https://doi.org/10.48009/1_iis_2020_141-146

INTRODUCING THE DEEP AND DARK WEB INTO HIGHER EDUCATION PEDAGOGY: AN EXPLORATORY STUDY

Gary Janchenko, Robert Morris University, janchenko@rmu.edu
Karen Paullet, Robert Morris University, paullet@rmu.edu
Frank Hartle, Robert Morris University, hartle@rmu.edu

ABSTRACT

Present-day television, Internet, and radio advertisements portray the deep and dark web as an underground place where nefarious and frightening activities occur. A place where drug lords reign and credit card information flows like mighty rivers. Research finds that the general population in the United States tends to understand very little about what the deep web and dark web actually are and that most people access the dark web in some form almost daily. The purpose of this exploratory study is to examine the existing literature to understand more of what information is currently published related to the public's knowledge of the dark web as a base for a future publication. From this research, the authors propose two training scenarios: one for university students and another for law enforcement. The results of future studies on this topic will serve to fortify both of those courses.

Keywords: Dark Web, Dark Net, The Onion Project, Silk Road, Cryptomarkets

INTRODUCTION

On any typical day, any of us likely use what we know as the Internet to make purchases, check schedules for transit or engage any number of other benign activities. Most of what we do and know happens as a result of typing a simple web address or searching for something into a search engine such as Google, Bing or Yahoo! and then clicking on a result that is provided. When something we are looking for is not listed, we might try one other search term before giving up or asking someone else to try to find whatever it is for us; in the end, we decided we did not need it that badly anyway. In reality, the part of the Internet that we are accessing is only a small portion of the Internet that is available. Some of the Internet is locked away behind paywalls, like newspapers or University libraries, but some of it is less available to most users. The dark web or dark net, as it is called, is a portion of the Internet that is a world of its own. Locked away behind paywalls and generally inaccessible to the majority of the public, the dark web has become somewhat of an enigma. Lately, the dark web is the subject of commercials and Internet ads trying to use ignorance and fear to get people to sign up for monitoring services for companies who claim to look for our personal information on the dark web and report it to us. The purpose of this paper is to give readers some understanding of the deep and dark web, to explore the current research, suggest pedagogical use cases for teaching students and professionals about the deep and dark web and lastly to setup cases for future research.

The Dark Net

The term "dark net" or "dark web" does not refer to a physical attribute to the Internet, instead, it refers to the notion that the pages categorized as dark web pages are simply not indexed by pages such as Google, Yahoo!, or Bing (Pergolizzi Jr, LeQuang, Taylor Jr, & Raffa, 2017). To access the Internet, the user downloads a specific encrypted browser released by The Onion Project (TOR) and after connecting to the browser, the dark net functions similar to any other web experience and there exists very little learning curve.

Akin to the experience of a user's access to eBay and Amazon to purchase everyday items, dark net users can access cryptomarkets of all imaginable types, ranging from drugs to credit cards and even hired hits (Martin, 2014). Another main difference, again, comes in the type of the browser and the underlying technology. The TOR browser has built-in encryption, all communication goes through Pretty Good Privacy cryptography (PGP) and then the payments in exchange for the goods or services purchases are facilitated by cryptocurrency (Broséus, Rhumorbarbe, Morelato, Staehli, & Rossy, 2017). The typical browser, i.e., Internet Explorer, Safari, Firefox, etc., does not have these features built-in.

Potential Issues with the Dark Web

The very characteristic that makes the dark web so enticing to so many users also makes it enticing for users who are attracted to it who can act under the cover of anonymity. Some users will never use the dark web for any illegal activities. Some users may just like to do normal web browsing in more anonymous browsing and shopping. Others, however, will use the anonymization to their advantage and conduct illegal activities, such as buy or sell drugs, buy guns, or any other illegal activities. Security experts and analysts have claimed that police agencies have almost no chance of beating the existing encryption currently employed by cryptomarkets. Some experts have claimed that authorities would need tens of thousands to millions of years to crack their algorithms (Martin, 2014). Despite the risks associated with accessing the cryptomarkets, buyers use the encryption to protect themselves as they engage in activities or make purchases. The biggest issue with the dark web may be that the general public simply is not informed enough about it to know that it is not necessarily a bad place and that they likely access the dark web daily.

