جامعة
الملك سعود
King Saud University

THE WEB'S EVIL TWIN

Ethical Issues in Computing & Research Method

Dr. Sarah Alsulaiman

Lamia Al Thunyan
Sara Al Muhareb
Yara Altwaijry
Leena AlQasem
Monirah Almotlaq

Table of Contents:

Abstract: 2

Introduction: 3

Literature review: 3

Methods: 6

Results: 7

Discussion: 9

Conclusion: 10

Reference 11

Abstract:

The Deep Web is the data on the internet that is not accessible by popular search engines. Since people have a false perception towards dark web; therefore, this paper investigated people ideas toward this new phenomenon. This paper examines how people perceived the dark web by conducting an online survey that resulted in people associating the dark web with illegal and illicit activities. The result of our questionnaire was that people first heard about the dark web through social media, family /friends, then news. Also, the findings showed that the majority thought about using the dark web. We found that most of the majority of respondents are familiar with the dark web and they specify its usage with illegal activity.

Introduction:

We are in the midst of the fourth technological revolution, the Internet has become intertwined within the daily life of all people. It has connected the world and enabled people connectivity. Furthermore, it has facilitated the transmission of information and news between the various places of the world in all its details and forms. But do the internet users actually know about the other side of the Internet, the hidden side or literally ‘’The Dark Web’’?

The Dark Web is marked by the unknown, The Dark Web is a part of the internet known as the Deep Web. The Deep Web is the part of the internet whose content is not indexed by classical search engines and cannot be accessed using search engines. The dark web is a subset of the Deep Web that requires some specific browser such as Tor browser, specific software, configuration, or authorization to access. The Dark Web is accessed for both legal and illegal purposes. The widespread use of Dark Web for illegal activities has made it a den of mystery. Users of the internet have different perceptions about the dark web. Some of them are familiar with it and the others did not hear about it.

This research paper sheds light on the different perceptions about the dark web. The present research paper contains the abstract and the general introduction, literature review, methods and results, the discussion of the results and for the last part it presents the conclusion.

Literature review:

This chapter is divided into four parts: the first part focuses on the studies that show the different layers of the Internet. The second part considers the studies that talk about the special browser (Tor) that is used to access the dark web. The third part explains the government’s efforts and dilemma with the dark web. The final part discusses the studies regarding the financial transactions that have taken place on the dark web.

Layers of the Internet:

The layers of the Internet go far beyond the surface web that many people access in their day to day life. The surface web is the part of the Internet that is indexed by search engines and can easily be accessed. It contains only 10 percent of the information that’s available on the Internet. Nath et al. (2019) stated that the deep web, on the other hand, consists of pages which are clearly approachable but not present in the result pages of engines. As they’re not indexed by any search engine and can be accessed using direct links such as URLs. It includes private information such as networks used at government agencies, banking sites, and cloud-based accounts (Google Drive) which require a username and password.

According to Nath et al. (2019), they estimate that the deep web is (400.000% to 500.00%) times larger than the surface web. Finally, the dark web is a part of the deep web that centers around illegal deeds and services. It can only be accessed by using a special browser such as Tor. Some people refer to the dark web as the place where humanity's darkest side surfaces.

Tor:

We live in a time of free-flowing data, where any person with an internet connection has all the information they could ever need at their fingertips. Although the internet has vastly expanded the capability to share knowledge, it has also made issues of privacy more complex, with many worrying that their personal information (including their activity on the internet) may be monitored without their permission.

Tor has the answer, like many concealed wonders on the internet, it is misunderstood. According to Ormsby (2015), Tor is software that allows users to browse the web anonymously. Established by the Tor Project, a nonprofit organization that encourages anonymity on the internet. The onion router which may sound like an unusual name, comes from the concept of 'onion routing' which is how people navigate the dark web. Data is transmitted through a sequence of network nodes that each "peel" away a layer of encryption. Each node only knows the location of the previous or next node, keeping the sender anonymous.

