BOOK CHAPTER | *"Even Though I Walk Through the Shadows.."*

The Dark Web – A Review

Stanley Okyere-Agyei
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems And Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: s.oagyei@yahoo.com
Phone: +233500008002

ABSTRACT

The internet consists of or can be divided into three parts. They are known or referred to as surface web, deep web and dark web. The dark web also known as the 'dark net', represents part of the deep web. TOR, 12P, and Freenet are some specialized tools needed to access the dark web as they cannot be accessed ordinarily. These tools anonymize the internet protocol address of the user. This web level is characterized by notoriety and the operation of illegal markets and activities such as the sale of illicit drugs, firearms, and hitman services amongst others. This review seeks to find out the usage of the dark web, findings in related literature, the ethical and unethical sides of the dark web as well as its involvement in cybercrime.

Keywords: Dark Web, Darknet, TOR, Internet, Cybercrime

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Stanley Okyere-Agyei (2022): The dark Web – A Review
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 209-214
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P34

1. INTRODUCTION

Interconnected networks or the internet as we know it, have become a very powerful and useful resource in modern-day. The world without the internet is unimaginable. Our everyday life tasks, communication, enjoyment, sharing, and exchange of ideas, news, and information all depend on an internet connection. It has enabled new forms of social interaction, activities, and social associations.

The internet however consists of or can be divided into three parts:

- Surface web – the 'visible web' is that part of the internet that is accessible by the general public.
- Deep web – the 'invisible web' is that part of the internet that is not visible to everyone. They require authorization and permission to access them (username/password). Some examples include social networking sites, email accounts, online banking, etc.

- Dark web – the 'dark net', represents part of the deep web. TOR, 12P, and Freenet are some specialized tools needed to access the dark web as they cannot be accessed ordinarily. These tools anonymize the internet protocol address of the user. This web level is characterized by notoriety and the operation of illegal markets and activities such as the sale of illicit drugs, firearms, and hitman services amongst others. A breakdown of the makeup of the dark web reveals some key layers that make it a haven for anonymity. These layers include no webpage indexing by surface web engines making it non-discoverable to even popular search engines to show results for pages within the dark web, the use of virtual traffic tunnels via a randomized network infrastructure, and inaccessible by traditional browsers because of its unique registry operator.

We will seek to answer the following focus questions in this review:

a. What are the roles played by the dark web?
b. How significant is the dark web in the operations of cybercrime and its activities?
c. Has law enforcement been successful in curbing illegal activities on the dark web?

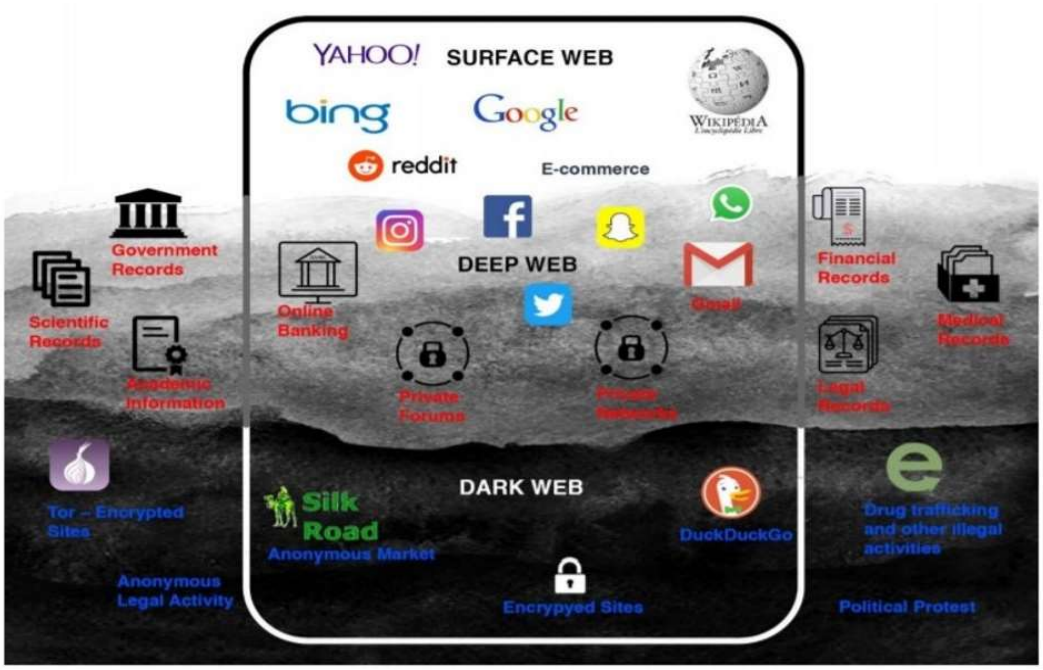

Figure 2. Representation of the surface web, deep web and dark web [5]

1.1. Background

The internet as we have come to know has enabled the formation of a global society hinged on digitization. This digital global society goes beyond race, legal jurisdictions nationalities and/or religion. Even though this society provides a whole lot of anonymity, the individuals that tend to use the internet are bound by the rules, regulations and laws of the country from which they originate a transmission or transaction according to a study by Papacharissi 2022[1]. How is this possible? Internet protocol addresses, IP addresses are unique identities that are linked or assigned to individuals or websites that surf the internet.

