ABSTRACT

Title of Document: THE DARK INTERNET: AN EXPLORATION OF CULTURE AND USER EXPERIENCE

Jeremy Foust, Chariah Ghee, Matthew Hartung, Kathleen Hynes, Chong Li, Patricia Mandrich, Kymberlee McMaster, Jared Reibel, Kamilah Tadlock

Directed by: Jon Hoffman

Lecturer, Department of Communication

Our research sought to investigate the culture of the Dark Internet through a combination of cultural analysis and experiential learning. We split our research into three major portions: analysis of culture of the Dark Internet through the way it is viewed by various media outlets and on the Dark Internet itself; how the culture of the Dark Internet reacts in times of crises; and a comparison of the experience of the users of Dark Internet marketplaces versus users of traditional internet marketplaces. Our cultural analysis was accomplished through the use of textual coding; by coding the articles, forums, and pages that we were gathering, we were able to find and observe key commonalities in behavior and communication among the sources. We also went through the process of purchasing goods from both Dark Internet marketplaces and traditional internet marketplaces allowing us to compare the experiences in a variety of ways including: ease of access, ease of purchase, delivery time, etc. This research aims to provide further insight into the nature of the Dark Internet and open the way for future research into this ever-changing culture.

The Dark Internet: An Exploration of Culture and User Experience

By: Team DIRE

Jeremy Foust
Chariah Ghee
Matthew Hartung
Kathleen Hynes
Chong Li
Patricia Mandrich
Kymberlee McMaster
Jared Reibel
Kamilah Tadlock

Mentored by: Jon Hoffman
University of Maryland Honors College: Gemstone Program

Thesis submitted in partial fulfillment of the requirements of the Gemstone Program
University of Maryland 2017

Acknowledgements

Team DIRE would like to acknowledge many people for their continuous help and support throughout our time in Gemstone. We would not have achieved our goals without the love and encouragement of our families and would like to thank them for their constant support of our project. We would like to acknowledge our librarian, Eric Cartier, for his early guidance in our search for literature. We would also like to acknowledge our mentor, Jon Hoffman, for his support and guidance through the many trials and roadblocks that we encountered. Finally, we would like to acknowledge the Gemstone staff for their support throughout our time in Gemstone and their flexibility in dealing with our unconventional project.

Table of Contents

Chapter 1

An Introduction to the Dark Internet

1.1 Dark Internet

Though their reach seems to grow more limitless with every passing year, the average online search engine can only index and provide access to a small portion of all sites, data, and networks available on the internet. The most infamous sub-section of the internet that cannot be so indexed is the Dark Internet - networks that deliberately employ unconventional protocols, ports, and encryptions to reduce unwanted access and keep its users anonymous. The concept of browser anonymity attracts a variety of people looking to keep their identities private in any cyberspace interaction. As this technology continues to develop and expand, it is likely to transform society as any major development in exchange has throughout history. The powerful capabilities and rich culture of the Dark Internet are the result of numerous components that contribute to the overall anonymity it provides.

One of the Dark Internet's most recognizable tools is the Tor browser, the primary method for accessing sites on the Dark Internet itself. Among the many uses of the Dark Internet, 15.4% of its hidden services, meaning websites that are only available on the Dark Internet, are comprised of illegal marketplaces, creating a haven for the trade of illegal drugs (Owen & Savage, 2015). The online drug trade has been revolutionized by the Dark Internet as it offers mass accessibility and relative anonymity compared to conventional markets for secure transactions. Another important area that should be considered for analysis is the role of Bitcoin, the first online currency to attain widespread adoption (Miers et al., 2013). Bitcoin’s ability to anonymize trade means that it has found natural and widespread usage when used for illegal transactions. While the Dark Internet is a relatively new and complex development, understanding various

aspects of its functionality is the first step to creating valuable knowledge on the ways in which it affects society.

It should be noted here that there are several terms necessary for the understanding of this paper: Dark Internet (also known as Darknet), Dark Web, and Clearnet. To begin, the Clearnet is the term we will be using interchangeably with traditional Internet; these terms refer to the Internet that you use in your day to day life through traditional web browsers such as Google Chrome, Safari, or Firefox. The Dark Web refers to areas on the web that cannot be found using typical search engines, such as Yahoo or Google either because they are secured in some way (Everett, 2009). The Dark Internet, on the other hand, is composed of servers that are more difficult to connect to, requiring special browsers such as Tor (Everett, 2009). These special browsers are able to access websites available on the traditional internet, but Dark Internet websites cannot be accessed through the traditional internet. This means that while our definition of the Dark Internet does fall under the umbrella term Dark Web, our research relates more specifically to the Dark Internet, as the browser: Tor Network is the specific focus of our research. The Dark Internet in its entirety is a large forum of anonymous exchange in many forms and as it expands it will inevitably influence the future of society.

1.1.1 Structure. The Onion Router, Tor, was developed in 1995 by the Naval Research Lab as a model for anonymous internet usage (Dingledine, Mathewson, et al., 2004). The routing technology was then adopted by civilians to create Tor, which is described as a "circuit based, low-latency communication service"(Dingledine, Mathewson, et al., 2004). According to a study completed in 2004, layers of encryption are used to create circuits that can step from one anonymous source or node to another

(Dingledine, Mathewson et al.). When a user makes a request, such as entering a website into the address bar, that request is encrypted then sent to a node server somewhere around the world. That node decrypts one layer of protection from the message, and then sends the message to the next node in the sequence. After several of these steps, the message arrives at its intended destination. This process affords the user a high level of protection for both identity and location.

Tor was first created with the intent to protect U.S. intelligence agents working out of dangerous territories. In an article on the effectiveness of the Tor network, David Gingrich notes that the problem with this original strategy was that agents were still easily identifiable because the only traffic known to be moving through the Onion Router was coming from U.S. intelligence (2014). Therefore, in order to effectively hide themselves, the U.S. opened Tor to the public, creating a free internet service able to conceal the identities of all its users (Gingerich et. al 2014).

1.1.2 A brief history of Dark Internet markets. The online drug trade expanded as the Silk Road, an online marketplace accessible only on the Dark Internet, began to obtain media attention and elevated user success. Since it was hosted on the Tor Network, anonymity was guaranteed to users especially through the use of Bitcoin. In order to create a trusted and honest environment within the marketplace, both sellers and consumers were rated by each other to inform all users of their marketplace professionalism. Within a short period of time, the Silk Road had become one of the most popular online marketplaces.

On June 1, 2011, an article entitled “The Underground Website Where You Can Buy Any Drug Imaginable” was published on Gawker, greatly publicizing the soon-to-be

infamous Silk Road and the Dark Internet in general. The Silk Road, which was first founded in February of 2011 by Ross William Ulbricht otherwise known as “The Dread Pirate Roberts”, was described as a hidden website on the Dark Internet where users could anonymously buy a variety of drugs and other services. Initially, the Amazon-like marketplace went relatively unnoticed by the mainstream media, but its revenues eventually rose to over USD $1.2 billion in sales and USD $80 million in commission (Bartlett, 2014). According to Bloom, the article's aftereffects were profound; the number of Silk Road newcomers swelled to thousands per week, while U.S. Senators Charles Schumer and Joe Manchin III reported the Silk Road to the DEA a mere five days after the article's publication (Kleiman, 2013).

Although the DEA requested to have the Department of Justice (DOJ) seize the website domain, it became a difficult undertaking. In order for the Silk Road to be permanently taken offline, the DEA and DOJ needed to determine the identity of the site’s administrators and take them into custody. However, because the Silk Road operates on the Tor network, it was nearly impossible to identify the IP address and name of the site’s administrator who was operating under the pseudonym of Dread Pirate Roberts. After over two years, it took the combined efforts of the DOJ, Federal Bureau of Investigations (FBI), DEA and other agencies to identify Dread Pirate Roberts as Ross Ulbricht and eliminate the Silk Road. Simultaneous with Ulbricht’s arrest, the United States government conducted an attack on the Silk Road website. Throughout 2013, the FBI seized thousands of Bitcoin, at the time worth millions of USD, from Silk Road accounts, and ultimately shut down the entire website. However, the seizure of the Silk Road did not have the effect on users as the government would have hoped; fear of police

operations and government shutdowns failed to deter users and instead caused them to adapt and relocate to other marketplaces (Décary-Hétu & Dupont, 2012).

The sudden seizure of the Silk Road resulted in a demand for new marketplaces for its users. While the FBI hoped that the shutdown would heavily diminish online drug sales, it appeared that the opposite had actually taken place. Spearheaded by the new pseudonym, Defcon, the remaining administrators from the original Silk Road relaunched the site in November 2013 just a month after its shutdown (Buskirk et al., 2014). This revitalization was named Silk Road 2.0 and offered the same services as the original, but with the promise of improved security against government agencies. However, the new site encountered security flaws within its monetary deposit function, and, as a result, $2.7 million in bitcoin were stolen in February 2014. Administrators were able to use their commissions on sales to refund hack victims, with 50 percent being completely repaid as of April, 2014. Silk Road 2.0 was eventually shut down a year after its development, along with other major online marketplaces, as a result of efforts by government agencies. Blake Benthall, better known as Defcon, was arrested and charged for narcotics trafficking, money laundering, and online hacking.

Once the Silk Road and Silk Road 2.0 were taken offline, several other online marketplaces took action to attract consumer traffic. In an analysis conducted by Dolliver and Kenny in 2016, the Agora, Pandora, Evolution and The Cannabis Road marketplaces showed the highest increase in traffic after the Silk Road shut down, in addition to Cloud-Nine and Hydra. However, some marketplaces excelled higher than others; in terms of the most prominent Tor Network marketplace to purchase drugs, Agora was one of the leading sites to gain success after the shutdown of the Silk Road. After sampling 2,325

vender accounts on the Dark Internet, Dolliver and Kenny found that 67.2 percent operated on Agora, and 32.8 percent on Evolution (2016).

While the Silk Road and the Silk Road 2.0 were seized by the government, the shutdown of the Agora network was a self-imposed decision. On August 26, 2015, Agora's administrators announced on its site as well as the Reddit forum, /r/DarkNetMarkets, that they will temporarily take their site offline in an effort to increase the site's security due to a detection of unwarranted activity on their servers. Even though the administrators kept their online following updated through Reddit forums, they have not yet announced when the site will be relaunched.

When Agora was taken offline, the Dark Internet drug market took a major hit. Agora had become the largest site for drug trade with over 17,000 listings of drugs (Dolliver, 2015). In a recent study conducted by Carnegie Mellon researchers, it was estimated that the Agora marketplace made $150,000USD a day in sales in February 2015 (Soska & Cristin, 2015). At this time, Agora was the second largest online drug trade site, eclipsed only by Evolution. However after Evolution went offline in March 2015, most of the market share shifted over to Agora (Soska & Cristin, 2015).

According to Christin, a computer science researcher from Carnegie Mellon, during this lapse in major online marketplaces, lesser-known sites - such as Abraxas, Alphabay, and Nucleus - attempted to pick up the customers (2015). "I don't know who will be the new crowned king, but people will pick up the pieces. The demand is here and people aren't going anywhere. They want their drugs and people will find ways of selling to them" (Christin, 2015). Christin also states that these events should be taken as a security reality check for all of site owners and that "Tor is not a magic box that provides

you a cloak of invisibility, Harry Potter style."

Due to the increased notoriety the original Silk Road gained over the last few years, many Dark Internet users have stopped using the Silk Road brand. Only a month after the original Silk Road was seized in October of 2013, the Silk Road 2.0 was launched. However once the Silk Road 2.0 was shut down, copycats, with no link to the original staff and community members, created the Silk Road Reloaded in early January 2015. This site was not hosted on the Tor Network, but rather another anonymous Dark Internet browser, I2P.

More recently, someone renamed the marketplace Diabolus Market to Silk Road 3.0 (Kushner, 2015). The site's homepage reads: "Welcome to Silk Road 3.0. We are an anonymous, professional and peaceful marketplace selling all sorts of goods and services. I am honored to welcome you to our community." The site's unnamed owner also decided to take the original moniker of the Silk Road's owner and call himself Dread Pirate Roberts.

Even though the talk surrounding the arrests and seizures of the Silk Road and the Silk Road 2.0 increased the amount of traffic towards Dark Internet marketplaces exponentially, little interest has been shown in new versions of the Silk Road (Christin, 2015). Over the past two years, consumers of the Dark Internet markets have been shaken by the disruptions of nearly all of the popular online marketplaces. In the scramble of the Silk Road sites, Evolution and Agora shutdowns, many users have raced to lesser-known sites such as Abraxas, Amazon Dark, Black Bank, and Middle Earth. Subsequently, all of these sites have been taken offline.

Currently, as of March 2017, the most prevalent marketplace, Alphabay, is not

gaining any popularity among users. Members of Reddit's "Darknet Markets" community and Alphabay's Tor-protected user forums, accuse Alphabay of intermittently stealing users' bitcoins. However, even with all of the marketplace chaos, the online traffic has not been deflected back to "street" dealers. Christin states that the overall anonymous online drug trade fluctuates around USD $100 million a year regardless of government involvement or exit scams. Exit scams meaning when a market builds up trust so that people will use it and trust the market to hold their money during transactions and once the administrators of the market decide that they are holding on to enough money they go offline taking the money they were holding for vendor and buyer transactions. The resilience of Dark Internet marketplaces demonstrates its value as a subject of academic research.

1.1.3 Existing Research. There has been a surge in research on the subject of the Dark Internet in recent years. This surge is most likely due to the increasing awareness of its existence as well as the increased utilization of the Dark Internet. An overwhelming amount of current research focuses on the risks that the Dark Internet poses to society. The topics of said research range from deviance on the Dark Internet, drug sales, markets, terrorist recruitment, to child pornography. Other research topics consist of studies which aim to understand the technical processes of the Dark Internet, studies to understand the functioning of Dark Internet markets, as well as studies which look to comprehend the users of the Dark Internet. The following review will discuss in more detail the common topics of research on the Dark Internet, as well as the multiple approaches to studying it, in order to understand the general body of literature based on the Dark Internet at present and assess gaps in said literature.

As previously mentioned many sources among existing literature focus on the drug trade through Dark Internet markets. An example of such is the book, *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*, is a prime example of such a source as it describes the increased access of drugs and the consequent rise in the drug trade that Dark Internet markets provide (Martin, 2014). The author does actually point out that it is limiting to growing research to only study deviant activity on the Dark Internet, however a large portion of this book itself centers on such illegal activity. The book poses the question of whether cryptocurrency and the sale of illicit drugs on the Dark Internet is more or less harmful than the traditional sale of illicit drugs. Martin also addresses the inner workings of Dark Internet markets, the relationship between the cryptomarkets, and the state, as well as the question of how to police said drug trafficking (2014) .