LITERATURE REVIEW

The Center for International Governance Innovation in Canada conducted a global study on the Dark Net which spanned across 24 countries. The study revealed that 71% of global citizens believe that the Dark Net should be shut down (Zohar, 2016). The survey consisted of 24,143 users from the following countries: Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, South Africa, South Korea, Sweden, Tunisia, Turkey, and the United States. Of those surveyed from the United States, 72% believe the Dark Web should be shut down

Mirea, Wang, and Jung (2018) conducted a study of the Dark Net that is in place for legitimate reasons. The researchers used a qualitative interview style of an online survey where participants answered questions based on four different Dark Net forums. The interview link was posted in the following forums which resided on the Dark Net in 2018: The Hub, Intel Exchange, Darknet Central, and DArknetM Avengers. The forums were selected because they were put in place for general discussions and not specific purposes. A total of 17 complete interview responses were analyzed Mirea et. Al., (2018) who identified five main themes to include the Darknet is not underground, the Darknet's anonymity provided freedom of expression, the Darknet is not a society on its own, the Darknet marketplace Silk Road, and the Darknet does not intrinsically breed criminal activities. An interesting finding of Mirea et Al. (2018) study is that most participants use the Darknet as a way to express their views within a society that enables a sense of belonging.

The Dark Web is used by the government, military and intelligence agencies. Due to the anonymous nature of the Dark Web, it can be used to shield military command and control systems. The military can use the Dark Web to discover activities that may present a risk to the troops. They can monitor the activities to prevent harm and destruction (Beshiri & Susuri, 2019). TOR can be used by the military to take down websites and intercept communications. Additionally, the military can post misinformation which could throw the enemy off their track. The Intelligence Community spends time looking for actors that do not want to be found. For example, after Edward Snowden disclosed classified information, anyone who attempted to download TOR was automatically fingerprinted electronically, allowing the National Security Agency (NSA) to potentially identify users (Tucker, 2014).

Faizan and Khan (2019) created a custom crawler made in Python to collect addresses of hidden services on the Dark Web. The researchers analyzed 6,227 datasets and manually classified them into 31 different categories to identify the nature and content of the information listed on the Dark Web. English is the most common language used on the Dark Web followed by Russian. The categories revealed that criminal content is a common factor but also revealed the following non-criminal content to include books, educational, forums, news and personal web sites (2019).

A study conducted at the University of Surrey (McGuires, 2019) revealed that the number of Dark Web listings that could harm an enterprise has risen by 20% since 2016. Of all listings (excluding those selling drugs), 60% could potentially harm enterprises. Data trading of intellectual property and trade secrets is becoming increasingly popular on the Dark Web which can have detrimental harm to an organization or enterprise.

Due to anonymity, it is hard to say who resides on the Deep Web. A team of researchers from Trend Micro analyzed Deep Web pages based on the language used. In terms of domains, English was the main language used in over 62% of the pages analyzed, followed by Russian with close to 7% of the pages analyzed. When analyzing language distribution based on URL's Russian beat English at 41% compared to 40%. Despite having fewer sites in Russian the sites that were used were much larger (Ciancaglini, et.al, 2015).

Ciancaglini, et.al. (2015) analyzed the top 15 vendors across all marketplaces on the Deep Web and showed that light drugs were most exchanged followed by pharmaceutical products, pirated games, and online accounts. Additionally, the researchers collected Web Reputation URL ratings for every link that points to the Surface Web to identify suspicious sites. Web Reputation, a URL rating site scans sites that a person visits then the URL is tagged for scanning and categorization. URL's that consistently get flagged as malicious will end up on a blocked list of known bad or infected sites. (Trend Micro, 2020).

