensures that his identity is completely anonymous. Suppose the killing operation was successful and the killer provided evidence to the tenant. The tenant paid the agreed price in bitcoin. Also, can the killer identify the tenant? No, his identity is also anonymous and the identity of the bitcoin by itself anonymous. Cybercrimes has targeted individuals such as politicians and organizations such as banks, where a criminal conducts a cybercrime with criminal motives such as revenge, money, etc. Certainly, this attack will have a financial or social impact on the individual or organization.According to CNBC and CNN news in 2019 thousands of Disney+ user accounts have been stolen by hackers and put up for sale on the dark web from 3 to 11$(8, 9).

Dark Web and Cyberterrorism: In this section we will start by defining cyberterrorism, what they mean. After that we will focus on the most targeted areas of cyberterrorism. Finally, we will analyze the reason for using the cyberterrorism for dark web. The definitions mentioned in the paper (Al Mazari, 2018) included that cyber terrorism is the use of technology and computer networks to launch attacks that cause individual or international harm with motive of political, religious, psychological or social. now let's figure out the most targeted areas of cyberterrorism (Al Mazari, 2018):

Military Forces: The military forces form the first line to defend national security, and therefore, this target is one of the most important targets. cyberterrorists are attacking military electronic infrastructures, functions, operations, services, systems and other force capabilities. Some of the most famous attacks Denial of Service (DOS), Espionage and data modification.

Government Cyber and Physical Infrastructure*:* This target is the second conservative on the security and stability of the state. Attacking this target is very natural to cause concern and fear to the people. cyberterrorists target government and physical electronic infrastructure and facilities. One of the most common denial of service (DOS) attacks.

Critical National Infrastructures: These systems constitute stability and comfort in the lives of people such as emergency services and energy facilities, media services, healthcare providers, transportation systems, educational institutions, postal facilities, telecommunication systems, dams and financial organizations. Attacking these systems could lead to the loss of billions of dollars or the loss of lives. Some of the most famous attacks Denial of Service (DOS) and malware.

Social and National Identity: Maintaining the identity of the organization or the state clean and reputable is one of the most important things locally and globally. Cyberterrorists distort the identity of the organization or country by spreading false rumors on social media. For example, denigrating a particular country will lead to economic, political, and other harm to that country. Based on the aforementioned attacks, we can divide cyber terrorism attacks into incursion is gaining access to computer systems and networks to get or manipulate information, service interruption aims to flood networks, servers or systems by sending a large number of packets, which makes the target unable to deal with the sent packets which lead to denial of service and disinformation is defame the reputation of target by spreading fake or harmful information (Al Mazari,, 2018).

Now we need to know how the dark web has helped cyber terrorists in terrorist operations. Previously, cyber terrorists used the surface web to exchange terrorist information, but it was fraught with risks in terms of revealing their identity and their location. So cyber terrorists considered the obscurity of the dark web very useful. It helped them to communicate, access various information, recruit and train, and spread and implement terrorist ideas (Weimann, 2016; Vilić, 2017). In 2015, cyber terrorists published an electronic book entitled "How to Survive in the West: A Mujahid Guide". The book includes titles “Hiding the Extremist Identity,” “Earning Money,” “Internet Privacy,” “Training,” “Bomb-Making,” “Transporting Weapons,” and “What Happens When You Are Spied on And Get Raided”. The use of Tor is one of the methods discussed in the book. This is considered an evidence that cyber terrorists use the Dark Web (Weimann, 2016).

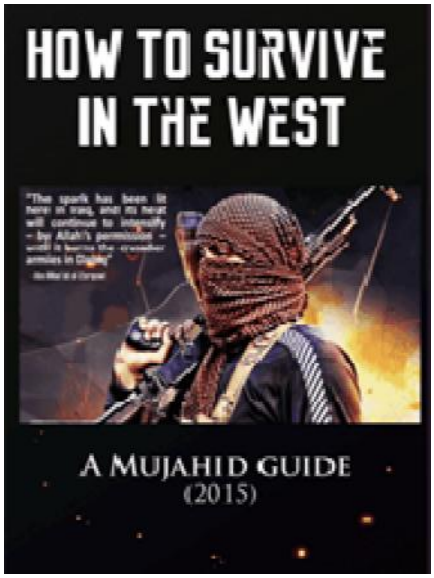

Figure 2: Cyberterrorism Guide

And do not forget the role of Bitcoin in cyber terrorist operations. Some groups that support the terrorist issue are financing cyber terrorists online. As we know bit coin is an acceptable currency anywhere on the Internet, so it is not possible to list the things that cyber terrorists can buy.