In order to study Dark Internet markets, researchers have used qualitative methods of gathering and analyzing data from publicly accessible cryptomarket forums. Martin found that the majority of Dark Internet markets prohibit the sale of obviously harmful goods such as child pornography or contract killing (Martin, 2014). However, it must be noted that such illicit activities do happen, and have been magnified by the Dark Internet, an example of such is child pornography, which, with the guise of anonymity is easier to share, create, and view without legal repercussions (Martin, 2014). The various illicit products that are sold on the Dark Internet, even when prohibited by some markets, coupled with its ability to keep users anonymous, has created a perception that the Dark Internet's sole purpose is to facilitate illegal activity (Martin, 2014). The book expounds on the common misunderstood views of Dark Internet markets, which liken them to

villainy and absolute lawlessness (Martin, 2014). Martin explains further how these views are a result of media which tends to report on the most egregious of findings in order to garner attention from the public (2014). In order to differentiate between illicit activities on the Dark Internet and non-criminal transactions, the book introduces the phrase cybercrimes, as an activity that may happen on cryptomarkets, but is not synonymous with all cryptomarket activity (Martin, 2014). The author acknowledges the existence of different forms of cybercrime, such as drug trading, child pornography, and hacking, but also observes that when researchers solely focus on cybercrime it creates literature that underemphasizes other important characteristics of cyberspace.

Another example of a study that centers on illegal activity follows the numerous steps a Dark Internet market user would take in order to access a website, obtain drug information sourcing, and buy drugs (Van Hout & Bingham, 2013). The study also looked at motives for buying drugs over the Dark Internet (Van Hout & Bingham, 2013). The participant in the study who documented all of these experiences was recruited through a Silk Road chatroom (Van Hout & Bingham, 2013). The authors found that the community support and harm reduction provided by the Dark Internet, maximizes consumer decision-making and positive drug experiences, and minimizes potential harms and consumer perceived risks (Van Hout & Bingham, 2013). These positive drug experiences come first and foremost from the users' ability to search through user feedback from Silk Road in order to discern whether a site or product could be potentially harmful (Van Hout & Bingham, 2013). The user for the single case study looked over user feedback as a big picture, such as, if there are nine good reviews and one bad review, the user is able to assume the site is trustworthy. The safety that the user felt was

attributed to the anonymity that the Dark Internet provides and the subsequent transactioning without any of the risks associated with street drug sourcing (Van Hout & Bingham, 2013). Another community feature characteristic of Dark Internet market transactions is that the success of the seller depends on their reputation; this in turn is affected by the buyer's experience who will then report it through user feedback (Van Hout & Bingham, 2013). An important feature of the Silk Road and other Dark Internet markets is that the user information and understanding is facilitated by an existing host of experienced drug users, who have enough knowledge on the subject to discern which sites and products are trustworthy (Van Hout & Bingham, 2013). The authors concluded that a combination of user research, a nested support system, which other users and their feedback creates, and anonymity allowed for a safe and positive drug buying experience for the user of the single case study. Though, this source provided ample information about how a Dark Internet market operates, even showing how safe it can be, the authors still only focused on the actions of drug buyers and vendors.

Yet another study on the Dark Internet market Silk Road conducted its research over a more broad time frame in order to collect information on the types of goods sold, as well as the revenues generated by both Silk Road operators and sellers (Christin, 2013). The study used mandatory buyer feedback reports in order to measure sale volumes, and estimate the dollar amount of sales. The author grouped the top twenty most popular categories of products sold on Silk Road with marijuana ranking as number one (Christin, 2013). The majority of the top twenty was drugs, the only items that were not drugs were books (ranked fifth), money (ranked eleventh), erotica (ranked thirteenth), and digital goods (ranked twentieth) (Christin, 2013). Additionally, the study assessed

customer satisfaction with the marketplace, noting that transactions involve excellent feedback from buyers (Christin, 2013). With this information Christin states that the feedback system appears to ensure seller reliability (2013). The article concluded that the majority of items sold over Silk Road are drugs, the user base is an international community, and that the number of sellers is increasing (Christin, 2013). Once again, this study that not only makes drugs the focal point of the research but also only chose to analyze one Dark Internet market, Silk Road, when there are numerous markets on the Dark Internet and little research on any of them.

There are articles, which deviate from the focus of drugs over Dark Internet markets, but many of them still center on illegal activity. An example of such was a study, which discussed a predicted increase in the illegal sale of wildlife through the Dark Internet (Harrison, Roberts & Hernandez-Castro, 2016). In order to understand the extent of the exotic wildlife trade on the Dark Internet, the researchers involved in the study archived numerous individual posts, searching each for keywords pertaining to wildlife trade and the trade of illegal elephant ivory (Harrison, Roberts & Hernandez-Castro, 2016). The results were compared to the amount of hits shown for keywords associated with cannabis, cocaine, and heroin in order to comprehend the extent of wildlife trade versus illegal drug sale (Harrison, Roberts & Hernandez-Castro, 2016). The results found very few mentions of illegal wildlife sale over the Dark Internet and attributed this to a lack of law enforcement over the clear internet, meaning that wildlife sales work successfully enough over the clear internet without government intervention that sellers do not feel the need to use the Dark Internet (Harrison, Roberts & Hernandez-Castro, 2016). This article chose to study an illegal activity that is not even very prevalent on the

Dark Internet (Harrison, Roberts & Hernandez-Castro, 2016). However, it seems that the authors expected increased wildlife sales over the Dark Internet most likely due to their perception that the Dark Internet is a haven for illegal activity. The study itself even uses drug sales as a point of comparison to wildlife sales, invoking the idea that the authors also assumed that drug sales would be high (Harrison, Roberts & Hernandez-Castro, 2016).

Another article, which may deviate from the well-researched topic of drug sales over the Dark Internet, instead discussed the increasing challenge of combatting crime with the rise of the Dark Internet (Vogt, 2017). The author goes on to describe the struggles of defining privacy on the Internet and its pressing implications for the current U.S. framework of privacy and the law (Vogt, 2017). The author additionally examines the inalienable right of privacy in the United States and considers how it must be applied to the Dark Internet as it becomes a greater part of everyday society (Vogt, 2017). The author advises the need for a continued system in which, with probable cause and warrants, the government retains a lawful avenue to access encrypted data, in order to lawfully incriminate those who have broken the law (Vogt, 2017). Though, this study is different in that it does not specifically center on drugs, Silk Road, or Dark Internet markets in general, the author still set out to speak on the illegal activity that does happen on the Dark Internet and how to deal with it (Vogt, 2017).

It is clear that there is a running perception of the Dark Internet as a predominantly market centered community, interested in the buying and selling of illegal activities and products, and the narrow scope of published literature reflects this. There are a few studies, which are interested in the culture of Dark Internet users, especially

those who engage in illegal activity. However, the compilation of literature overall concerns itself majorly with policy, illegal activity trends, and law enforcement. This focus leads to gaps in the research as most studies focus on illegality and deviance, rather than the general user base community.

As the Dark Internet grows and becomes a bigger part of everyday society, researchers of the subject would benefit from focusing on its users as a whole. This does not mean yet another study on merely the users who buy or sell drugs, but instead, the general user base and what attracts them to the anonymity of the Dark Internet. As its number of users increases daily, it becomes increasingly pertinent for us to analyze the culture of this tight knit community in order to comprehend the reasons why anonymity has become all the more valuable in our modern society as well as its implications on society itself.

1.2 Bitcoin and Cryptocurrencies

Although the true identity of the developer of the popular online cryptocurrency, Bitcoin, is unconfirmed, it is theorized that Bitcoin was invented by a group of anonymous users who are referred to as Satoshi Nakamoto, in October 2008 (Nakamoto, 2008). A study conducted by author William J. Luther in 2013 tried to model the failure to rise to wide stream popularity in Bitcoin and other cryptocurrencies despite their promising features in the technology age. In this journal, Luther describes how Bitcoin, and other cryptocurrencies, utilizes cryptography in order to ensure the security of online transactions prevents users from spending the same digital notes more than once, governs and monitor the supply of these notes in circulation, and ensures the anonymity of those who choose to use it (2013). This utilization of cryptography to ensure the security of

online transactions is commonly referred to as the blockchain. Blockchain technologies utilize an everchanging peer-to-peer database of records, which in the case of Bitcoin, record and place a stamp on every transaction. Additionally, the "stamp" for every transaction is based off the "stamp" of the previous transaction, making it that all transactions and "stamps" are in a chronological order. Each "stamp" in the database adds a new block to the chain, allowing for very rapid transactions that cannot be modified without making major changes to the whole blockchain. Thus, the process of making major changes to the blockchains is impossible, for a retroactive change made to a block will also have to make change to the blocks preceding it. Essentially, a change cannot be made to a single block in the chain without changing the entire chain in itself. This has allowed the creation of numerous anonymous marketplaces on the Dark Internet, while also being adopted as a form of currency in many well-established Clearnet marketplaces, the term Clearnet being used to refer to the traditional internet that is used through Chrome, Firefox, etc.. To date, the majority of major governments have yet to recognize Bitcoin or any other cryptocurrencies as legitimate form of currency that can be used for official transactions. However, since its creation Bitcoin and other cryptocurrencies have become prominent forms of anonymous and untraceable payment on both the Dark Internet and the Clearnet, drawing the attention of the public and academics alike.

Previous research conducted on Bitcoin and other cryptocurrencies have focused on why Bitcoin is so secure as a form of payment, and why that has lead to increased popularity. Specifically, researchers have identified that the blockchain technology that Bitcoin utilizes allows it to be a very secure form of payment, that doesn't need a central authority or group of administrators to recognize and approve every transaction.

Blockchain technology has allowed Bitcoin to be used in large volumes on online, anonymous markets, without many major faults. The development of blockchain technology and Bitcoin go hand-in-hand, as for Bitcoin and other cryptocurrencies cannot exist without the novel development of the blockchain technology (Nakamoto, 2008).

The blockchain technology that Bitcoin and other cryptocurrencies has become so popular, that many researchers believe that it will become a widespread technology that will eventually change to the global economic landscape. A review journal written by Sarah Underwood in 2016 recognized the novel technology of blockchain in the form of Bitcoin, and hypothesized of the potential other uses of the technology. In this journal, Underwood discusses how not only has blockchain popularized Bitcoin already, but the potential improvements on the technology could possibly cause Bitcoin to become even more widely used. Additionally, the author points out how blockchain can "revolutionize industry and commerce and drive economic change on a global scale because it is immutable, transparent, and redefines trust, enabling secure, fast, trustworthy, and transparent solutions that can be public or private" (Underwood, 2016). The journal goes on to discuss how the basis for blockchain technology can go on to be the basis of applications of creating, utilizing, and validating secure data in many different industries throughout the globe. For example, Underwood points out in her review that there are potential businesses that are attempting to adapt the blockchain model in order to expedite financial transactions while also increasing security. A plethora of new startups and other organizations are committed to utilizing the blockchain technology in order to help it become mainstream in many different industries. In addition, these new organization have had very successful starts, with many major companies investing in

them. Overall, the very secure and the very rapid speed of transactions of the blockchain network have propelled it to become a readily utilized technology. However, researches still want to understand how Bitcoin is utilized as an asset on online, anonymous communities.

In addition to the novel blockchain technology that has initially popularized Bitcoin, in recent years, many major developments have launched Bitcoin to attract major attention from the public and the academic community. These developments include, but are not limited to, the Winklevoss twins attempting to establish an official exchange trade for Bitcoins, Republican presidential candidate Rand Paul accepting campaign donations in the form of Bitcoin, and many major Clearnet marketplaces accepting Bitcoin as a form of payment. Since its rise to prominence, a plethora of studies have been completed to qualitatively and quantitatively determine the value and function of cryptocurrencies. The majority of academic studies pertaining to Bitcoin are focused on two distinct major areas. The first effort has been to understand the relatively volatile value of Bitcoin compared to established and recognized forms of currency such as the United States Dollar. The second effort is an attempt to dissect and explain the unique attributes of Bitcoin that have helped it become prominent, and provide potential for it to become a well-established form of currency in the future. In addition to this effort, academics have made attempts to qualitatively understand the consumer experience of using cryptocurrencies on an anonymous Dark Internet marketplace.

The value of a single Bitcoin in United States dollars has been known to fluctuate greatly not only over time, but also over the many marketplaces that accept Bitcoin as a form of payment. Many studies have attempted to examine factors that determine the

value of a Bitcoin over time among different Dark Internet marketplaces. One study attempted to quantify the exchange rate between a Bitcoin and United States dollars, and provide reasoning behind the changes in value of a Bitcoin (Li and Wang, 2017). Li and Wang found that over a short period of time, the value of a Bitcoin was heavily dependent on real world market factors that also affect the value of the United States dollars and other currencies. Specifically, it was found that significant positive or negative correlations, with very short lag periods, were found between the value of Bitcoin and the United States money supply, the United States interest rate, and the total value of transactions. The authors of this study attribute the short-term changes in Bitcoin value with these factors upon the plethora of economic literature that finds that an asset's value is highly dependent on exchange price dynamics. The confirmation of these findings by other research can be beneficial for if more information is found on why the value of Bitcoin is so volatile, and what is causing it, then that information can help people who want to purchase Bitcoin while making an uniformed decision on whether the value of the Bitcoin will rise or fall in the short term.

However, the findings from other studies do not align with those previously mentioned. One study attempted to perform the efficient market hypothesis on Bitcoin and found that it failed (Nadarajah and Chu, 2017). The efficient market test determines if an asset's value, such as Bitcoin, can be determined by the available information on the asset. By failing this test, it can be argued that the value of a Bitcoin cannot be quantified from external factors. Last, studies have tried to examine why the value of a Bitcoin varies over different Dark Internet marketplaces, and apply reasoning for this variance (Pieters, 2017). This study analyzed a large number of markets that account for 32% of

all Bitcoin transactions by volume, and found that the value for a Bitcoin on anonymous marketplaces, like those on the Dark Internet, tends to deviate greatly from the average value of a Bitcoin. The current set of research that is aimed at establishing the factors that affect the value of a Bitcoin, both over time and among marketplaces, is difficult to define due to Bitcoin's nature in how its value relates to its use.