Only 4% of Internet content is visible to the general public when using search engines such as Google. The other 96% of the content is visible behind the Deep Web. The reason that Google is not picking up the 96% is mainly that businesses associated with the Deep Web are either illegal or bad for the public as a whole (Mwila & Phiri, 2019). The anonymity associated with the Deep Web such as the use of a tor browser has brought about notorious web sites. The Deep Web can cause harm to a computer or person if not used appropriately.

FINDINGS

Our review of the literature has revealed a lack of studies that deal with research about the general public's understanding of the deep and dark web. The literature that was useful for this research often repeats the same generalized findings regarding the deep and dark web's origins and use in law enforcement activities. A 2018 study by Abhineet Gupta surmised that perhaps the reason for the lack of substantial information on the subject is due to the "secretive" nature of the dark web (Gupta, 2018). Gupta echoes the same information as other studies have documented in that the general public's knowledge of the deep and dark web is that it is solely for illegal and nefarious activities.

DISCUSSION, CONCLUSION AND FUTURE RESEARCH

Educating Students on the Deep and Dark Web

The results from this research, as well as the results from the proposed future research, may be used to create a course or to create material to embed into existing courses for students to help educate on the dark web. When we access the Internet for our mundane shopping or web browsing needs, we are only scratching the surface of what is publicly available. Indeed, much of what is on the Internet is locked away behind the paywalls and in unindexed systems of newspapers, library systems and government entities and only about 0.3 percent are available to us through Yahoo!, Bing, and Google (Goodman, 2015).

In Future Crimes, author Marc Goodman describes how little Google indexes of the internet as the equivalent of only fishing the top two feet of the world's oceans. Beyond the depths, lies a separate Internet that goes by the dark net or often the dark web where user traffic is not searchable, and everyone goes by a secret name. Shopping takes place in cryptomarkets yet still functions with the familiarity of Amazon and eBay where the sellers are still rated by the buyers and feedback plays such a crucial role that buyers' risk being banned from platforms for not leaving feedback for purchases.

Creating a full course or course materials on the dark web could help more people understand what it actually is and how many of us use it daily for legitimate reasons such as accessing online library searches or reading the news behind a paywall. Before the course or course materials could be created, it would be important to understand the current state of knowledge. Therefore, it is proposed for future research to administer surveys, starting with college students, to understand what it is that students know about the deep and dark web. The results of the survey data would be used to craft course material related to the deep and dark web and work towards dispelling rumor and myth in favor of fact and practical application of the platform.

Educating Law Enforcement on the Deep and Dark Web
Investigating, identifying and prosecuting drug sales in the physical world and on the surface web is difficult. While doing the same on the dark web is not impossible it is a multitude more difficult. Attribution is at the heart of any criminal case. By its nature, the dark web via TOR was created to allow the government to transfer and communicate secretly. The foundation of the network is to prohibit attribution. Once released into the wild and adopted by those looking for anonymity, freedom, and/or anarchy it proliferated into an enormous, virtual, lawless enclave. While a vast majority of the dark web is not used for nefarious purposes, the most popular areas that include drug marketplaces are the most popular (Hayes, Cappa, & Cardon, 2018), posit that drugs make over half of the total marketplace items for sale and that two-thirds of the individual selling on marketplaces are selling drugs.

Attribution aside, many more issues are investigating and prosecuting drug sales on the dark web. The internet, to include the surface web, the deep web, in the dark web, are virtual and omnipresent and there are several prosecutorial and jurisdictional problems both in the United States and globally. The dark web makes it easy for international drug producers to ship drugs anywhere in the world anonymously. Because these illegal drugs are so easy to find, purchase and deliver and because the entire transaction is anonymous, purchasers perceive anonymity to be a safer alternative than buying traditional way, "on the street" (Pergolizzi, et al, 2017). Drugmakers can manufacture and sell drugs from locations where law enforcement is ineffective or nonexistent or where functioning governments are weak. Even with international cooperation, the many multifaceted laws and conflicting jurisdictions, as well as unwilling partners, make it difficult for law enforcement to adequately combat dark web drug sales in a coordinated manner and with the unified focus (Brown, 2015).