Dark Web and Cyber warfare: In this section we will start by defining cyberwarfare, what they mean. After that we will describes five common attacks used in cyber warfare. Finally, we will analyze the reason for using the cyberwarfare for dark web.

The author mentioned in the paper (Robinson, 2015) some definitions of cyber warfareand compare it, where the author summarized by relying on the mentioned definitions that there is no approved definition of cyber warfare, however, we still need to know what does cyber warfare term means. We can say it refers to cyber-attacks on a government by Another government, or by large groups of citizens. Its purpose is to cause damage or disrupt computers or networks. The term can be used to describe inter-company attacks(14, 15). Now we will describe the attacks (16):

Espionage: The most important component of cyber warfare is cyber espionage. In the process of espionage, the attackers view the data or copy it secretly and illegally. Espionage occurs locally, for example, between companies and organizations, and globally between countries.

Distributed Denial-of-Service (DDoS): A denial of service attack is one of the most widespread and simple attacks across the Internet. The attacker floods the target system, for example, military defense systems by sending a large number of packets, which makes the target unable to deal with the sent packets.

Data Modification: This is one of the most dangerous types of attacks used in cyber warfare. The attacker maliciously and secretly modifies some sensitive data in the system. The danger lies in making war decisions based on these data, whether the decision-maker is human or machine.

Infrastructure Manipulation: Such as emergency services and energy facilities, media services, healthcare providers, transportation systems, educational institutions, postal facilities, telecommunication systems, dams and financial organizations. Manipulating these systems maliciously and illegally causes many material and human losses. Previous attacks usually rely on malware, which is software that is included in the system for harmful purposes. One of the most common examples of malware used for military purposes is Stuxnet which is an advanced computer program designed to penetrate and control systems targets programmable logic controllers (PLCs)(17).This type of malware has made great progress in cyber war. It was categorized as a moral gift to cyber warfare compared to real weapons such as the bomb. This is because it causes less damage while achieving the same goal.

Cyber warfare aims to cause painful damages of unknown origin, often from a distance. Despite the damage, but it is more ethically, as there are no human losses, if any, very little. All that the cyber war aims to do is harm to the systems, devices and data. So, the question remains, what is the role of the dark web in cyber warfare? After knowing some of the crimes that occur in the dark web that we mentioned in the third section, which included government leaks and malicious programs. In addition to the terrorist operations that we discussed in section four and how to plan them using the dark web. We can say that the dark web has an indirect role in cyber warfare. This means that terrorist operations threaten national security and in order to maintain national security we need to wage cyber war to stop terrorist operations. In order to wage a cyber war, we need some malware in addition to sufficient information about the target. Of course, this is a simple example of the relationship of the three sections with each other and their relationship to the dark web. According the Washington Post "President Trump approved an offensive cyberstrike that disabled Iranian computer systems used to plan attacks on oil tankers in the Persian Gulf , even as he backed away from a conventional military attack in response to its downing Thursday of an unmanned U.S. surveillance drone, according to people familiar with the matter"(18).

Dark Web and Cybersecurity: In this section we will discuss why cyber security is important. And what is the relationship of cybersecurity in the dark web. But first we need to understand what cybersecurity means in order to determine why it is important. Cybersecurity is Tools, techniques and activities for protection the assets of users, organizations, agencies and governments. This means preventing security risks to ensure the privacy and integrity of data or data systems(19). We need cybersecurity because society depends on the cyber world in their daily lives, from shopping to banking services, communications, and social media via the Internet. Even criminals' or terrorists' operations have become cyber operations. But in the end, the cyber world is associated with the real world and any decision or action taken in the cyber world will affect the real world. Based on that, cyber security emerged because we need to secure the cyber world in order to secure the real world(20).

Now the question is why do we have to secure the dark web? As we mentioned earlier, we need to secure the cyber world, and the dark web is part of the cyber world. The Dark Web is also considered a portalto illegal activities of all kinds. Therefore, the competent authorities have to monitor and secure the dark web so that the damage does not extend to our real world. Although it will be a difficult task, it is not impossible. Here are some possible techniques used to monitor the dark web(21):

- Tor uses a database built on a distributed system (distributed hash table). The system contains nodes responsible for storage and maintenance. Due to the distributed nature of the system, monitoring received requests from a specific domain will be possible by publishing nodes.
- Web data can be analyzed to find non-standard domains. While maintaining customer privacy. This method helps to know the activities available in the dark web.
- Monitor social media sites such as Pastebin. Social media is often used to exchange new services, including hidden services. It may contain new dark web domains.
- Get a snapshot of every dark site once it is discovered. Because most of the dark sites go offline from the Internet for a time and then return with a new domain name.
- Tracking illegal activities now and in the future and link them to the actors can be done by building a database contains information about dark sites.
- Gathering information about dark web users, vendors and available services. This helps to build profiles which makes tracking easier.