Surprisingly, Chertoff (2017) found that Tor was initially developed with very different intentions. At the turn of the twenty-first century, the Naval Research Laboratory (NRL) developed Tor with the purpose of granting anonymity to U.S. military personnel. To certify the anonymity of military users, the NRL implemented it in October of 2003 as an open-source browser. This meant that military traffic was buried in a crowd of anonymous civilian users.

Ormsby (2015) found out that the dark web has some sites that are reachable through entry points like the Hidden Wiki that work like stooge sites. They may need an invite or recommendation to get in, but obstacles to access are not that high because they are not the real deal. They are just there to divert journalists and law enforcement while they operate the genuine sites elsewhere. At best, they are a testing ground where they can pick helpful contributors and invite them to the place nobody else knows exists. Others are ghost sites that require you to have the authorization from somewhere else like a real-life contact.

As stated by Kumar (2019), today many organizations keep a secret website on Tor, including nearly every major newspaper, Facebook, and even the US Central Intelligence Agency (CIA). This is because a Tor website exhibits a commitment to privacy. The New York Times and the CIA, for example, are both anticipating facilitating interactions with people who can provide sensitive information.

The Government and the dark web:

The dark web is a place where identities are hidden, everyone is kept anonymous, criminals and ordinary users cannot be distinguished. It’s home to illegal marketplaces. While it’s not illegal to visit the dark web world, it provides access to illegal activity. Nevertheless, it helps people who live in repressive regimes like those in Russia, Iran, and China where they lack the freedom of speech to communicate freely. There is plenty to do without breaking the law. Users can socialize and join book clubs. Journalists protect the identity of their sources using Tor browser. However, Sandep Rathore stated that Tor browser can be illegal in some countries due to strong encryption which is considered illegal in these countries.

Protecting political dissidents, privacy advocates, and whistle-blowers should not come at the expense of empowering child abusers, arms traffickers, and drug lords. According to Michael Chertoff (2017), criminals should be exposed to maintain average user’s privacy. Enforcement agencies can resolve the issue and unmask the criminal by employing government hackers to place deanonymizing tools in the electronic devices accessing illegal sites, and enforcement would bring charges against these users. Number of users may decrease due to the risk of being caught when using illegal sites. If government attempts to break Tor, it would most likely thwart all its efforts because a more powerful version would be created. Moreover, shutting it down would simply make these activities shift overseas which makes it even harder on authorities to resolve the problem. It would also harm individuals in oppressive regimes who rely on anonymity for free expression.

The United States is constitutionally dedicated to protecting freedom of expression on the internet. Some countries are threatened by the freedom of speech and wish to have complete power because it would let citizens circumvent state censorship. Governments can reduce dark web issues by establishing some agreeable regulations that govern the Dark Web.

Eric Jarden (2015), found that since technological efforts to weaken or break the system are riddled with problems of either stifling freedom of expression efforts or garnering technological counteraction from online activists, the best way forward is to manage, and hopefully minimize, the costs of the anonymous network through active and judicious policing. Dark web policy must be thoughtfully classified in order to balance between legitimate users like dissidents and the responsibility of government to stop illegal actions.

Financial transactions:

Financial activities on the dark web are mostly done by cryptocurrencies. Since it's impossible to proceed your payment by other payment methods such as cash or credit card because they would reveal your identity. A hidden network and a transactional currency that cannot be tracked are a recipe for a place where illegal activities would arise. Nath et al. (2019), found that most transactions are traceable to individuals or entities in the real world, the use of cryptocurrency such as bitcoin has allowed for anonymous exchange of money.

According to A.S et al. (2019), bitcoin is a decentralized digital currency that uses anonymous, peer-to-peer transactions. They figured out that users' addresses are associated with and kept in a wallet. The wallet consists of an individual private key, which is a secret number that grants that individual to spend bitcoins from the comparable wallet, similar to a password. The address for a transaction and a cryptographic signature are used to certify transactions. 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.