Collecting evidence and determining the identities of actors requires special technologies and skills. A large part of the skills is commonly referred to as hacking or network investigative techniques. Attribution is key to prosecution. Without knowing who the criminal actors are, law enforcement cannot bring a case. Hacking solves several of these problems by either assisting in identifying actors running marketplaces, gaining access to the marketplace by brute force and mapping its structure, identifying customers' monikers and potentially their real identities, and/or dismantling the marketplace through hijacking. This surveillance and search and seizure have many potential pitfalls both constitutionally and legally as law enforcement may break the laws of foreign countries while attempting to enforce the laws in the United States (Ghappour, 2017).

Another issue confronting law enforcement conducting dark web drug investigations is the fourth amendment question of unreasonable searches and seizures. Stewart (2018), suggests that there are many unanswered questions when it comes to the seizure and searches of packages with suspect illegal drugs without a warrant. This question is particular to attribution as many packages are sent with aliases. There are disagreement and confusion in the courts as to whether or not packages addressed to aliases can be seized and searched with probable cause. There is further confusion as to how to determine what packages are legitimate and what solely as part of a criminal scheme. Unaddressed this issue has the potential to affect law enforcement investigative abilities and have a serious impact on the public's fourth amendment protections.

Prosecuting online dark web drug sales is another issue confronting law enforcement. While Title 21 United States Code (USC) Controlled Substances Act is utilized to prosecute illegal drug sales, it was not written explicitly for online sales since there was no such thing when it was codified. Nugent (2019), explains that both the "crack house statute" and the conspiracy aspects of Title 21 may be used they are ambiguous and far from perfect and have thus far not been adequately challenged. For this reason, Title 21 requires expanding or amending to cover the virtual realm of drug sales.

While prosecution is undoubtedly needed there is conflicting data as to its efficacy. Lokala et al. (2019), analyzed the connection to dark web supply of drugs into an area and overdoses. The study showed strong time-lagged correlations among the dark web supply of opioids and overdose-related incidents. The deaths from overdoses are at epidemic levels (Hayes, Cappa, & Cardon, 2018). Strong enforcement is needed to limit the ease of obtaining dark web supplied drugs. The dismantling and prosecution of the drug marketplaces may not be effective at reducing the availability of the drugs and reducing the willingness to partake in its sales. Décary-hétu, & Giommoni, (2017) put forward data that indicates the impact of law enforcement crackdowns on dark web markets. Looking at marketplaces after law enforcement disruption shows a limited reduction in time and scope. While some dark web dealers retired after some initial arrests, the number of dealers recovered to nearly its preoperational level within a month. After two months they were just as many new dealers as before. In addition, after two months sales were twice as high in the same period. This study shows that the deterrent effect of dark web marketplaces is limited to a few months. While that may be discouraging, recent studies indicate that scientific targeting of specific actors has greater efficiency to a dark web criminal network. Da Cunha Bruno Requião et al. (2020), showed that targeting 766 individuals out of 10,407, belonging to a pedophile dark web network, produced more potent takedown of the network. Focusing on the individuals with the most connections enabled on enforcement to focus on the actors responsible for structuring the whole criminal enterprise. With limitations on law enforcement resources, and know-how, as well as legal limitations, this study shows that targeting is key to having the greatest impact.

Future Research

The researchers are using the current literature to create a survey on perceptions of the dark and deep web. The researcher intends to find out participants' knowledge and understanding of the dark and deep web, TOR, online anonymity, policing and what they believe takes place on the dark web. The current survey consists of 16 questions and is in the process of clearing IRB. Once the study is approved it will be distributed to undergraduate students at a mid-Atlantic University. The results of the study will be published in future articles.

REFERENCES

Beshiri, A.S. & 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.