According to the FBI news in 2019, the *SaboTor* operation has been successful, an international effort targeting drug trafficking organizations operating in the dark web. As a result of this operation, 61 people were arrested, 50 accounts closed and seizing large amount of drugs, weapons, and money (22). Moreover, there has been a tendency to develop technologies

that monitor the dark web in recent years, such as *Black Widow* which is "a highly automated modular system that monitors Dark Web services and fuses the collected data in a single analytics framework"(23). And always remember as a regular user you must protect yourself through knowledge: your reading of this paper increased your knowledge of the dark web and what can happen in it and what impact it has on us. Therefore, the more knowledge, the greater the awareness. Use multi-layered security for the services you use, for example, when you enter a site, do not save passwords, and if you save them, use an alert that you entered the site. Finally, keep the security software up to date.

Conclusion

In conclusion, we have discussed the role of the dark web in cybercrime as the dark web has formed an ideal environment for cybercrime. The role of the dark web in cyberterrorism has also shaped the origin or creator of terrorist operations. We also discussed the role of the dark web in cyberwarfare and noticed that the role of the dark web is indirect but of strong influence. Finally, we have noticed protecting the cyberworld from the dark web means that it is feasible to protect the real-world from the negative impact of the dark web.

“The Dark web is not as dark as you think. When you buy or sell illegal goods online, you are not hidden from law enforcement and you are putting yourself in danger,” said Europol Executive Director Catherine De Bolle (22).

REFERENCES

Kemp, S., *Digital, 2019: Global Internet Use Accelerates.* 2019.

Kemp, S., *Digital IN 2018: World’s Internet Users Pass The 4 Billion Mark.* 2018.

Finklea, K.M., *Dark web*. 2015, Congressional Research Service.

Sos, S.O.S., *History of The Dark Web (Timeline).*

Ramírez, J.M. and L.A. García-Segura, *Cyberspace: risks and benefits for society, security and development*. 2017: Springer.

Viano, E.C., *Cybercrime, organized crime, and societal responses*. 2017: Springer.

Balduzzi, M. and V. Ciancaglini, *Cybercrime in the Deep Web.* Report by Black Hat EU, Amsterdam, 2015.

News, C., *Hacked Disney+ accounts are reportedly being sold for as little as $3*. 2019.

News, C., *If your Disney+ account got hacked, it's probably your own fault.* 2019.

Al Mazari, A., et al., *Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies*, in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*. 2018, IGI Global. p. 608-621.

Weimann, G., *Going dark: Terrorism on the dark web.* Studies in Conflict & Terrorism, 2016. 39(3): p. 195-206.

Vilić, V.M., *Dark web, cyber terrorism and cyber warfare: Dark side of the cyberspace.* Balkan Social Science Review, 2017. 10(10): p. 7-25.

Robinson, M., K. Jones, and H. Janicke, *Cyber warfare: Issues and challenges.* Computers & security, 2015. 49: p. 70-94.

Gortney, W.E., *Department of defense dictionary of military and associated terms*. 2016, Joint Chiefs of Staff Washington United States.

Schreier, F., *On cyberwarfare*. 2015: Geneva Centre for the Democratic Control of Armed Forces.

Geers, K., *Cyberspace and the changing nature of warfare.* SC magazine, 2008. 27.

McMillan, R., *Siemens: Stuxnet worm hit industrial systems.* Computerworld, 2010. 14.

Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers. washington-post, 2019.

Sevis, K.N. and E. Seker. *Cyber warfare: terms, issues, laws and controversies*. in *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*. 2016. IEEE.

Tarter, A., *Importance of cyber security*, in *Community Policing-A European Perspective*. 2017, Springer. p. 213-230.

Chertoff, M. and T. Simon, *The impact of the dark web on internet governance and cyber security.* 2015.

Office, F.N.P., *J-CODE Announces 61 Arrests in its Second Coordinated Law Enforcement Operation Targeting Opioid Trafficking on the Darknet.* FBI news, 2019.

Schäfer, M., et al. *Black Widow: Monitoring the dark web for cyber security information*. in *2019 11th International Conference on Cyber Conflict (CyCon)*. 2019. IEEE.

****