In addition to attempting to establish the value for Bitcoin, researchers have also focused on establishing how Bitcoin can be utilized which has allowed it to rise as the most popular form of currency on Dark Internet marketplaces. Researchers have attempted to do this using qualitative methods that examine the role of Bitcoin in an anonymous marketplace, and also be gaining experience using a Bitcoin on a Dark Internet marketplace first hand. One method of how Bitcoin is utilized on anonymous marketplaces that researchers have hypothesized as to why Bitcoin has become popular on anonymous marketplaces is that it can easily be held by the marketplace itself to solve peer-to-peer disputes. One study examined that a certain feature Bitcoin possesses that makes it desirable on anonymous marketplaces, is that the Bitcoin can be held in escrow by a marketplace, while a transaction is occurring between a vendor and customer (Ortolani, 2015). Although this attribute is not unique to Bitcoin in itself, being able to hold a cryptocurrency in escrow without a recognized financial institution or some other middle man has expedited and secured transactions on the Dark Internet. By doing this, it allows purchasers and vendors on the Dark Internet to conduct business without having to spend large amounts of time making sure the transaction is handled as agreed upon. This utilization of Bitcoin is especially helpful when there is a disagreement between a vendor and a customer; the Bitcoin will be held by a third party or Marketplace until an

agreement is reached between both parties. This specific feature helps prevent scamming by vendors, which makes the Bitcoin a desirable currency for customers on Dark Internet marketplaces, which also allows it to be a more secure form of payment on the Dark Internet.

The study of this utilization has been validated by other studies where the researchers have found that Bitcoin it utilized much like tangible forms of payment (Koblitz and Menezes, 2015). This study, much like the previous, examines how the transactions on the Dark Internet using Bitcoin share key similarities to real world transaction between two parties where a bank or other financial institution is involved as a mediator. The study concludes that the increased level of security via blockchain technology using Bitcoin is what makes it viable and popular on Dark Internet markets. Along with identifying the major beneficial features of Bitcoin that make it desirable, researchers have tried to use Bitcoin on Dark Internet marketplaces in order to gain a qualitative understanding through first-hand experience (Van Hout and Bingham, 2013). Overall, the studies that attempted to qualitatively understand the features of Bitcoin in relation to its popularity on anonymous Dark Internet marketplaces have seen success, but additional research is needed to confirm these studies. It can be stated that the increased security of Bitcoin and other cryptocurrencies, along with how the Bitcoin can be utilized, on online, anonymous marketplaces has been beneficial in its rise to prominence on the Dark Internet.

1.3 Online/Digital Culture

The majority of existing literature on the topic of Dark Internet culture and communities largely focuses solely on that of the illegal drug trade, i.e. of the Silk Road.

While this community of users poses significant implications for the Dark Internet and online marketplace interactions as a whole, they are not the whole of the social and economic data worthy of further study and consideration. Silk Road's founder himself, Ross Ulbricht, described the Dark Internet in a court statement as a practical social device offering a variety of functions, claiming its value as a tool "giving people the freedom to make their own choices, pursue their own happiness, how they saw individually fit" (Ulbricht, 2015). The Dark Internet and its vast forums facilitate "a shared experience of personal freedom... where open discussions about stigmatized behaviors [are] encouraged and supported" (Maddox et al., 2015).

The Dark Internet has provided a home to a new kind of online culture due to its virility as an alternative social network. Gehl compared the practicality and user reactions to multiple forms of social networks on both the Dark Internet and the Clearnet (2016). His research concluded that Dark Internet culture differs greatly from that of those in the mainstream, such as Facebook, likely as contemporary social networking sites are associated with the use of real-world identities and, perhaps because of this, are considered to be a safe and acceptable online practice (Gehl, 2016). On the Dark Internet, however, such formalities and identification information submission are not observed, and the further obstacles placed by the Tor router enable this enhanced anonymity. This allows users to not only engage in business transactions but also engage in interpersonal interactions under the veil Tor's IP address encryption provides.

The enhanced anonymity provided by the Dark Internet has accelerated the development of a new digital culture. Under a cloak of relative anonymity, Dark Internet users are granted a higher level of immunity from repercussions for their actions online,

prompting them to engage in social interactions and communication they may not have otherwise. Eric Jardine, a researcher from the Center for International Governance Innovation (CIGI), explains that this social phenomenon is not unique to the Dark Internet, but is characteristic to anonymity itself: "Anonymity provides space for people to think and voice opinions that are against the grain" (Jardine, 2015). This fact has proven especially significant for citizens under repressive government regimes accessing Tor for the sake of voicing their opinions without fear of censorship or government surveillance. Under such conditions of anonymity and little apparent risk of criminal repercussions, unique online cultures have developed, honing what is arguably the purpose and meaning of the internet in its most raw form, described by Australian researchers (Maddox et al., 2015) as "to change society through radical reconfiguring of the relations of power, information and exchange".

The lack of face-to-face interaction with a familiar figure does not inhibit the formation and maintenance of interpersonal bonds, as sociologists might have suspected. On the contrary, Postmes et al. researched the effects of anonymity on group behavior argue that anonymity, especially in a visual context, diminishes the relative importance of interpersonal concerns in favor of a focus on the known or emergent characteristics of the group as a whole (2001). In fact, they discovered that anonymity "...increases the salience of group identity and group identification, thereby enhancing the group's influence" (Postmes et al., 2001). Social identities and the sense of belonging to a group is particularly salient on the Dark Internet, due partly to the visual anonymity the Dark Internet provides, which obscures physical features and interpersonal differences and thereby "diminishes the relative importance of interpersonal concerns in favor of a focus

on the known or emergent characteristics of the group as a whole" (Postmes, 2001). Therefore, anonymous users on the Dark Internet—whose appearance as well as name, location, and IP address is hidden—are favored to exhibit group identification and increased group influence as opposed to salient, unique individual behavior independent of a group or community. Since social groups cannot only develop, but flourish under the guise of anonymity, it can come as no surprise that a unique, legitimate community of anonymous users have established their own online culture within the Dark Internet. The repercussions of this rapidly-developing online community have not yet been studied in great detail, even as the subject becomes all the more relevant as it relates to anonymous social interactions on the traditional internet.

To the average person, the topic of browsing and communicating on the Dark Internet is met with ignorance, fear, or a combination of the two. During our research, we experienced this effect several times firsthand; when telling friends or family the research we were aiming to do, they often asked what the Dark Internet was and/or then proceeded to worry for our safety in conducting this research. For Dark Internet users, however, researchers have observed that individual users' behavior displays heightened salience in identifying with the social structures available to them; groups, forums, and chat rooms through an anonymous lens produce meaningful personal interactions between users, who could be typing from anywhere in the world. The value of anonymity on the Dark Internet allows for its headquarters for whistleblowers, political dissidents, and citizens living under oppressive, authoritarian governments. Obviously, enhanced anonymity has not produced a utopian digital world merely comprised of commerce and positive human interactions. Despite the obvious social advantages the Dark Internet provides, Reicher

determined that enhanced anonymity not only permits for less social inhibitions resulting in unresponsiveness to social norms and standards, leading to antinormative behavior (Reicher et al., 1995). Therefore, we must further the cultures and social structures native to the Dark Internet as areas of study as this social phenomena is arguably one of the most new and current social structures and its development has skyrocketed past preconceived notions of the Dark Internet and its uses. What originated as the development of encrypted communication for the Naval Research Laboratory has expanded in size, scope, and functionality well beyond its original intentions.

1.4 Anonymity Online

Whether in the office or at the store, the threat of social stigmatization holds most people back from acting without inhibition. Each day, countless people abide by that little inner voice governing their behavior and choices. But when the connection between person and action gets blurred, to what extent does this restraint disappear? This is a question researchers have asked with an increasing frequency since the birth of the internet. As a platform, the internet has provided researchers countless opportunities to see the impact that differing levels of anonymity has on human interaction. From comment sections to forums, academics have scoured the internet to study the impact of anonymity on human interactions.

One area of academic interest is the impact of anonymity on disinhibition. The online disinhibition effect refers to the tendency of individuals to "act out more frequently or intensely" while online than they would in person (Suler, 2004). This behavior can be either positive (benign disinhibition) or negative (toxic disinhibition). In this paper, (Suler, 2004) identified six different factors that led to this effect, including

dissociative anonymity and invisibility. It was also noted that this disinhibition is not the emergence of the "true self", but as another side to the same personality brought to light by the new environment (Suler, 2004). A person's core beliefs and principals remain untouched, while certain personality traits simply become more pronounced, and others less so. However, recent research has linked another factor to the appearance of toxic disinhibition. In their paper, Lapidot-Lefler and Barak cite the lack of eye-contact as the chief contributor to toxic disinhibition, surpassing both dissociative anonymity (lack of personal information) and invisibility (lack of defining characteristics) (Lapidot-Lefler and Barak, 2012). To better define this interaction, Lapidot-Lefler and Barak proposed a broad-scope concept of online sense of unidentifiability. This includes the concepts of anonymity, visibility, and eye contact while also noting that an individual's perception of his or her sense of unidentifiability impacted his or her online interactions.

While not immediately related to anonymity, the concept of bad samaritanism has some interesting implications with relation the online marketplaces. Bad samaritanism is the liability of an individual who fails to provide aid in an emergency situation. Polder-verkiel explored the concept of bad samaritanism online by comparing the case of Abraham Biggs, a young man who committed suicide in 2008 with approximately 1500 people watching via his webcam to the fatal assault of Kitty Genovese in 1964 during which 39 neighbors supposedly looked on without intervention. (Polder-Verkiel, 2012) concluded that perceived reality of the situation, rather than anonymity, had the largest moral relevance in both online and offline interactions. There is a noticeable disconnect between what happens on the internet and what happens in "real life". Polder-Verkiel noted that this disconnect can stem from two questions: is the image being viewed real or

has it been altered, and is the image happening in real time or is it on a loop? With these two questions in mind, many viewers don't respond to a threat until they can be certain what they are viewing is real. While not as extreme as murder or suicide, parallels can be drawn between these cases and those who browse Dark Internet marketplaces. To what extent are those who visit marketplaces that sell illegal drugs even if they don't partake in those illegal activities?

One last area of interest is the impact of anonymity on online discussion. As news sources are moving to a digital format, there are more opportunities to post opinions while withholding their identity. A common view by academics is that allowing anonymity in these posts decreases the civility shown by the users. In his study, Arthur Santana analyzed the comment boards of news articles about immigration that allowed both anonymous and non-anonymous postings. Santana found that 53 percent of comments posted anonymously were uncivil, compared to 28 percent when posted non-anonymously (Santana, 2013). However, further studies have found that anonymity may not be a key factor in civility. Janne Berg further expanded this line of research to see if the highly controversial nature of the article had a significant impact on the civility. Contrary to prior research, (Berg, 2016) found that anonymity did not have a major negative impact on the quality of discussion. Rather, the controversial or polemic nature of the topic had a much larger impact on the discussion quality, and that anonymity "might have received too much blame for the low quality of political discussion online". Many earlier studies disregarded the content of the articles selected in their studies, attributing any results solely to anonymity. By taking this additional variable into account, Berg highlights the tendency of many researchers to focus on anonymity (the

lack of personal information) rather than exploring the possibility of more contributing factors.

Academic discussion of anonymity online has seen an increased relevance in recent years. Yet even with the added attention, it has been difficult to pin down the exact impact of anonymity on online discourse. With each new study, for each question that is answered, two new ones come to light. When conducting research on a platform such as Tor, which prides itself on high levels of anonymity, it is vital to look at any impact that anonymity might have on the discourse produced by users.

1.5 The Gaps in Research

Despite numerous advances in the Dark Internet's popularity and mainstream usage, specific parts of it remain a great mystery to most. In particular, bitcoin usage and the marketplaces on the Dark Internet continue to suffer from lack of study. Further research is required in order to provide documentation for information and make it readily available. This needs to be done so its potential benefits can be exploited, and possible threats avoided or mitigated. The mystery surrounding these specific parts of the Dark Internet, from the average person's perspective, is not unwarranted, as gaps in existing research of these specific parts leave knowledge on the topic with many unanswered and unexplored questions.

The Dark Internet's massive amount of data has proven to be challenging for researchers to explore and exploit due to technical challenges that arise when attempting to locate, access, and index available Dark Internet data (Rocco et al., 2005). Various specialists have explored the development of possible research tools, which would enable any web-based information-seeking individual to be able to navigate the Dark Internet

with ease in order to gain access to the vast masses of data available and determine the relevant data of their choosing. Prototypic methods of achieving these aims have been developed, such as the DynaBot, which aims to circumvent the difficulties experienced while operating under the Dark Internet by a systematic method of matching, probing, and ranking discovered sources (Rocco et al., 2005). The DynaBot, which utilizes a service class description-matching module and a source-based analysis module for probing and ranking, still requires further research devoted to its enhancement in order to successfully operate as an efficient method of Dark Internet data extraction, data which includes but are not limited to: news-related information made unavailable by government or corporate censorship, political discussion, and access to online markets. Increased ease and accessibility to data of the individual user as the result of some developed information-sorting method would likely result in a great increase in Dark Internet usage, allowing more people to access information that remains unavailable on the public internet.

Our team will attempt to fill a crucial gap in the current research of the Dark Internet by analyzing the use of Bitcoin and other cryptocurrencies and their overall effectiveness and usage among online marketplace users. As of right now, significant studies have already been conducted on bitcoin and their value. We plan on building off of these studies in order to create new knowledge specifically on how bitcoin affect transactions on the Dark Internet. All transactions on Dark Internet Marketplaces require that some type of cryptocurrency be used instead of recognized currency, and there is a lot to be researched on how this affects the large amount of transactions that occur daily on the Dark Internet.

Although previous research has already been done to analyze specific groups of people such as the case study done on cyber terrorism by Chen et al. in 2008, our group could adapt their methods in order to study the exact groupings of individuals who use the Dark Internet and also establish knowledge in the public about the topic and use by the general public. Pre-existing analyses of different, but similar, online marketplaces such as the Silk Road could be taken advantage of as resources to adapt to our research goals of understanding how different levels of anonymity affect the behaviors of users on the Dark Internet. In order to take it one step further, we can compare the user interactions of Dark Internet marketplaces to other competitive online marketplaces such as Amazon to see how behaviors on the Dark Internet vary from the public internet where there is no anonymity at all in order to create a bridge between the Dark Internet and the Clearnet.

Textual analysis of communication on the Dark Internet can be directly compared to communication using conventional browsing. In addition, we can gain knowledge on the communication norms of Dark Internet communities. As a prominent example, marketplaces such as the Middle Earth have thriving forums where users can congregate to discuss the site, its services, and other activities specific to the Dark Internet.