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International, 277*, 88–102. https://doi.org/10.1016/j.forsciint.2017.05.021

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1), 55-119. Retrieved from https://reddog.rmu.edu/login?url=https://reddog.rmu.edu:3479/docview/1707836020?accountid=28365

Ciancaglini, V., Balduzzi, M., McArdle, R., & Rosler, M. (2015). Below the Surface: Exploring the deep web. Trends Labs. Retrieved from https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

Da Cunha Bruno Requião, MacCarron Pádraig, Passold, J. F., dos Santos, L. W., Jr, Oliveira, K. A., & Gleeson, J. P. (2020). Assessing police topological efficiency in a major sting operation on the dark web. Scientific Reports (Nature Publisher Group), 10(1) doi:http://reddog.rmu.edu:2081/10.1038/s41598-019-56704-4

Décary-hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous. *Crime, Law and Social Change, 67*(1), 55-75. doi:http://reddog.rmu.edu:2081/10.1007/s10611-016-9644-4

Faizan, M., & Khan R.A. (2019). Exploring and analyzing the dark web: A new alchemy. First Monday.org. Retrieved from https://firstmonday.org/article/view/9473/7794

Ghappour, A. (2017). Searching places unknown: Law enforcement jurisdiction on the dark web. *Stan. L. Rev., 69,* 1075.

Goodman, M. (2015). Future Crimes. New York: Doubleday.

Gupta, A. (2018) The dark web as a phenomenon: a review and research agenda. The University of Melbourne. Retreived from http://hdl.handle.net/11343/213940

Hayes, D. R., Cappa, F., & Cardon, J. (2018). A framework for more effective dark web marketplace investigations. *Information, 9*(8), 186.

Lokala, U., Lamy, F. R., Daniulaityte, R., Sheth, A., Nahhas, R. W., Roden, J. I., ... & Carlson, R. G. (2019). Global trends, local harms: availability of fentanyl-type drugs on the dark web and accidental overdoses in Ohio. *Computational and Mathematical Organization Theory, 25*(1), 48-59.

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket.' *Criminology & Criminal Justice, 14*(3), 351–367. https://doi.org/10.1177/1748895813505234

McGuire, M. (2019). Into the web of profit: Behind the dark net black mirror threats against the enterprise. University of Surrey. Sponsored by Bromium. Retrieved from https://www.bromium.com/wp-content/uploads/2019/06/Bromium-WoP-Behind-the-Dark-Net-Black-Mirror.pdf

Mirea, M., Wang, V., & Jung, J. (2018). The not so dark side of the darknet: a qualitative study. *Security Journal, 21*(2), pp. 102-118.

Mwila, K., & Phiri, J., (2019). The Deep Web. Experiment Findings. Retrieved from https://www.researchgate.net/publication/335336010_The_Deep_Web

Nugent, T. J. (2019). Prosecuting Dark Net Drug Marketplace Operators Under the Federal Crack House Statute. Fordham L. Rev., 88, 345.

Pergolizzi, J. V., LeQuang, J. A., Taylor, R., Raffa, R. B., & NEMA Research Group. (2017). The "Darknet": The new street for street drugs. *Journal of Clinical Pharmacy and Therapeutics, 42*(6), 790-792. doi:10.1111/jcpt.12628

Stewart, K. (2018). The fourth amendment, dark web drug dealers, and the opiod crisis. Florida Law Review, 70(5), 1097-ii.

Trend Micro, (2020). All about Trend Micro Web Reputation Services (WRS). Business Support. Retrieved from https://success.trendmicro.com/solution/1058991-information-about-trend-micro-web-reputation-services-wrs

Tucker, P. (2014). If you do this, the NSA will spy on you. Defense One, Retrieved from https://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/

Zohar, S (2016). The "Dark Net" should be shut down: CIGI-Ipsos global survey: But what about its benefits? Centre for International Governance Innovation. Retrieved from https://www.cigionline.org/articles/dark-net-should-be-shut-down-cigi-ipsos-global-survey-what-about-its-benefits