This makes it easy for law enforcers to track or monitor individuals who do any activities on the internet using the IP addresses assigned to them. It is at this point that the dark web comes in because of the anonymity it provides. The dark web dates quite back as far as 1969 when a University of California student sent the first electronic message using a computer and the ARPANET system. The Advanced Research Projects Agency Network (ARPANET) was the first wide-area packet-switched network with distributed control and one of the first networks to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet. It was after this that individuals who use the internet created dark nets using the ARPANET system.

Since then, various tools like the onion router (TOR) have been developed to aid anonymous internet surfing on the dark web. Beshiri [2] in 2009 in his study stated that the dark web racks in 57% of illegal content amongst other crimes such as illicit drugs, child pornography, data theft, sale of fake currencies, etc. Forensic examiners say that the privacy of the anonymous user is one of the most serious concerns [3].

2. RELATED WORKS

The Internet is a globally built system of computer networks. It is a network of networks in which users behind a computer and with access can get information from any other computer. These connected users sometimes can interact or have a chat directly with each other. The internet was built and developed or invented by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was christened the ARPANET. Its sole purpose at the time was to create a network that enables users of a research computer at one university to connect to other research computers at other universities. In the event of a military attack, the ARPANET's design made it possible for messages to be routed or rerouted in more than one direction; the network could continue to function even if parts of it were damaged [4].

3. DARK WEB

The dark web dates quite back as far as 1969 when a University of California student sent the first electronic message by the use of a computer and the ARPANET system. Internet users after this discovery created darknets and in the early 1970s, the first dark web drug deal transaction, e-commerce, took place between some university students with their dealings being kept secret and undetected by the ARPANET [5].

How to Access the dark web

New encryption technology and anonymization browser applications like TOR and Freenet now make it possible for any individual to access the dark web which once used to be a preserved territory of hackers, cybercriminals, and law enforcement agents. The TOR, an acronym for The Onion Router, developed in the late 1990s by the U. S naval research lab is a network browser that affords its users to access or visit with the '. onion' registry operator [6].

Figure 2. Warnings found on the surface web that explains to users how to access the dark web [5]

Cybercrime

INTERPOL defines cybercrime as "crimes against computers and information systems, where the purpose is to gain unauthorized access to a device or deny access to a legitimate user. It goes on to further describe cyber-enabled crime as a 'traditional' crime facilitated by the Internet, such as fraud, theft and the sale of fake goods [7]. 'Old wine in new bottles?': research conducted by Peter Grabosky expresses how cybercrime or virtual crime is quite similar or relates to a crime that happens physically. The only difference is the medium in which either crime is conducted [8]. The dark web provides a hub for criminal attacks as it serves as a gateway to the world of virtual crime through the provision of anonymity to users. The following are some of the well-known crimes that do happen on or over the dark web: drug trafficking, frauds, arms trafficking, contract killers, congestion attacks, phishing, revenge attacks, child pornography, etc.

4. IMPLICATIONS FOR AFRICA

Several reports have indicated or predicted that there is going to be a major shift in some crime areas in Africa, a shift from online surface crimes to the dark web as law enforcement intensifies its enforcement on the surface web leading to the growth and establishment of these underground crimes.

A 2017 report by Trend Micro in association with INTERPOL examined the Middle East and North Africa underground markets describing the Middle East and North Africa underground as a melting pot for cybercrime, culture and ideology. This combination of culture and ideology makes the market unique and highly influences the services and products offered. In their data-based study based extracted between July and December 2016, Trend Micro finds that dark net markets and clientele are present in North African countries with a variety of products and services being sold on their websites. The data-based analysis argues that despite not being as big as its counterparts, the Middle East and North African underground is active with a growing client base and the expertise and resources needed to manage it will develop as well hand in hand with the development of the underground [9].

The INTERPOL and the Trend Micro report, Western African cybercriminals are becoming more sophisticated and shifting to more complex business models and operations. They are gaining more social engineering expertise that is allowing them, complemented by increasingly available tools and services such as crypters, key loggers, etc. to steal money via elaborated crimes from individuals and companies around the world. They further predicted that these skillful criminals will eventually found their own criminal markets and communities online to promote their crimes and sell their products leading to a boom in the Western African underground dark web market [10].