Additional gaps in research (that are not solely exclusive to the Dark Internet) exist due to the fact that interactions are taking place over a digital medium. One of these major differences between online and face-to-face communications is the lack of a shared physical area where interaction takes place. This results in the changing of social boundaries, such as the difference between personal and mass communication or the distinction of time at home as separate from time at the office. Users can post messages

in secure private locations, but can communicate on an open public message board. This hybridization of the public and private spheres (Arendholz, 2013) creates new social spheres separate and apart from real life contexts. The nature of online communication enables people to feel anonymous but also connected to a heterogeneous global village. Since users feel that their interactions cannot be traced back, they can communicate on a personal level to a completely anonymous public. This is also a result of the ease in registering or leaving online communities, which makes online communication perceived as having less social obligations.

Chapter 2

Cultural Analysis of Texts

2.1 Introduction

Communication and culture are linked in such a way that one cannot be understood without the other. Communication provides the guidelines to learning what behaviors are appropriate in a specific society (Jandt, 2015). Therefore, in order for a culture to uphold its beliefs, it needs a channel to communicate through. The channel through which communication is achieved can reflect upon the character of the culture. Focusing on the Tor network as a society, we can form conclusions about the society's culture through user communication (Jandt, 2015). Also, in order to understand a culture's reaction to events and crises it is important to first understand the ongoing everyday day culture (Kiesler, 2014). Within any given society, there will be at least two subcultures with similarities and differences in how they behave and interact (Peppas, 2001). As we have grouped users of the Tor Network as a society of its own, we anticipate that several distinct sub-cultures may arise by observance of users' behaviors and language. As we analyze the content of respective forums, we hope to learn more about faithful users of these marketplaces and the vast drug underground culture that is involved. We seek to gain valuable research on topics such as the operation and ideals of these sites.

Our goal is to answer the following question: what cultural themes are present and how do their expressions affect the dynamics of the Dark Internet? We hypothesize that the increased levels of anonymity provided by the Dark Internet allow users freedom from repercussion; therefore users will more likely display anti-normative behaviors in contrary to the powers that be than users of message boards over the public internet.

2.1.1 behavioral coding and coding analysis. In a multi-national and cross-

cultural virtual platform, it is important to study the impacts of the knowledge sharing process. There have been endless studies on how national cultural values affect implicit and explicit knowledge sharing processes. But how can researchers study cross-cultural mass communication when each member of the community does not explicitly identify with a national culture? The key to answering this question is by studying the development of the Dark Internet culture by way of communication.

In order to study a culture's communication, this project will apply behavioral coding to textual communications. Sometimes referred to as "interaction analysis", this method is a major tool in evaluating the overt behaviors of the subjects. This way, it is possible to collect and interpret qualitative data quantitatively. Because self-reporting is not possible, direct observation of overt written behaviors is essential to our research question.

2.1.2 culture effects. According to Bibb Latane, there is the potential for cultures to be run by a dynamic social impact (1981). In this theory, Latane proposed that shared habits and ideas produce concrete manifestations of a particular culture. More specifically, cultures can be viewed as a society that is a self-organizing, complex system composed of interacting individuals, each obeying the norms and principles of the specific social impact (Latane, 1981). This theory contains propositions that measure how cultural elements and social structures emerge from individual experience and everyday interactions.

One of the previously stated propositions is that individuals differ. Humans differ with respect to demographic, physiological, and psychological variables such as age, social status, intelligence, and temperament. Many of these differences can be affected by

social influences such as values, cognition, and habits. These factors all determine how people react toward each other and the world. (Latane 1981) notes that a particular group of differences include characteristics that can form an individual's credibility. This is essential in the Dark Internet, in which the majority of the community remains anonymous. A person's influence can potentially become a shaping factor when determining subculture norms.

2.1.3 comparative information. Once our research question has been defined, the behavioral coding can begin by determining a measurement and analytic plan. Fortunately, there are coding schemes that address these specific questions. However, since behavioral coding can be a complex and time intensive process, the challenge lies within refining the coding schemes in order to produce the most relevant results. The most basic steps of any coding schemes are determining who, what, when, and how to record behaviors.

First, it is important to determine whose behavior is relevant to answering any research question. Once the subjects are determined, the next step is to determine what behaviors are of interest. Behaviors can matter for its own sake or because it is representative of another construct (Yoder & Symons, 2010). Once researchers know what behaviors to observe, they must identify the period of time they should be observed. Depending on the behavior, the observational period should be altered to efficiently measure the frequency and duration rates of the behaviors (Riley-Tillman et al., 2011).

Last, researchers need to be aware of how the behaviors will be recorded. Researchers must be the least intrusive as possible in order to prevent impacting the data recorded. Observations can potentially be affected by reactivity, which is the change in

behavior as a result of the observation itself (Harris & Lahey, 1982). However, textual analysis requires no interaction with online users, being completely unintrusive, making this issue irrelevant.

Once the process of the behaviors has been set, the coding manual needs to be scored. Coding systems are usually composed of a combination of nominal codes and rating scales. This is what translates qualitative data into quantitative. Coded data can be interpreted using inferential statistics that can appropriately analyze behavioral rates and proportions (Fleiss, 1973). It is evident that behavioral coding can be a complex, however establishing a refined approach can allow researchers to address research questions in a way that effectively reflects the behaviors of a culture.

2.2 Methodology

Websites that are accessed through both the Dark and conventional internet fall under the following three varying levels of anonymity: (1) identifiable, (2) pseudo-identifiable, and (3) non-identifiable. In an (1) identifiable level of anonymity, a user's name is linked with the account in connection with personal information (i.e. Facebook). In a (2) pseudo-identifiable level of anonymity, a username is used. They are identifiable by this self-made tag, but there is no connection to personal information (i.e. Reddit). Finally, in a (3) non-identifiable level of anonymity, the site does not require users to use any form of identification. This distinction is significant because the varying levels of anonymity allowed us to observe behavior from users experiencing varying levels of anonymity on the website on which they are participating.

We first identified six sites to study by using the previously stated levels of anonymity. Three sites will be taken from the conventional internet and three sites will be

exclusively for the Tor Network (.onion sites). Additionally, all six sites needed to meet the following requirements: contains a blog or consistent posting of articles, topics must discuss controversial political topics (i.e. abortion, terrorism, current events), and allow for users to leave comments.

There will be samples of data in the form of text from each of the six sites. Then, by following coding system developed by Boykin, Tyler and Miller, we will code the language used in the text. The coding system will categorize the dynamics involving the cultural themes and behaviors of the users of the Dark and conventional internet. There are ten types of behaviors that are assumed to be present on the internet: movement expressiveness, verve, affect, orality, communalism, individualism, competition, object orientation, priority placed on cognition over the display of affective expression, and maintenance of a bureaucracy orientation (Boykin, Tyler, & Miller, 2005).

The first cultural themes used to code the language, movement expressiveness in terms of the Dark Internet, appears in the form of rhythm through speech patterns (Boykin, Tyler, & Miller, 2005). Verve refers to the receptiveness to high levels of stimulus meaning Dark Internet users' focus on and reaction to events, such as a market shutdown, and the affect cultural theme relates to the emotional response to such events (Boykin, Tyler, & Miller, 2005). Orality manifests in knowledge gained and passed on through word of mouth (Boykin, Tyler, & Miller, 2005). Communalism relates to the feeling of duty towards the Dark Internet community, while individualism refers to the feeling of autonomy by the user (Boykin, Tyler, & Miller, 2005). Competition has to do with a person's need to do better than their peers (Boykin, Tyler, & Miller, 2005). Object orientation involves the feeling of positivity in response to objects, which evolves into an

individual's association of self-value with material possessions (Boykin, Tyler, & Miller, 2005). Priority placed on cognition over the display of affective expression is in contrast to the cultural theme of affect; it refers to an objective and rational reaction to events (Boykin, Tyler, & Miller, 2005). Bureaucracy orientation relates to a focus on structure and rules with an impersonal approach to relationships and events (Boykin, Tyler, & Miller, 2005).

For our purposes, we evaluated texts using the results of our behavioral coding to make up the basis of our interpretation of the sources' view of the culture of the Dark Internet. The texts were accessed from the following sources: Silk Road, The Hub, Intel Exhange, Reddit, Wired, Motherboard, and Huffington Post.

2.3 Results and Discussion

2.3.1 Dark Internet forums – Silk Road

The Silk Road, arguably the world's most infamous online marketplace, was not entirely unlike a marketplace on the Clearnet. It was a fast-paced, constantly changing market housing many diverse industries that are awash with communication and commerce at every hour of the day. Users from seemingly every corner of the world gathered on the encrypted site and its forums to sell, buy, and discuss their latest transactions, as well as Dark Internet-related current events. While both have since been taken down, the Silk Road and Silk Road 2.0 stood for years in defiance of the best efforts of government organizations.

In the midst of countless scandals and obstacles, the Silk Road and Silk Road 2.0 gave birth to a whole new kind of online community. The millions of daily interpersonal interactions between users are not solely limited to the buying and selling of goods; but

momentous social phenomena was observed as our team was able to study Silk Road 2.0 users demonstrating extremely high levels of the behavior communalism and loyalty to their fellow users, both buyers and sellers. On the Silk Road Service News Forum, a thread entitled “Free Ross!!” with 49 comments inspired many reactions of communalism and affect when regular users of the marketplace jumped to the defense of its founder, Ross Ulbricht, after one anonymous commenter had posted, “Why help someone who supports the drug trade and organized crime?”. Highly emotional responses were posted to this specific commenter immediately, as many users were both affectively enraged that someone would describe Ulbricht in such a way, especially while in the very same moment using the Silk Road for whatever reason themselves. These defensive reactions demonstrated the behavior communalism as well, as responders were quick to vindicate Ulbricht and the original Silk Road as a whole, out of obvious loyalty to both he and the community he had founded. While some commenters remained civil and logical in their defense of Ulbricht, many others’ strong, unfiltered emotions governed their responses; all of which clearly demonstrate their loyalty to their Dark Internet community.

2.3.2 Dark Internet forums – The Hub. Another public forum we analyzed was The Hub. Analysis of the forum consisted of selecting at least one forum thread from every two months since the forum started in January of 2014. Looking at the data, it is apparent that there are certain behaviors that do not appear often on this forum; certain behaviors such as orality, individualism, competition, and object orientation. On the other hand, movement expressiveness and affect show high behavior occurrences. Reading through the Hub forums, one can’t help but find numerous arguments between users, typically littered with slang terms and spelling errors, the latter of which could potentially

be attributed to anger or frustration. Comments like "oldf*g talk to mch poopoo lulzzzz", "smokn a brick of hash" and "[user] is weaponized autism" are surprisingly commonplace. In addition, most users do not care much about correct spelling or grammar, which can sometimes make deciphering the meaning of forum posts difficult. All in all, between the name-calling and drug references, the Hub radiates a juvenile atmosphere.

However, this atmosphere was temporarily replaced with a calmer, much more somber one during mid 2014. This period of time, where the Dark Internet forum was showing low occurrences of affect and movement expressiveness, coincides with the time that Ross Ulbricht was being sentenced. This sizeable dip in numbers could potentially be occurring when the members of this community were discussing what they perceived to be a serious topic. A man famous in Dark Internet history had been apprehended by the law, and his fate was uncertain. Worry and concern for Ulbricht may have been what led the Hub frequenters to take on a more serious tone, and cease their arguing and inane trolling. Then, later in 2014, when Ulbricht stopped being a major headliner in the mainstream news, the community communication gradually reverted back to their old ways, and the arguing and trolling gradually returned. The data does not show any other major trends apart from this dip.

2.3.3 Dark Internet forums – Intel Exchange. Intel Exchange (IE) is a pseudo-anonymous, Reddit-like forum in the sense that users need to be registered with a username in order to participate in discussions, but personally identifying information is not required. Once a username is established, there are slight identifications that the site includes to signify the role of usernames on each discussion board (topic). The website

automatically indicated whether the user is the IE Administrator, the board creator (author), or a general forum participant (user). These identifiers are significant when it comes to regulating the discussions.

IE is a highly regulated forum, relative to other sites on the Dark Internet. The Administrator (Admin) of IE includes a set of rules for participation on the forum. Most of the guidelines were established by Admin, however he/she opens a forum for a community discussion on any desired edits to the guidelines. This set of guidelines and community involvement creates a unique phenomenon of topics and cultural behaviors of this Dark Internet site.

Before the text can be analyzed for cultural behaviors, it is important to take consideration into the topics of discussion. This analysis involves the consideration of the aforementioned forum guidelines. The Admin states that there are certain subjects that are not allowed such as child pornography and requesting physical harm against another person. Any post that violates this rule will be taken off the site and the user can potentially be suspended from the site. Due to this system, the community of IE developed an interesting self-regulating system to keep the site “clean”.

One major example of this self-regulating system can be seen through the redirection of resources. For example, any user that attempts to discuss a topic that involves an illegal activity (or any topic that is against the guidelines) will be met with two responses. The most common response is to be called a n00b (or a similar insult that indicates ignorance). Another response would be a redirection to another site that will allow that topic of discussion. These responses are mainly given to those who are not at all familiar with the Dark Internet. There is a distinct division between unskilled users

who are not familiar with how the Dark Internet works (most common requests are for "hacking someone") and those that are extremely knowledgeable about the Dark Internet. It can be deduced that if a user needs to ask where to find a service or how to access a site, they do not need to be a participant.

Furthermore, this self-regulating system attempts to keep the immoral topics off of the site in order to prevent an association with the common negative assumptions of Dark Internet activities. It can be seen that users will warn and demand other users to not discuss topics such as child pornography or assassination requests. On the other hand, any other topic is available for discussion and users actively participate in boards that are, on average, at least 40 comments long. A few of the most common forum topics are: government/government corruption, personal cyber security, file hosting, current events, and surveillance law.

In this forum, the more active community members mostly consist of Dark Internet veterans. This means that the major users of this forum are there to discuss topics that they find serious and everyone who participates in these conversations need to have a vast knowledge of the inner workings of the Dark Internet. The more active forums, those with at least 25 comments, were analyzed using the behavioral coding outlined in the methodology.

The three main behavior-expression occurrences are movement expressiveness, cognition, and bureaucracy orientation; as proven through averages shown in Appendix D. Movement expressiveness most likely stems from the unique language that is prevalent throughout Dark Internet cultures. There are terms and phrases that are used between the authors and users; if you do not understand what is said, do not expect

anyone to explain it to you. This relates to the preceding conclusion that there is a clear division between the Dark Internet veterans and the uninformed. This is a method that can simply and easily maintain the divide between these two groups. The movement expressiveness is not subtle at all. In addition to openly ignoring requests for explanations, some users will explicitly reply with statements similar to "if you have to ask what this is, you do not need to know about it."