Blockchain technology provides total anonymity, it's a decentralized public ledger which keeps immutable record of the transactions on the network. This record is stored across multiple users which adds a level of security and reliability. Block chain doesn't require a centralized authority to verify the transaction. A significant set of changes has been made to their anonymity network which includes next generation crypto algorithms, enhanced authentication schemes, and redesigned directory. They have increased the size of the onion addresses and also made them absolutely private. It will help them better to combat against leaks and cyberattacks.

Moreover, a recent report by Chainalysis (Leading Crypto-Payment Analytic Firm) (2019) shows that bitcoin transactions on the dark web grew from approximately $250 million in 2012 to $872 million in 2018. The firm projected that bitcoin transactions grew high and reached more than $1 billion in 2019. The report also noted that the proportion of bitcoin transactions tied to unlawful deals has decreased by 6 percent since 2012 and now accounts for less than 1 percent of all bitcoin activity.

Methods:

The chosen research method is an online survey, since the anonymity of surveys allows respondents to answer with more candid answers. The survey mostly contained closed-ended multiple choice questions with yes and no answers, and a few checkbox questions. The sample included both genders, All age groups and all nationalities from Riyadh, Saudi Arabia. Subjects were people who have heard about the Dark Web.

Results:

The survey included 1196 individuals from both genders, 54.3% were males and 45.7% were females, with different age group (Figure 1).

The result of our questionnaire was that people first heard about the dark web through social media (79.5%), family /friends (17.7%), or news (2.8%).

Also, the findings showed that 60.1% thought about using the dark web. These majority were inquired if they actually used it, and 20.8% of them did. They were asked about their experiences, and their results showed variety of experiences (Table 1). As for the 39.9% who did not think about using the dark web, we asked them to clarify why. (Figure 2). Also, for the 79.2 % who thought about using this platform, but they did not enter it, their justification was either fear (62.2%), indifference (19.6%), or illegal perception of it (18.3%).

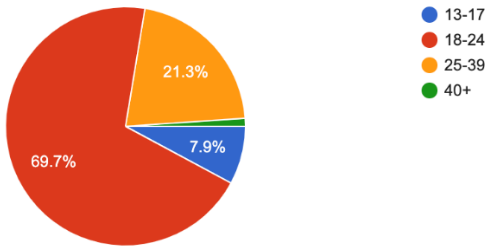

Figure 1. Difference of age group

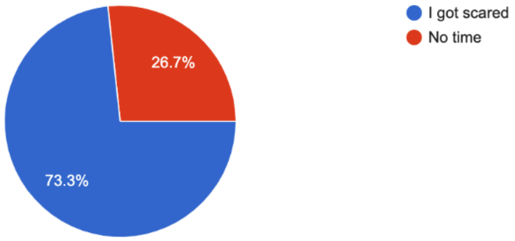

Figure 2. Reasons for participants who did not think about using the dark web

Table 1. Examples of responses

Response	***Example***
Disappointment	"Exciting at first but then it was normal and anticlimactic."
Discomfort	"It was a horrible experience, you see drugs to human trafficking and weapons, or pay for watching people get killed or tortured. Crazy!"
Pleased	It was a marvelous experience. I like the freedom of ideas and information.
Regret	"Back in 2017 I entered dark web in order to see how it was, I thought it was cool to have access to it. Then after one day, my laptop got hacked. The virus was called wannacry. All my files got encrypted more than 80Gb of my old photos, videos and songs. I couldn't see any solution except re-formatting my whole system and delete everything. In the end, I think that I deserved that because I entered the web without having any antivirus system on my laptop."
Interesting response	"The dark web does not hold the same reputation as it used to back in the old days. Now it is observed by government and have some regulations. However, it is not reliable because everything you want can be downloaded from videos, photos, and files that are dangerous to your software system. For example, you can easily be hacked by anyone, buy drugs, employ a hitman for murder. There are great number of videos of rape, torture, murder. It sure requires some experience to use it. "

Our results depicted that the percentages of people who perceived a user of the dark web is either a criminal, a hacker, or a regular person are 83.3%, 69%, or 25.6%, respectively.