5. RESEARCH GAPS/ FINDINGS

Under this heading, we discuss the areas in which we identified some gaps within the current sark web literature as reviewed. In the wake of technological advancement, it is becoming increasingly difficult for law enforcement agencies to track, identify and shut down internet websites that allow the practice of illegal activity especially more so that these activities are ceasing to exist in their current form. The dark web has allowed decentralized communication between people making it increasingly difficult for monitoring by law enforcement. Law enforcement seems to be more focused on the deanonymization of browsers that grant access to the dark web as a means of clamping down on people or users for buying and selling on the dark web. The focus should rather be on increasing law enforcement operations that seek to bring down the source of illicit activities on the dark web. For example, law enforcement should be focused on the source of drugs rather than the dark web marketplace as there would be no drug to trade on the dark web if there is no source.

6. CONCLUSION

This paper sought to conduct a literature review into the roles played by the dark web, how it has enabled cyber-crime and how law enforcement bridges that gap between the society. Due to the secretive nature of the dark web, information and research available on this topic was challenging. In answer to the first question which required the roles played by the dark web being investigated, the online marketplaces for illegal activities are still a major use and remain a major headache for society and law enforcement. The second research question was aimed at the significance of the dark web in the operations of cybercrime and its activities.

Some evidence showed that the subject matter, the dark web serves as a tool for many criminal activities as well as training grounds. The dark web in real terms has lowered the barriers of entry into the world of cybercrime. Finally, to answer the third research question, law enforcement agents in the area of the dark web have not had an easy one in pursuit and the closedown of markets that trade on the dark web. However, the dark web infrastructure has been reacting to these law enforcement incidents in an attempt to mitigate these loopholes that are continually exploited by the authorities.

7. RECOMMENDATION FOR POLICY AND PRACTICES

Government must define the tactics for the dark web regulation. These tactics should be defined in such a way that there is suppression of criminal web activity which takes place on the dark web as well as protecting the anonymity of innocent dark web users. Government can rely on the combination of the capabilities of various state agencies to effectively deploy the dak web

policies. There is also the need for governments to pass legal frameworks which are very essential in the support of the dark web criminal investigations.

8. DIRECTION FOR FUTURE WORKS

A number of future directions can be proposed for organizations and users in order to protect themselves on the dark web from criminal activities. There is a need for a deep understanding of the dark web and its accompanied threats as well as those of malicious malware. The dark web, for an organization, is useful or can be utilized for intelligence gathering by way of monitoring marketplaces on the darknet for stolen and trade of customer or company data and/or potential brand misuses. There is however still some danger in exploiting these opportunities as you could collaborate with criminals by granting them access to your own networks. Organizations in as much as utilizing the dark web to their advantage must adopt some application isolation which rides on layered defense mechanisms in identifying threats to stop cybercriminals from getting unauthorized access to corporate networks.

REFERENCES

1. Papacharissi, Z. 2002. "The Virtual Sphere: The Internet as a Public Sphere," New media & society (4:1), pp. 9-27.
2. A. S. Arber S Beshiri, "Dark Web and Its Impact in Online," in Journal of Computer and Communications, 7, 30-43., Kosovo, 2019.
3. C. M, "A public policy perspective of the Dark Web," in Journal of Cyber Policy. 2. 1-13, 2017.
4. https://www.techtarget.com/whatis/definition/Internet
5. Online African Organized Crime from Surface to Dark web - INTERPOL July 2020
6. https://www.kaspersky.com/resource-center/threats/deep-web 2022
7. Definitions retrieved from INTERPOL public website and documents www.interpol.int
8. P. Grabosky, "Virtual Criminality: Old Wine in New Bottles?" in Social and Legal Studies 10: 243-49, 2001
9. M. R. Fuentes, 'Digital Souks: A Glimpse into the Middle Eastern and North African Underground', *Trend Micro*,
10. 2017, p.37, https://documents.trendmicro.com/assets/white_papers/wp-middle-eastern-north-african-
11. underground.pdf (accessed 26 February 2020).
12. 'Cybercrime in West Africa Poised for an Underground Market', *Trend Micro & INTERPOL*, 2017, p. 30-31,
13. https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf (accessed 26 February 2020).
14. The Dark Web as a Phenomenon: A Review and Research Agenda - Abhineet Gupta - 719080 The University of Melbourne Semester 1, 2018
15. Dark Web: A Web of Crimes - Shubhdeep Kaur1 · Sukhchandan Randhawa1 202
16. Dark Web, Its Impact on the Internet and the Society: A Review – Upulie H.D.I, Prasanga P.D.T 2021
17. Digital Souks: A Glimpse into the Middle Eastern and North African Underground 2017
18. Trend Micro and INTERPOL: Cybercrime in West Africa Poised for an Underground Market