Second, cognition is another common behavior in this community. Serious topics (e.g. internet security, international politics, social support systems) are continuously discussed and most statements and opinions are expressed with proof to back them up. It is common for many users on the Clearnet to make statements and claims on those topics without providing any credible evidence. However, on the Dark Internet, it is easy for a user to not trust or believe a statement because of the nature and perception of the darkened as a whole. The inclusion of a high cognition index acts as a way for users to establish credibility and develop trust on an anonymous platform.

Last, no matter how opinionated someone can get, the users all make a point to follow the admin's site guidelines. This provides a high bureaucracy orientation. Any user that breaks these rules will be reported to the admin and then disciplinary action will take place such as having the text removed or a temporary/permanent ban on participating in discussions. Once again relating to the self-regulation, the bureaucracy orientation behaviors can be traced back to this community's culture.

2.3.4 Reddit. Reddit posts from the /r/DarkNetMarkets subreddit were analyzed from the "Top - All Time Page (the top 25 most popular post of all time)" as well as less popular posts from the Fall of 2016 to Winter of 2017. The average frequency per post of

each behavior is shown in Appendix E. Reddit consists of many different subreddits of community users, where the most popular post from the most popular subreddits often appear on the "All" page of Reddit (/r/All). Additionally, users can subscribe to subreddits of their interest, and the most popular post from these subreddits will appear on the user's "frontpage" when they are logged in. Although there are many subreddits on Reddit that have to deal with the Dark Internet, we chose to examine the subreddit of /r/DarkNetMarkets because it is one of the most popular and active of subreddits that have to deal specifically with the Dark Internet, with over one hundred and twenty five thousand subscribers. Additionally, almost all of the content on the subreddit pertains to current trends and occurrences happening on the Dark Internet's marketplaces; irrelevant post can be reported by users and removed by the subreddit's moderators. Due to these specific traits of this subreddit, it was a meaningful subreddit to analyze with respect to finding trends in textual analysis.

The actual posts from many different subscribers (commonly referred to as "OP" or "Original Poster") and the top voted comments/responses from other subscribers on each post were included in the analysis. Post and comments on Reddit can be sorted in a variety of different ways including "Top", "New", "Hot", and "Controversial". In order to get a wide variety of text included in our analysis, we chose to look at many of the post on the Top page from all the post every posted to the subreddit, and also new post from the period we were analyzing the subreddit. This allowed us to draw conclusions based on what the subscribers seem to find the most interesting, subscriber responses after major Dark Internet events occurred, and also subscriber post that did not receive much attention from other subscribers. These types of post that do not receive much attention

usually have a limited amount of responses/comments from other users, and never reach the front page of the subreddit where the majority of the subscribers do not end up seeing it. However, the majority of posts to this Subreddit do go unnoticed, and do not reach the front page.

The majority of the post and comments are about topics, which include, but are not limited to vendors on the market, current events pertaining to Dark Internet markets, and product reviews. With respect to results of the textual analysis, the most common overall occurring expressions from this analysis included affect, communism, cognition and object orientation. This shows that the /r/DarkNetMarkets subreddit tends to take distinct opinions on the other user's statements and views. Many of these expressions can be specifically seen when there is disagreement between a vendor and a customer, and one of the two trying to inform the rest of the subreddit of the other's actions.

A popular post that shat can be seen as a microcosm for the expressions most often shown in this Subreddit is the most popular post of all time (Fuckgc, 2016). In this post, the author is describing his experience with a vendor reporting the author to the authorities, resulting in a swat team raiding his house, which serves as a warning to the rest of this Subreddit to avoid this vendor. Affect is repeatedly shown when the user shows his anger towards the vendor by using slurs and other insults to describe his actions. Communalism is shown when the user states, "PLEASE up vote this! everyone needs to know!" Cognition is not shown in this post for it is a rather reactionary post, but object orientation is shown when the user shares how he is distraught over what the SWAT team has done, "house it ron to shit! furniture? destroyed! electronics? gone! door? fucking splinters! carpet? toast." Overall this rather lengthy post displays the

consistent expressions users display when they are attempting to share information about an event or another user. These type of post are quite popular on the Subreddit, with at least 5 out of the 25 top posts of all time on this Subreddit being a similar type of post to this.

Additionally, when reading the top comments of the posts on the subreddit as users converse and debate with each other, clashing personalities and beliefs among the subscribers can be seen clearly. When characterizing the behaviors, the majority are reactions either by the user or reactions to the other peer. This aligns coherently to the format of Reddit, where a user makes an initial post, and other users are free to respond to either the OP, or the other users responding to the OP. Some of the most popular comments/responses on the post mentioned previously show the other user's showing sympathy to the user, "this is everyone's worst nightmare", or agreeing with the user for they shared a similar experience, "I actually dealt with [this vendor] before, he was really immature... it took like months for [The Marketplace] to finally resolve the complaint and the whole time he kept saying I was wrong because others didn't complain about it." For the majority of the most popular posts on this subreddit, the majority of people will have responses along these lines, which shows the community aspect of this subreddit where users notice and appreciate user's information which can be helpful.

Lastly, when analyzing the behaviors over time, each behavior tends to remain constant, with no real spikes when dramatic events occur on the Dark Internet. A wide range of expressions and responses can be seen when major events occur that pertain greatly to the Dark Internet, but overall the majority of posts by users and responses by other users tend to follow a pretty consistent behavior. An example of a major post that

included a lot of different expressions and responses is the post where the Silk Road 2 being seized is discussed. A wide variety of comments showing different expressions and beliefs are shown when many users are trying to input their beliefs and speculation as to how the event occurred. Many comments are praised by other users for the potentially beneficial information that was provided, but many are mocked or ridiculed for the other users do not respect the commenter's opinion or beliefs.

2.3.5 Wired. With a focus on technology, Wired's articles target those who thrive on the world wide web. These are people who make a new home on the forums found around the internet, and as such it is not surprising that Wired focuses on this strong community bond. Whether within a marketplace or the community of readers, every article we've looked at has highlighted the communal aspects surrounding both its content and its readers. This is something that dates back to some of the earliest mentions of the silk road, where nearly all information about the budding marketplace came from word of mouth within the Wired community. In an attempt to focus our analysis, we selected the articles by searching the Wired archives with the term silk road.

Another thing of note is that Wired typically holds Tor and the various Dark Internet marketplaces in high regard. In each article from Wired, there was at least one occurrence of the communalism trait. As Wired is a primarily tech-based site with strong tendencies to freedom of speech an expression, it is unsurprising that they would feel a communal bond with a service that promotes those same ideals. Even when discussing the drugs, the weapons, and the child pornography sometimes found on the Dark Internet, the authors provide a neutral analysis rather than negative judgement. When discussing a study on the large portion of Dark Internet traffic related to pedophilia, the author

included a note from the study's author saying that "caution is advised" when drawing conclusions about the study's results (Greenberg, 2014). The author continued to ask questions where as another source may have accepted the study at face value due to the reputation of the Dark Internet. In the face of the known negative aspects of a community whose virtues they believe in, the contributors to Wired endeavored to show their readers the benefits that Tor could provide in spite of it's downsides.

Another point of note is the shift in the bias of Wired following the Snowden leaks. Initially, we could detect no real opinion from Wired. The authors seemed more focused on cataloging the formation of the Silk Road rather than pushing a political view. However, starting after the summer of 2013, which is when the initial events surrounding Snowden went down, nearly every article we've analyzed contains some trace of trait 3 (Affect). These events brought the personal privacy and the rights of whistleblowers to the public eye. This is epitomized by an article posted at the end of 2016 where the Wired staff noted that "now is the time to contribute to the organizations that make it their mission to protect the internet and your rights online"(Wired Staff, 2016). As such, it is unsurprising to see the contributors at Wired develop an affinity for the freedom provided by the Dark Internet.

The last behavior we've noticed is the orality trait. The earlier the article, the more likely it is to mention hearing facts from a community member, a staffer, or someone other than the author. As we looked further, it seems as if this follows the trend of increased knowledge of the dark net the events surrounding the Silk Road. As the marketplace gains more public attention, the less Wired needs to rely on "He said/She said" for their facts. This may be due to them conducting more first-hand

research/digging or to the overall cloak of mystery being pulled away from the Dark Net markets.

2.3.6 Motherboard. Motherboard, a "multi-platform, multimedia publication" run by VICE, is a news site devoted to tech and science and relies on both longform reporting, blogging, and film to present news to the public. Motherboard's varying reporting methods and option to pitch stories to the editor means that the articles found on the site span from simple reporting on events taking place in tech and science to opinion articles. This nature makes Motherboard a good source of information regarding the Dark Internet because articles are written by interested parties whose interest varies from reporting on the events taking place, to defending the use of the Dark Internet, to vilifying many of its practices. As such, Motherboard authors often embed links to other articles written on Motherboard or other news sites to help to validate the information or opinions being shared or even to oppose a previous opinion shared on the site. Motherboard also does not allow for commenting on their articles so authors can post without their opinions being attacked; however, this also means that the only information being shared on Motherboard are the articles that have been deemed worthy of posting by its editor.

The most common trends found to be mentioned or displayed in Motherboard articles written regarding the Dark Internet are: orality, communalism, an objective and rational reaction to events, and bureaucracy (Appendix G). The trait, objective and rational reaction to events, can be explained as an author's desire to report well for the news site. The other three traits mentioned describe the community of the Dark Internet itself. These traits are often highlighted as belonging to the Dark Internet community

because they are the most noticeable. Traditionally, the articles that focused more on Tor and anonymity were the ones that highlighted the passing of information by word of mouth and the sense of community.

The tradition of learning information through orality is a key identifying feature of the Dark Internet culture as viewed from Motherboard. In one article, a user of Dark Internet marketplaces relayed that "[he] could buy drugs from someone after reading dozens of reviews on their service and product, and feel confident that [he] was getting what [he] was paying for" (Spotz, 2014). The necessity of oral communication relates greatly to the usage of the Tor as a method of preserving anonymity; without being able to look up sellers, buyers are forced to rely on the reviews posted by other buyers and this creates the community that is so prevalent. Another user highlighted this tradition of orality describing the research that goes into choosing a vendor, highlighting the ease with which he was able to evaluate the vendors: "A vendor's rating and number of sales on the market will give you an immediate idea of how reputable they are" (Whitaker, 2014).

Another key feature is a sense of duty towards the community: communalism. Dark Internet users are identified as having a strong communalism and this is conveyed in a variety of ways. The previous article by Spotz highlighted the importance of the tradition of orality that allows users to be able to identify sources of high-quality product; this tradition of reviewing also relates to the user's sense of duty towards their community (2014). Users share the information about their experiences on the Dark Net in order to allow for other members of their community to make informed choices about their vendor needs. Members of the community also engage in supporting their

community in other ways through communication not on the Dark Internet; Whitaker described this as an alternate way to research vendors beyond reviews: " there are also several dark net market communities (such as the darknet markets subreddit and DeepDotWeb) where buyers discuss vendors and warn about scams" (2014).

The final feature that was especially prevalent to the community of the Dark Internet, as viewed by Motherboard, was a focus on structure and rules: bureaucracy; this feature relates to the previous two features because its focus highlights the importance of the previous two and ensures that their traditions are continued by new members of the community.

2.3.7 Huffington Post. Our analysis of the depictions of the Dark Internet in the mainstream media proved extremely useful in determining the perspectives and opinions of the general public, revealing specific biases and opinions that largely stemmed from ignorance of the realities of the Dark Internet and of the thriving online communities which have blossomed there. As we strive to accurately explore the culture, opinions, and practices of the Dark Internet, we utilized textual analysis methods on articles and news sources that highlight the experiences, hot topics, and controversial headlines on the Dark Internet. By performing a textual analysis of articles related to the Dark Internet published by The Huffington Post, a left-leaning American news site, our team was able to identify and examine marked behaviors and common patterns present throughout the collection of texts. Specifically, for the Huffington Post, articles that have been tagged with the keywords "Dark Web" "Dark Internet" "Bitcoin" "Tor" etc., were screened, read, and coded to observe the behaviors, expressions and reactions that are common and

uncommon on the Dark Internet. The Huffington Post offered articles, as a left-leaning news source, offered information regarding the Dark Internet which leaned towards liberal perspectives, while some articles still were surprisingly quite conservative. Once all articles were collected and coded, we concluded that there are several behaviors that have been relevant in almost all articles. The top three behaviors present are Affect, Communalism, and Cognition.

Affect, or the emotional response to high levels of stimulus, was strongly apparent within almost all articles. The emotional responses in question were majorly that of fear or discomfort towards the Dark Internet, which could be attributed to the general public's lack of knowledge of the Dark Internet, as well as responses to security, current events, government control, etc. Emotional responses that our team coded for affect ranged from mild to extreme, often portraying clear opinions against all use of the Dark Internet. Caroline Knorr, a guest journalist for The Huffington Post and "parenting expert" from Common Sense Media, even went as far as to characterize the Dark Internet as something out of a scary movie: "No one knows how much of a threat [the Dark Internet] is to regular people" (Knorr, 2016). These evidently outlandish affectual claims in disapproval of the Dark Internet, which commonly portrayed fear as the most frequent emotional response, alluded more to the ignorance of the affected individuals regarding the Dark Internet, rather than to the dangers posed by the Dark Internet itself. The biases portrayed by these writers and commenters were at times more apparent than others; an editor for Common Sense Media, an organization which aims to aid parents in their regulation information and media accessible to young people.

Despite the majority of Americans having and enjoying internet access on a daily

basis, there still remains a collective ignorance regarding the Dark Internet, which has consequently invoked a certain degree of fear towards the subject. As it is human nature to fear the unknown, journalists and commenters of The Huffington Post frequently displayed high levels of negative, reactionary affect towards information regarding the Dark Internet. Admittedly, much of this information was cast in a negative light, and the majority of the topics discussed with regards to the Dark Internet was extremely negative, taboo, and often even illegal. The prominence of negative affect in our textual analysis can greatly be attributed to the perceived negative attitudes toward the Dark Internet by lay people with little to no prior knowledge of its structure, functionality, or uses in a modern context. Our analysis revealed that certain buzzwords and key phrases were more often than not the extent of the average person's knowledge of the Dark Internet. Most of these buzzwords were exceedingly negative, such as "illegal drug trade", "child pornography", and "terrorist recruitment". It appeared throughout our research that the majority of the topics The Huffington Post deemed newsworthy enough to go to print regarding the Dark Internet were only the dangerous, frightening, and/or scandalous. It is by this media bias that we may suggest that the prevalence of negative attitudes towards the Dark Internet can largely be attributed not to the public's knowledge of the tool, but lack thereof. As the Dark Internet continues to become increasingly part of the mainstream and infiltrate popular culture, we can look forward to these attitudes becoming more progressive and positive, as people become informed of the uses and benefits the Dark Internet has the potential to provide for the average person, the economy, and for society as a whole.