We enquired the participants if they think that using the dark web is crime, the results stated that 31.9% agree, 18.9% disagree, 49.2% think maybe. In the same matter, we surveyed if they think it is ethical to use it, the results reported that 11.2% think that it is ethical, 58.2% think it is not, whereas 30.6% think maybe it is ethical.

Most participants (80.8%) believe that it is possible to profit from the dark web whereas others didn't; additionally, when participants were asked about their knowledge of how financial transactions are done in dark web, their responses resulted in either cryptocurrency, bartering, or cash (Figure 3).

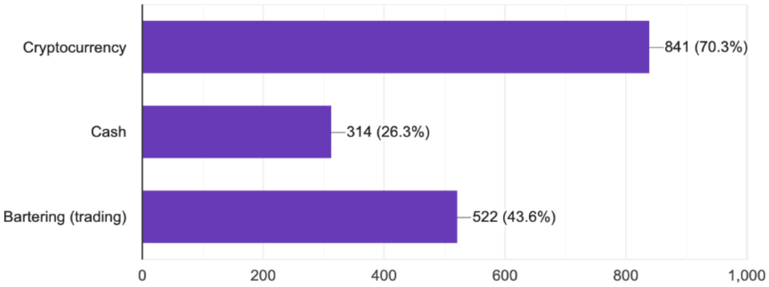

Figure 3. Methods of financial transactions on the dark web

When asked about the risk of identity theft upon using dark web, the results were described as either greater than regular web, lower, or the same. (Figure 4).

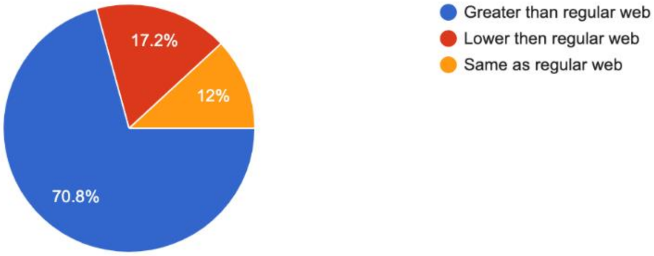

Figure 4. The comparison to the risk of the dark web to regular web

Results showed that 24.8% participants believe that the dark web is authorized by someone, 35.5% participants do not, and 39.7% participants don't know. Also, 33.4% partakers think that there is someone who has the authority to shut down the dark web, whereas 66.6% did not. Additionally, majority of participants (86.3%) perceive that the dark web helped in increasing crime rates. Lastly, most participants (74.3%) suppose that there can be bad consequences to using the dark web.

Discussion:

When the participants were inquired about how they first heard about the dark web, it came as no surprise that the majority of them discovered it from social media. Hence, the information that they're obtaining is biased. As social media tends to dramatize things and only involve the bad side to attract people's attention. Moreover, not all the information on there is valid and accurate. For instance, if you look up "the dark web" you'd be horrified by what some people can do and what they're into. Yet, it's not all bad ,you can't let a rotten apple spoil the whole batch, the dark web does have a good side that includes research papers, chess games, book clubs etc.

The majority of participants assumed that most dark web users are criminals, and they are not to blame. There are a lot of criminals and bad people on there, but the majority of them are people with sick interests. Regular people had the lowest percentage which wasn't surprising because people tend to associate the dark web with bad people. But there are some people on there that worry about the violation of their privacy, or something as simple as data about them being collected, or they'd like to enjoy practicing some activities while their privacy is respected. In order to maintain their privacy and stay anonymous they use the dark web.

Considering most participants assumed that dark web users are criminals, it's expected that they'd presume that using the dark web would be a crime. As we discussed the dark web isn't all bad and does have some benefits. Since using the dark web has been viewed as a crime people also supposed that it's unethical. The reason behind that is people tend to make the assumption that if something is illegal then it is also unethical because breaking the law does carry some sense of immorality.