The behavior affect was consistently present among the bodies of texts our team

studied from Huffington Post. In another article, “Americans Don’t Care Enough About NSA Spying To Protect Themselves, Survey Says” many users reacted to hearing about the government “spying” or surveilling Americans. One user commented, “Does anyone really think there is anything that is secret? Right now if you own a phone, computer, and Internet you only have the illusion of privacy” while another user felt “concerned that almost half the country thinks it's ok for the government to spy on everyone.” Within this behavior, we may conclude, there are overlapping emotions of fear, concern, and anxiety but can also be coupled with optimism, curiosity and excitement depending on the situation. Significantly, there are two sides of user emotion within the Dark Internet. When accessing the Dark Internet, users often already know what to expect. The chase of the anonymity on the Dark Internet and the privacy entices users to experience the Dark Internet. Within Huffington Post articles, the types of reactions fluctuated between positive, negative, and with neutral being the least prevalent.

Another coded behavior that stood out in our data collection was cognition, or objective and rational reactions to events, the opposite of the behavior affect. In contrast to the recorded affect patterned behaviors, the cognition expressions and behaviors were often positive. Although exhibited less frequently than affect, cognition was recorded at a great extent throughout studies of Huffington Post articles related to the Dark Net. This behavior was largely exhibited by journalists whom they themselves had prior experience using the Dark Internet for personal reasons. Our team found it worthy to note that with increased exposure and knowledge of the Dark Internet, Tor, The Silk Road etc., journalists and Huffington Post subscribers were more likely to exhibit cognitive behavior as opposed to affective. That is, with increased knowledge on the subject of

discussion, participants were more likely to engage in a civil, intellectual manner driven by logic and reason as opposed to emotional responses largely driven by fear and preconceived notions and perspectives. Along with these cognitive behavioral responses occurring in users with more experience and comprehension of the Dark Internet, the responses themselves were across the board neutral or positive with regards to the subjects of the Tor-related articles. This contrasts greatly from the affective responses that were recorded, which were consistently negative, demonstrating highly negative emotional responses to Dark Internet-related topics and current events. Our team can surmise from these patterns of behavior that the small population of people who are experienced with the Dark Internet are actively engaging in attempts to spread information about its uses and functionality to the greater online community. This motivated attempt to disseminate information regarding Tor and the Dark Internet serves not only for the purpose of improving the public's perception of the tool, but also ultimately to expand the size and scope of the Dark Internet community.

This feeling of duty towards community was also a marked behavior pattern our team studied in our texts, communalism, was found within our study of Huffington Post online news articles as the third most frequently exhibited behavior behind affect and cognition. This can likely be attributed to the fact that most Dark Internet users feel more comfortable engaging in communal behaviors displaying loyalty to the Dark Internet community while they are in fact on the Dark Internet. In "The Drugs Dilemma at World Economic Forum 2014: Right for Another Reason," the author highlighted panelists from the World Economic Forum and their thoughts to solving the "Drug Dilemma" that utilizes the Tor Network on the Dark Internet. Since drug markets are a big part of the

dark net's user traffic, the Dark Internet heavily contributes to the outcomes and consequences of drugs. Due to the widespread and well know traffic of drugs, many people blame Tor and market places for the cause of such knowledge. However, in "Americans Don't Care Enough About NSA Spying To Protect Themselves, Survey Says" user's come to the defense of the Dark Internet stating that it's not what you may or may not do on the internet, if the government wants to get you, they will. One user stated, "if the gubmint [government] really wants to get you, they will get you no matter your innocence. They can manufacture, invent, or twist all the data and come up with any number of weird and wacky reasons to take out an inconvenient person." Therefore, our team determined a common perspective within the Dark Internet community in that no matter what you do or what services the Dark Internet provides, it is not responsible for the actions of the government.

The comments section of Huffington Post articles within the surface internet seem an unlikely place for avid Tor users to gather to discuss their vibrant, ever-growing community, especially due to the overwhelmingly negative perspectives surface internet users and laypeople have displayed in high numbers towards the topic. Despite the fact that Dark Net users likely feel more comfortable displaying communalistic behaviors when navigating the actual Dark Internet, this was nonetheless a key behavior exhibited in our analysis of this body of texts. The majority of communalism exhibited in the texts was reactionary responses to defend the Dark Internet's legitimacy and usefulness of function. One user, quoting the Silk Road's founder, Ross Ulbricht, who operated under the pseudonym Dread Pirate Roberts, exhibited communalistic behaviors in their defense of the Dark Internet, specifically the Silk Road, by addressing its value as a

communication tool: "'My hope is that a high level of discourse will be fostered [on the Silk Road], and as a community, we can become strong in our beliefs, with a coherent message and voice as the world begins to take notice of us'" (Isaacson, 2014). Given the relatively small population of regular users on the Dark Internet in comparison to the vast mainstream use of the surface internet, communalism was a prominent behavior in Dark Net users, reflecting their self perceptions of themselves as a close knit community that works together to function. These users themselves directly impact the Dark Internet's functionality, not only by attracting new users through word-of-mouth interactions, but also by the creation and maintenance of exit nodes to support the speed and efficacy of the Dark Internet itself.

Dark Internet users, even while navigating on surface internet forums such as the comments sections of The Huffington Post, were quick to defend the value and legitimacy of their community and online resource, citing its usefulness as an anonymous place for discussion, diversion from censorship, and its growing place as a prominent global economy and the many industries it is home to. Whatever the logic for the users´ defense of the Dark Net, our team noted that these defenses were largely made in response to users displaying negative affect. Simply put, Dark Internet users are often quick to defend the legitimacy of the Dark Net to its critics, who most frequently focused their critiques in the illegal activity the Dark Internet is known for. From this data, we can conclude that Dark Internet users are frequently and consistently engaging in cognitive and communalistic behaviors to defend the Dark Internet and inform others with less favorable opinions of its practicality and usefulness both as an online tool, a budding community, and a rapidly-growing commercial marketplace.

Lastly, cognition, or objective and rational reaction to events, was another top behavior to be coded through Huffington Post articles. Many authors and readers, had positive rational reactions to certain events surrounding the dark net. Cognition was mostly found in the author's tone and words in an article as they rationally explained news, experiences, discussions and problems of the Dark Internet. Most cognition reactions involved details, different perspectives and possible solutions to preconceived Dark Internet notions. More knowledge and research were developed before an overall conclusion was produced within the article. Affect, on the opposite side, dealt with readers' comments and views on the information presented. The comments presented by users and readers of the Huffington Post were their real reactions to the events that center around the Dark Internet.

Within these top behaviors, they suggest an overall sense of community within the Dark Internet. There may be separate and opposite stances within the community as with any, but it is undeniably that a sense of pride and group user loyalty - a kind of online patriotism of sorts - exists and is flourishing within the Dark Internet community.

Chapter 3

An Analysis of Dark Internet Experience

3.1 Introduction

As discussed before, academics have made attempts to qualitatively understand the consumer experience of using cryptocurrencies on an, anonymous Dark Internet marketplace. Our team will be attempting to add to this understanding via a first hand purchase of an item on a Dark Internet marketplace by using Bitcoins. Through the use cryptocurrencies to make a purchase on the Dark Internet, our team attempted to answer the following research question: to what extent does Bitcoin affect Dark Internet online transactions and how does it compare to the traditional buying and selling of goods? Additionally, we aimed to understand how these differences could be used to inform the public to the intricacies of how Dark Internet market function. For the purpose of this study we will be undergoing the process of experiential learning, in which we will behave as a buyer and experience both purchasing processes on the Dark Internet and Clearnet and then use our experiences to draw conclusions regarding Bitcoin's affect on transactions and the similarities and differences between Dark Internet and Clearnet marketplace transactions.

Based on research discussed previously, it has been shown that using a bitcoin on the Dark Internet will show many similarities to the use of conventional currencies in traditional online transactions. For example, it was found that over a short period of time, the value of Bitcoin fluctuates greatly with real world market factors, just like traditional, recognized currencies (Li and Wang, 2017). However, we hypothesize that there will be distinct differences unique to the bitcoin, as it is by nature inherently different from standard forms of currency due to its nearly untraceable nature, that will reveal themselves via the process of purchasing an item on a Dark Internet marketplace. We

believe that by going through the entire process of making a purchase, it will highlight these inherent differences. Bitcoin is not backed by any legal institution, is an entirely digital currency, which can only be stored on electronic media, and relies on peer-to-peer networking and cryptography to maintain its integrity (Brito et al., 2013) (Barber et al, 2012). A longitudinal study of Silk Road transactions found that the bulk of all exchange trades were speculative, and thus Bitcoin was used as a commodity rather than a currency (Christin, 2013). Understanding these distinct and qualitative differences and experiencing them firsthand will shows how Bitcoin greatly affects transactions on the Dark Internet. This understanding can then be built upon, and be used to inform the public who does not have knowledge of how Bitcoin and Dark Internet marketplaces function.

3.2 Methodology

In order to acquire information pertaining to our research question and hypothesis, as a team we fundraised money and then purchased approximately $700 worth of Bitcoin in August of 2016 enough bitcoin as necessary, which was used for transactions on the Dark Internet and the Clearnet. State Grants or any other source of State funding cannot be used to purchase a bitcoin, so our team acquired funds to purchase the bitcoin. by our own means. To accomplish this, we relied on an online crowdfunding campaign as well as a food sale held on the University of Maryland campus. These campaigns have provided us with sufficient funds to purchase $700 worth of bitcoin for research purposes.

Once we purchased this amount of bitcoin, we used it to help accomplish our research goals. We attempted to purchase the services of two separate authors, two from

the Dark Internet, and two from the public internet, who were hired to write academic papers for us. We also attempted to use conventional currency to hire two additional ghostwriters from the public internet. Four purchases were made to complete this task, but not all of the papers were received. Once we received our papers, we were going to be able to compare them using methods described below, to assess the quality of the products obtained through different services and methods of payments. We initially chose to purchase an academic paper through ghostwriting service because it is available over both the public and Dark Internet, the quality of the product can be directly assessed, and it is not illegal to purchase. However, because the ghostwritten paper's never arrived, an additional item was required to be purchased to test our hypothesis. We decided to purchase fake IDs off both the public internet and the Dark Internet. We then decided to compare these fake IDs to an actual ID to gain a qualitative understanding of the value of the products purchased. It is important to note here that the purchase and possession of fake IDs is legal, it is the use of them that is not legal and for the purposes of the research being conducted we purchased the ID but turned our purchase over to the Gemstone staff for destruction.

In order to actually purchase the bitcoin(s), there were many different sites that we can use to make the purchase, such as Coinbase or bitcoin.com. Different online markets, both on the Dark Internet and public internet, allow for the purchase of a bitcoin, or fractions of a bitcoin. The purchasing of a bitcoin is very similar to setting up a traditional bank account; an initial sum of money is deposited, and this money can then be used at any time for a variety of purposes. We can also sell our bitcoin(s) back to many of these sites to receive payment in USD in return. During the time that we possess

this bitcoin, it will be contained in a digital wallet app installed on a teammate's smartphone, ensuring that we will be the only ones with access to this bitcoin.

Our plan for the usage of this bitcoin was to aid in our analysis of the way transactions are conducted on the Dark Internet and Clearnet. Market sites such as eBay and Amazon have become household names by establishing reputations as companies that provide reliable and high quality service. Success on Dark Internet marketplaces is achieved in a similar manner: maintaining a high reputation for good business. However, one major differing factor is the Dark Internet's much higher capability for anonymity, provided through tools such as bitcoin. The initial trust that always exists in a legal, regulated setting, like a brick-and-mortar store or commercial website, is not guaranteed for those who wish to conduct transactions on the Dark Internet. This variance in market regulation may have significant effects on the development of markets on the Dark Internet.

Throughout the whole process of buying and keeping track of the value of our bitcoin, we hope to gain insight into the process of buying and owning bitcoin and being a consumer on Dark Internet markets. Excluding the beginning and final value of the bitcoin at the time of purchase and use, there will be no numerical data to gather. Rather, the data collected and analyzed will be completely qualitative with respect to the experience of purchasing and using a bitcoin, and the final deliverable we will receive from the ghostwriting services. Using bitcoin for purchases on Dark Internet markets will also allow us to gain a better understanding of the overall purchasing process on these markets.

This first-hand experience and the familiarity that this experience will grant us

will best enable us to gain a better grasp of using bitcoin and acting as a consumer on the Dark Internet. This is important to study and understand because Bitcoin (and other cryptocurrencies) is a new, and possibly revolutionary, mechanism for payment. Bitcoin, unlike other forms of recognized payment, is not backed by any major bank or other financial institution, which forces sellers and consumers to have a certain level of trust when utilizing Bitcoin (Angel and McCabe, 2015). To be able to understand and qualify the concept of using an anonymous currency is important for informing people and society as whole who do not have faith in using this form of currency.

3.3 Discussion

We fundraised and utilized $700 to acquire as much Bitcoin as possible in August, 2016 from a Genesis Bitcoin ATM in Greenbelt, Maryland. The Genesis Bitcoin ATM operates by transferring the money deposited by the user into their personal Bitcoin wallet. Specifically, the Genesis Bitcoin ATM recommends using the Breadwallet application the iPhone or Android if the consumer does not already have a Bitcoin wallet. We used the Breadwallet application for we did not already have a personal Bitcoin wallet. On this application, the user is given a unique wallet, that can be represented by a QR code or a very long string of letters and numbers. On the Breadwallet application, users can view their wallet contents, view their recent transactions, and transfer Bitcoin to other wallets via entering the character string or taking a picture of the QR code. Most transactions of Bitcoin on this wallet, and other wallets, can take up to an hour to process. This is due to the multiple authentication checks that are made between the wallets to ensure that the transaction is legitimate. The user can see the transaction being initiated within seconds, but the Bitcoin cannot be used for other purposes until the validation is

complete.

The initial part of process of obtaining a digital asset in the form of Bitcoin via cash was very similar to the traditional experience of depositing cash via an ATM. There were some minor differences in the two processes, but those differences did not create any major advantage or disadvantage between the two with respect to ease of the process. In both experiences, any person can approach an ATM with the cash they want to deposit, and within a couple of minutes, the user can see the end result being uploaded onto the virtual wallet. This is especially true today, where many major banks allow the user to view the amount of money they have in any of their accounts via a phone application that is often referred to as a virtual wallet. Additionally, in both cases the user is given a receipt with the record of the transaction in case there is some type of dispute during the process.

One unique attribute about the process of obtaining a Bitcoin via a Bitcoin ATM is that any person can obtain a Bitcoin using this process; the only requirement is that the person has a smart phone or device that is capable of downloading the Breadwallet application to create a Bitcoin wallet. This is different from utilizing an ATM to transfer cash to your account with a bank; a person must be already be registered customer with the bank with some sort of account to deposit money, and becoming a customer at a bank can be difficult considering a person's financial background. Additionally, a person depositing money to a bank account must also have a debit or credit card with them to initiate the deposit. A person using a Bitcoin ATM to secure a Bitcoin only needs cash and a smart device to complete the process of acquiring a Bitcoin in their Bitcoin wallet.

Additionally, the user must create a PIN or set up a fingerprint scan on the

application to ensure that only the owner of the wallet can access its contents in the case that the device in which the wallet is located is lost or stolen. Once the wallet is created by the user, the application generates and prompts the user to write down a recovery phrase. This recovery phrase can be entered into the Breadwallet application on any device in the case that the user lost the device that their previous wallet was on. Additionally, if the applicants detects that the user has taken a screenshot on their phone of their recovery phrase, a new recovery phrase will be generated and a message appears saying how it is not recommended to have the recovery phrase stored on a phone for other application could potentially see it. In January of 2017, the member of our team who was holding the Bitcoin wallet on their phone, received a new device. Because of this, the team member had to redownload the Breadwallet application, and enter the recovery phrase. After around two hours of processing, the wallet's contents were recovered onto the new device.

With regards to having multiple layers of security to keeping the contents of the Bitcoin wallet secure so that only the true owner is able to access it, it is somewhat similar the multiple levels of security that a person has to go through when accessing their bank account. When a person makes a purchase with their debit or credit card, a person usually needs another piece of information to complete the purchase. These pieces of information include, but are not limited to, a PIN, the person's zip code, or a signature. Additionally, many smart device applications, developed by banks and other financial institutions, that allow a person to check their bank account have multiple levels of security that must be passed by the person before they can access the information in their accounts. This is done so if a person's device is lost or stolen, the person who recovers the

device cannot view or conduct transactions using the lost device.

However there is a pretty distinct difference when it comes to the recovery of a Bitcoin wallet and the recovery of a bank account. Generally, if a person losses the information to their bank account, the bank will provide them with multiple ways to recover or update their information to access their account. For example, the PNC Mobile application for the iPhone requires the user to enter their username, password, and unique identifier before logging into their account. However, if one of these pieces of information is forgotten or lost, there are multiples ways of recovering it (including an email password recovery or contacting customer support). It is very unlikely that a person who has lost or forgotten their access information for their bank account will ultimately become locked out of their account and never be able to access that money in their account again. However, if the owner of a Bitcoin wallet on Breadwallet, loses their device and also their recovery key, it is very likely that they will never be able to access the contents of their wallet no matter how much or little Bitcoin is in their wallet. There have been popular, but unconfirmed, stories of the internet of people losing millions of dollars worth of Bitcoin on their hard drive because the person threw away what they thought was an empty hard drive, and had no way to recover the contents. For example, a popular internet story that is often discussed on forums such as Reddit and 4chan talks about a British man who threw away a hard drive with Bitcoins on it in 2009 because he believed they would never be valuable. Since then the value of those Bitcoins on the hard drive has reached a value of over 7.5 million dollars, but this man has no way of recovering the contents of that hard drive. Whether this story is true or not has not been confirmed, but it does give insight into the lack of recovery options for a hard drive that

has Bitcoins on it, or a Bitcoin wallet in itself.

Once ATM and other fees associated with purchasing the Bitcoin, our team had approximately 1.08 Bitcoins to utilize at our discretion. As of March 20th, 2017 the value of 1.08 Bitcoins is worth approximately $1,070. During this timespan, the value of this Bitcoin peaked on March 3rd, 2017 at over $1,300. However, from March 15th to March 18th the value of a single Bitcoin dropped by over $300.

The experience of the value of Bitcoin changing over a short period of time is very different than the same experience but with traditional currency such as United States dollars. First of all, the amount of Bitcoin held is completely relative, for the value of Bitcoin is all in comparison to another form of currency. United States currency is not usually compared to another currency by people in the United States who are using it on a day to day basis. And in addition to the value of a Bitcoin always being determined to the value of another currency, the value of Bitcoin can be very volatile on a day to day basis. Because the value of a Bitcoin is so volatile, there have been times where half of a single Bitcoin has been worth more than multiple Bitcoins during the course of one calendar year. This is different than traditional forms of currency such as the United States dollar; it can take months, years, or even decades for the value of a single United States dollar to change by even a couple percentage points.

Once we had the Bitcoin secured in our wallet, we were free to find vendors on both the Clearnet and the Dark Internet with which we could use our Bitcoin to purchase fake IDs for a qualitative comparison. To find the vendors which we decided to purchase from, we had to create a criteria for the identifications that both vendors could meet. This criteria included, but was not limited to, being able to create an ID from the same state as

each other, being able to have the final product delivered in less than a month, and accepting Bitcoin as their form of payment. We were able to find a vendor source on both the Clearnet and the Dark Internet that met with our criteria, but the process of locating a specific vendor to purchase from differed in the two experiences. We purchased both of the identifications via Bitcoin within two days of each other, by submitting the same information for the identification to both websites. The identification from the Clearnet was approximately $100 at the time to purchase, and the identification from the Dark Internet was approximately $150 at the time to purchase.

Deciding on a specific vendor to use on both the Clearnet and the Dark Internet was very different. The major difference between the two different sources was that, on the Clearnet, there were many different sources that were able to provide an ID that met the criteria we wanted, but very few of these vendor's accepted Bitcoin as a form of payment. However, on the Dark Internet, all of the vendors on the marketplace we were utilizing had to accept Bitcoin as a form of payment, but very few of these vendors offered a product that met all of the criteria for our identification. Therefore, the process of finding the final two vendors to purchase an identification from was very different for the two experiences.

To determine a final vendor to purchase an identification from on the Clearnet, it was as simple as utilizing a specific google search, and reading the information provided on their websites. We were able to determine a list of potential websites (who accepted Bitcoin as a form of payment) that could be used to purchase the identifications and comparing the advantages and disadvantages. These advantages and disadvantages include: product reviews, price of the identification, the extent as to what information we

would have to provide, ease of the purchase, perceived reliability of the website, and reviews of the products provided by that website. Overall, the process of finding a Clearnet website that accepted Bitcoins to purchase a fake identification provided us with many options, which made us believe the source we purchased our fake identification was the best source available.

Finding a vendor on the Dark Internet who could provide us with the specific fake identification we sought to purchase was a much different, and overall more difficult experience. First off, we contained our search to one specific Dark Internet website (Alphabay) in which our team already had a registered account. Although there were many different Dark Internet websites where we could have potentially found a vendor that could have provided us with our desired product, the Dark Internet website that we ended up using was the most popular and widely used marketplace among Dark Internet users. This led us to believe we were maximizing our chance of finding a reliable vendor, even when it was possible to find an even more reliable vendor with a better product on a different Dark Internet website. Second, the search engine the Dark Internet website utilized left our team confused and lost on trying to locate a vendor. For example, there were several categories our product could have fit under, including documents, fraud, or miscellaneous item. If we were to purchase a more popular item that is sold on this or other markets, this would have not have been a problem. For example, there were countless and specific categories that had a plethora of different illegal drugs that were sold, many of which had hundreds of ratings and reviews. If a customer were to purchase a specific drug on this market, they would have no trouble trying to navigate the market in order to reach the hundreds of different products that they could potentially purchase.

Eventually, we did find a small amount of vendors who could potentially provide us with our desired identification. However, these vendors did not have many product reviews, and were rarely used (less than five total sales for this specific product). Even though we were unsure of the level of trustworthiness among the vendors, we decided to purchase an identification from the vendor with the highest overall rating on our desired product. If we were attempting to purchase an illegal or illicit product such as drugs that was more popular, we would not have had this same problem. There are countless vendors and products for almost all drugs and more popular products with hundreds of ratings.

In order to purchase the identification on the Dark, Bitcoins had to be transferred from our Bitcoin wallet to a new wallet that was associated with our account on the site we utilized to purchase the identification of the Dark Internet. This process took approximately one day, and took multiple authentication checks to have the Bitcoin transferred. Once we made the purchase to the vendor, the Bitcoin was held in escrow by the website and gave us an option to mark the transaction complete (in which case the entire Bitcoin value would be transferred to the vendor) or dispute the transaction and have a moderator review the purchase. We received a message on the website within a couple days from the vendor providing with the tracking number of the package, and asking to mark the transaction complete when we receive the package. Within a week we received the package containing our identification. It was an international package that was marked as an inactive credit card so it could make it through customs.

The identification that was purchased through the Clearnet was purchased via a website that was found via a google search. We submitted a form on the website which contained all the information that would be on the identification. After that form was

submitted, we received instructions to pay a certain Bitcoin wallet address a specific amount of Bitcoin. If the Bitcoin was not received within 24 hours, the order would be cancelled. We successfully submitted the payment to the website, and it was confirmed that the order was placed when examining the order on the website. However, we have yet to receive any response or identification from the website since we submitted the payment, although the information on our order has read "Downloaded" for weeks.

Over the whole process of obtaining a Bitcoin, and then eventually using that Bitcoin to purchase a fake identification on both the Clearnet and Dark Internet, there were many differences between the two methods, as well as differences between using a Bitcoin to purchase an asset and using a more traditional form of currency to purchase an asset. With respect to actually obtaining a Bitcoin, the process mimicked depositing cash using an ATM. There was a minor difference in that anybody with cash and a smart device could go to a Bitcoin ATM and end up with a Bitcoin in their Bitcoin wallet; a person does not have certain financial credentials or already have a Bitcoin wallet to use the Bitcoin ATM. Additionally, the security systems in place to keeping a Bitcoin wallet secure were very similar to the virtual wallet application on smart devices that many major banks and financial institutions have for their customers to use. However, a unique difference is that it is possible for a person to easily lose access to their Bitcoin wallet, and the contents of it.

With respect to finding a vendor to purchase from, and eventually purchasing a product, on the Clearnet and the Dark Internet, there were major differences between the two, and in comparison to traditional purchases. In regards to finding a reliable vendor, it seemed that we had many different options on the Clearnet, but only a few of them took

Bitcoin as a form of payment. On the Darktnet, it was tough to find a vendor who offered the exact product we were looking for and had any reviews from previous customers. With respect to results, we have received minimal to no communication from the Clearnet vendor, and it is almost impossible to contact them with questions about our products. We also have yet to receive the product in over a month (it was advertised that it would take four weeks to deliver the product). Meanwhile, the Dark Internet source reached out to us immediately after we submitted our purchase, gave us information so that we could track our package, and got us our product in less than a week after purchase. In comparison to an internet purchase using traditional currency, both of the purchasing experiences via Bitcoin had their own unique attributes, while also sharing common attributes with a traditional internet purchase. On the Clearnet, we had a variety of different vendors to choose from when selecting our product. On the Dark Internet, we were able to track our product while it shipped much like if we were using a traditional internet marketplace such as Amazon. In both cases, we were able to pay for product relatively quickly using our Bitcoin. However, in only one of the cases did we end up receiving what we had paid for.

Chapter 4

Conclusions

Throughout our research on the Dark Internet, the thing that has most impacted our progress has been the ever-changing nature of the Dark Internet itself. By following the major events of the Dark Internet marketplaces, we were able to observe thisclosely as well as dealing with its impact on our research intimately. Upon beginning our research, we set out to do a multitude of different things some of which we quickly learned were not possible at the time for a multitude of reasons and others that were at first possible when planning our research, but by the time we tried to actually execute our plans, they had become impossible.

As previously stated, we initially started our experience analysis with the goal to purchase papers from both the traditional internet and the Dark Internet to compare the process, however, by the time we were able to fundraise the money for this procedure, the source we were planning to use on the Dark Internet was no longer offering services and we were unable to find a replacement. This led us to changing our project to the purchasing of identification cards.

While the nature of the Dark Internet itself impacted the way our project proceeded, so too did the topic of the Dark Internet itself. The topic of the Dark Internet and its many facets and functionalities is generally met with ignorance - and sometimes even fear - from the general public. This fear largely stems from large crisis moments that have hit Dark Internet marketplaces, by means of FBI shutdowns, thereby creating media frenzies and sensational news headlines characterizing the Dark Internet as a place dedicated solely to drugs, weapons, and illegal pornography. As the news of drug busts are known to produce excitement and discussion within any real life community, the provocative nature of the Silk Road, Agora, and other similar Dark markets known for

their illicit goods have quickly become the quintessential images associated with Tor and the Dark Internet as a whole. This image has spurred a plethora of literature, which focuses on the aforementioned illicit goods, and various illegal activities performed over the Dark Internet. Much of the existing literature includes studies about users' experiences through Dark Internet drug trade, the illicit goods sold over these markets, and proposals on how to police these illegal activities. The lack of literature on non-illegal Dark Internet activities exacerbates its negative image and stunts the growth of knowledge about it by narrowing research to a scope that only encompasses a very small portion of the Dark Internet. The prevailing stigma surrounding the Dark Internet has only furthered the public's own ignorance, and its legitimacy and practicality as a social and economic tool is squandered. By taking advantage of the tools posed by proper utilization of the Dark Internet, rather than evading them due to fear, ignorance, or both, the everyday person stands to benefit from joining a remarkable, rapidly changing online community that engages millions of users from every corner of the Earth.

Despite Tor's user-friendliness and ease of access, entering and navigating the Dark Internet remains a mystery to most people online, and thus the Dark Internet as well as its complex communities remain in the shadow of what people consider normative, everyday internet use. Team DIRE came across such instances of fearful stigmas in the process of studying the Dark Internet for this project. With the intention of analyzing ghostwritten papers the team had originally planned to buy, our team attempted to enlist the help of the University of Maryland English department. Our team asked several professors in the English department if they would provide an old essay prompt, which has been used for examples or practice tests, and grade the ghostwritten papers written

for that prompt in order to compare and contrast the paper from the Dark Internet versus the paper from the clearnet. The English department reacted to this proposal with an unanticipated amount of fear and, surprisingly, anger at the idea of any professor consenting to our team's proposal for suggesting its relation to student plagiarism as well as the nature of our project itself. An email from the English department was forwarded to its faculty members to demand that they must not agree to work with our team. The director's negative perception of the Dark Internet led him to believe that the English department would not have the University of Maryland's approval to work with a team that is associated with the Dark Internet. The department specifically, did not want a prompt from the University of Maryland used for the project due to its association with the Dark Internet. The negative stigma of the Dark Internet caused these extreme reactions and ultimately contributed to the collapse of that section of our project. This instance was a learning experience for our team, helping us realize that in order to reach out to anyone in the general public for help with the project we had to be exceptionally clear in our communication to ensure understanding that the phrase Dark Internet is not synonymous with illegal.