Since an abundance of the participants picked cryptocurrency that means that they're aware of how transactions on the dark web work. As cryptocurrency helps assure the buyers' and sellers' anonymity.

To our surprise, a fairly large percentage of the participants also picked cash, which makes no sense since using cash would beat the whole purpose of anonymity in the dark web. The buyers' and sellers' identity would no longer be a secret. So instead of going through the trouble of using the dark web and finding a reliable source you can just go to your local black market and get whatever you desire. Furthermore, when trading you can lose anonymity therefore exposing yourself to unwanted danger. For instance, the seller could ask you for inappropriate content in exchange for the product or service you'd like.

The participants suspected that shutting down the dark web wouldn't be possible. In a way they weren't wrong, since the dark web isn't a single set of sites so much as a network of sites that you need special protocols or software in order to find. In order to "shut down" the dark web you'd need to shut down the whole Internet. Surprisingly, shutting down the whole Internet is feasible in some countries with what's known as the internet kill switch. It's a countermeasure concept of activating a single shut off mechanism for all Internet traffic, it exists in India, Turkey, the United Kingdom and a few more countries. Whereas some countries like the United States for instance, they monitor the dark web and target illicit websites. Silk road as an example was shut down by the FBI.

Limitations:

Since the dark web is a fairly new concept, research and articles revolving around it have been very limited. Furthermore, People aren't very aware and educated about the dark web which means that a large portion of society was excluded from our research.

Strength:

One of the few research in Saudi Arabia that focuses on the dark web.

Conclusion:

The dark web is like a black hole that sucks you into it, that's what makes it an interesting topic for researchers. Though it is strengthening its hidden roots, it is still a mystery to most Internet users. Our paper found that the majority is familiar with the dark web and associates its usage with illegal activity. Moreover, it was found that more than expected tried to access the dark web, but failed, only a small number were successful.

Reference

Nuruddin Bin Razali and Nur Razia binti Mohd Suradi. (2019). *A Nest for Cyber Criminals:The Dark Web.* Malaysia: self service.

Aditi Kumar and Eric Rosenbach. (2019). The Truth about the Dark Web. *FINANCE & DEVELOPMENT*, 25.

Arbër Beshiri and Arsim Susuri. (2019). Dark Web and Its Impact in Online Anonymity and Privacy. *Computer and Communications*, 14.

Asoke Nath and Romita Mondal. (2019). Dark Web The Uniluminated Side of the World Wide Web. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING*, 10.

Bellaby, R. (2019, August 17). *Why people need the dark web, whether they want it or not*. Retrieved from The lse Us Centre: https://blogs.lse.ac.uk/usappblog/2019/08/17/why-people-need-the-dark-web-whether-they-want-it-or-not/

Finklea, K. (2017). Dark Web. *Congressional Research Service* , 16.

Indian Government's Internet Kill Switch – How Much Is It Justified? (2018, June 8). Retrieved from Trak.in: https://trak.in/tags/business/2011/03/16/indian-government-internet-kill-switch/

Jardine, E. (2015). The Dark Web Dilemma: Tor, Anonymity and Online Policing . *Centre for International Governance Innovation and Chatham House.*, 13.

McGoogan, C. (2016, december 20). *social media blocked in Turkey*. Retrieved from the telegraph: https://www.telegraph.co.uk/technology/2016/12/20/turkey-blocks-access-facebook-twitter-whatsapp-following-ambassadors/

Mihnea Mirea and Victoria Wang and Jeyong Jung. (2018). The not so dark side of the darknet: a qualitative study. *Security Journal* , 16.

Ormsby, E. (2015, August 1). *If you found it by browsing, it's probably not dark web*. Retrieved from ALL THINGS VICE: https://allthingsvice.com/2015/08/01/if-you-found-it-by-browsing-its-probably-not-dark-web/