Through our experience using Dark Internet marketplaces and cryptocurrencies to anonymously purchase a product, we gained valuable knowledge about the purchasing process that can be used by others in order to expand knowledge of the Dark Internet for both academic and public communities. For this section of our project, we utilized ethnographic techniques to study a truly lived experience of acting as buyers ourselves. From this study, we were able to not only observe but actually experience the interactions between a consumer and seller on the Dark Internet. We found that the process of making

an anonymous purchase using the Dark Internet has unique qualities and attributes (when compared to the traditional experience of purchasing an item on the internet) that make it appealing to a certain group of people. These unique qualities and attributes also have the potential to be adopted into mainstream, Clearnet marketplaces that could improve the experience for vendors and purchasers alike. This is because much of the public is not familiar with the process of using the Dark Internet, and the lack of knowledge contributes towards the negative stigma that many have believe the Dark Internet has. By providing and expanding knowledge about the purchasing process using cryptocurrencies on the Dark Internet, an opportunity is created to lighten the negative stigma associated with Dark Internet, and hopefully set the stage for the unique qualities of cryptocurrencies and the Dark Internet to be adopted by internet marketplaces.

Throughout the entire process until upon receiving the purchased item, our team gained new information about the intricacies of how Dark Internet markets and cryptocurrencies operates at almost every step. Furthermore, our team believes that were those that are aware of Bitcoin, but ignorant of the process of using it, to gain the same knowledge that we gained through our experience, then their views on Dark Internet markets and cryptocurrencies would change for the positive view by recognizing their practicality and usefulness. For example, when we used the Bitcoin ATM to initially acquire the Bitcoin, we learned that the only things needed to acquire a Bitcoin was a smartphone and cash, the entire process itself took less than thirty minutes. If a larger quantity of people were privy to this fact, it could reduce any lingering hesitancy regarding purchasing their Bitcoin as they would feel encouraged by how simply and efficient the process really is. This is the first of many new pieces of information that we

gathered in our experience that could be used to inform those who do not have prior knowledge.

Another area where we gained information through recording a lived experience was the process of finding a vendor and making a purchase. Going into this process of purchasing a fake ID, many of our group members were skeptical due to purchases we attempted to make using Bitcoin and the Dark Internet in the past. However, when we selected a vendor on the Dark Internet to purchase a fake ID from, we learned that there were multiple security methods in place to ensure that the transaction went smoothly for both parties involved. We learned that people who made a transaction from that vendor before were able to publicly review every aspect of the transaction from vendor communication to discreetness of the package they received. The vendor we selected did not have a large amount of previous reviews, which was a deterrent from choosing the vendor. However, as soon as we made the purchase, the vendor was extremely communicative, and was willing to provide us with information about the transaction. This led us to believe that even vendors on the Dark Internet who do not make many transactions are still conduct their transactions in a very professional manner. Our team was happy to leave this vendor a positive review to their page, highlighting the ease of communication and quick shipping time that we had experienced through our actual lived experience of purchasing the ID.

Additionally, in this purchasing process we learned that the Bitcoin we utilized to purchase the fake identification was held in escrow by the marketplace we utilized which allowed us to dispute the transaction with the marketplace if there was a discrepancy between what we paid for and what we received. This was another example of a piece of

information we learned during the process that increased our knowledge, and made us as a team feel confident achieving our overall goal of using Bitcoin to make a successful purchase from the Dark Internet. As we went through the steps of utilizing the Dark Internet in order to purchase a fake ID, we gained new information at almost every step, making us more comfortable with utilizing both cryptocurrencies and Dark Internet marketplaces. We believe if people who knew little to nothing about the process of using cryptocurrencies to make a purchase on the Dark Internet actually went through the process similar to us, they would also become more comfortable with the how cryptocurrencies and the Dark Internet function. If more of the general public could gain information of the intricacies and mechanisms of how the Dark Internet purchasing process work, it is possible that they could be more inclined to make a purchase similar to us, or simply engage in Dark Internet communication and culture.

Lastly, as our project evolved, we became more aware to the pitfalls of making digital transactions in order to acquire a product on the Clearnet, making us even more aware to the advantages of using the Dark Internet to make purchases. Before we attempted to purchase a fake identification, we wanted to hire a ghostwriter from both the Clearnet and the Dark Internet to write a mock essay for us. We wanted to do this, and allow English professors at our university to analyze the papers, so we could gain quantitative understanding of the papers differed from those purchased from the Clearnet and the Dark Internet. However, as we set out to purchase these papers, we arrived at two problems; the first being the lack of vendors on the Dark Internet, and the second being that the vendor's on the Clearnet never delivered the agreed upon product, which is the same thing that happened with the fake identifications. So out of the four different

products we attempted to purchase, the only product we successfully received was the fake identification from the Dark Internet. So for our specific experience, we were only able to make a secure and efficient purchase using the Dark Internet. Although we cannot conclude that the Dark Internet will result in a more secure transaction for every single product, from our experience, it was the only transaction that occurred without any discrepancies.

References

Angel, James, and Douglas McCabe. "The Ethics Of Payments: Paper, Plastic, Or Bitcoin?." Journal Of Business Ethics 132.3 (2015): 603-611. Business Source Complete. Web. 23 Feb. 2016.

Arendholz, J. (2013). (In) appropriate online behavior: a pragmatic analysis of message board relations (Vol. 229). John Benjamins Publishing.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency. In *Financial cryptography and data security* (pp. 399-414). Springer Berlin Heidelberg.

Bartlett, J. (2014). The Dark Net: Inside the Digital Underworld. *Random House*. ISBN: 0434023159

Berg J. (2016). The impact of anonymity and issue controversiality on the quality of online discussion. *Journal Of Information Technology And Politics*, *13*(1), 37-51. doi:10.1080/19331681.2015.1131654

Biddle, P., England, P., Peinado, M., & Willman, B. (2002, November). The darknet and the future of content protection. In *ACM Workshop on Digital Rights Management* (pp. 155-176). Springer Berlin Heidelberg.

Boykin, A. W., Tyler, K. M., & Miller, O. (2005). In search of cultural themes and their expressions in the dynamics of classroom life. *Urban Education*, *40*(5), 521-549.

Brightplanet. (2012, October 12). Deep Web Search and Dark Web Search - Similar Names; Major Differences. Retrieved from: http://www.brightplanet.com/2012/10/deep-web-and-dark-web-major-differences-

between-confusingly-similar-names/

Brito, Jerry and Castillo, Andrea. (2013). "Bitcoin: A Primer for Policymakers" (PDF). Mercatus Center. George Mason University. Retrieved 22 October 2013.

Burrell, I. (2014, August 28). The Dark Net:Inside the Digital Underworld by Jamie Bartlett, book review. Retrieved April 02, 2017, from http://www.independent.co.uk/arts-entertainment/books/reviews/the-dark-netinside-the-digital-underworld-by-jamie-bartlett-book-review-9696473.html.

Buskirk, J. V., Roxburgh, A., Farrell, M., & Burns, L. (2014). The Closure of The Silk Road: What Has This Meant For Online Drug Trading?. *Addiction, 109*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/.

Chen, H., Chen. C, Lo, L., Yang, S.C. (2008). *Online Privacy Control Via Anonymity And Pseudonym: Cross-Cultural Implications*. Behaviour & Information Technology 27.3 (2008): 229-242. Psychology and Behavioral Sciences Collection.

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd International Conference on World Wide Web* (pp. 213-224). ACM.

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160-175.

Dingledine, R. & Mathewson, N. Anonymity loves company: Usability and the network effect. D*esigning Security Systems That People Can Use*. O'Reilly Media, 2005.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation

onion router. Naval Research Lab Washington DC.

Dolliver, D. (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal of Drug Policy, 26*(11), 1113-1123. Retrieved November 3, 2015, from http://www.sciencedirect.com/science/article/pii/S0955395915000110.

Dolliver, D. S., & Kenney, J. L. (2016). Characteristics of drug vendors on the Tor network: a cryptomarket comparison. *Victims & Offenders*, *11*(4), 600-620.

Everett, C. (2009). Moving Across to the Dark Side. *National Security, 2009*(0), 10-12. Retrieved from http://dl.acm.org/citation.cfm?id=2304406.

Fuckgc. (2016, July). HE FUCKING DID IT!!! Message posted to https://www.reddit.com/r/DarkNetMarkets/comments/4pquar/he_fucking_did_it/?st=IZIO0I22&sh=22297470

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *new media & society*, *18*(7), 1219-1235.

Greenberg, A. (2014). Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains | WIRED. Retrieved December 11, 2014, from http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

Harrison JR, Roberts DL, & Hernandez-Castro J. (2016). Assessing the extent and nature of wildlife trade on the dark web. *Conservation Biology : The Journal Of The Society For Conservation Biology*, *30*(4), 900-4. doi:10.1111/cobi.12707.

Horsley, J. S., & Barker, R. T. (2002). Toward a Synthesis Model for Crisis Communication in the Public Sector An Initial Investigation. *Journal of Business*

and Technical Communication, *16*(4), 406-440.

In brief. (2014). Network Security, 2014(9), 3. doi:10.1016/S1353-4858(14)70086-8.

Isaacson, B. (2014, January 30). The Deep Web Is Filled With Drugs, Porn And ... Book Lovers(!). *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2014/01/30/illegal-libraries_n_4682897.html.

Jandt, F. E. (2015). An introduction to intercultural communication: Identities in a global community. Sage Publications.

Jardine, Eric, The Dark Web Dilemma: Tor, Anonymity and Online Policing (September 30, 2015). *Global Commission on Internet Governance Paper Series, No. 21.*

Kiesler, S. (2014). Culture of the Internet. Psychology Press.

Kleiman, J. A. (2013). Beyond the silk road: unregulated decentralized virtual currencies continue to endanger US national security and welfare. *Nat'l Sec. L. Brief*, *4*, 59.

Knorr, Caroline. What Every Parent Should Know About The Dark Web. *The Huffington Post*. 2016. Retrieved from http://www.huffingtonpost.com/common-sense-media/what-every-parent-should-know-about-the-dark-web_b_8046106.html

Koblitz, N., & Menezes, A. J. (2016). Cryptocash, cryptocurrencies, and cryptocontracts. *Designs, Codes and Cryptography, 78*(1), 87-102.

Kushner, D. (2015, October 22). The Darknet: Is the Government Destroying 'the Wild West of the Internet?'. Retrieved November 3, 2015.

Levine, Yasha (16 July 2014). "Almost everyone involved in developing Tor was (or is) funded by the US government". *Pando Daily*. Retrieved 30 August 2014.

Luther, William J. (2013, September). Cryptocurrencies, Network Effects, and Switching Costs. Mercatus Center, George Mason University.

Maddox, Alexia and Barratt, Monica J and Allen, Matthew and Lenton, Simon, Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital 'Demimonde' (September 8, 2015). *Information, Communication & Society, 1-16,* 2015, DOI: 10.1080/1369118x.2015.1093531.

Martin, J. (2014). Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs. Springer.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013, May). Zerocoin: Anonymous distributed e-cash from bitcoin. In Security and Privacy (SP), 2013 IEEE Symposium on (pp. 397-411). IEEE.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, *58*(1), 7-38.

Ortolani, P. (2015). Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin. Oxford *Journal of Legal Studies, gqv036*.

Owen, G., & Savage, N. (2015). The Tor Dark Net.

Lacson, W., & Jones, B. (2016). The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. *International Journal of Cyber Criminology*, *10*(1), 40.

Lapidot-Lefler, N., & Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers In Human Behavior*, *28*(2), 434-443. doi:10.1016/j.chb.2011.10.014.

Li, X., & Wang, C. A. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision Support Systems,*

95, 49-60.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013, May). Zerocoin: Anonymous distributed e-cash from bitcoin. In Security and Privacy (SP), 2013 IEEE Symposium on (pp. 397-411). IEEE.

Monetarists Anonymous. (2012, September 29). Retrieved April 02, 2017, from http://www.economist.com/node/21563752.

Nadarajah, S., & Chu, J. (2017). On the inefficiency of Bitcoin. *Economics Letters, 150*, 6-9.

Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Consulted 1.2012 (2008): 28.

Ortolani, Pietro. "Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin." *Oxford Journal of Legal Studies (2015): gqv036*.

P. Resnick and R. Zeckhauser. Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. *Adv. in Applied Microeconomics, 11:127–157*, 2002.

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *Academy of management review*, *23*(1), 59-76.

Perry, D.C., Taylor, M., & Doerfel, M.L. (2003). Internet-Based Communication in Crisis Management. *Management Communication Quarterly,* 17(2), 206-232. Doi:10.1177/0893318903256227

Peppas, S. C. (2001). Subcultural similarities and differences: an examination of US core values. *Cross Cultural Management: An International Journal*, 8(1), 59-70.

Pieters, G., & Vivanco, S. (2017). Financial regulations and price inconsistencies across bitcoin markets. *Information Economics and Policy*.

Polder-Verkiel, S. E. (2012). Online Responsibility: Bad Samaritanism and the Influence of Internet Mediation. *Science And Engineering Ethics*, *18*(1), 117-141. doi:10.1007/s11948-010-9253-z.

Postmes, T., Spears, R., Sakhel, K., & De Groot, D. (2001). Social influence in computer-mediated communication: The effects of anonymity on group behavior. *Personality and Social Psychology Bulletin*, *27*(10), 1243-1254.

Project, I. T. (n.d.). Tor. Retrieved April 02, 2017, from https://www.torproject.org/about/corepeople.

Reicher, S. D., Spears, R., & Postmes, T. (1995). A social identity model of deindividuation phenomena. In W. Stroebe & M. Hewstone (Eds.), *European review of social psychology, Vol. 6 (pp. 161-198)*. Chichester, UK: Wiley.

Rocco, D., Caverlee, J., Liu, L., & Critchlow, T (2005). *Exploiting the Deep Web with DynaBot: Matching, Probing, and Ranking*.

Santana, A. D. (2013). Virtuous or Vitriolic: The effect of anonymity on civility in online newspaper reader comment boards. *Journalism Practice, 8*(1), 18-33. doi:10.1080/17512786.2013.813194.

Scott, M. (2014). Irked by N.S.A., Germany Cancels Deal with Verizon. Retrieved from: https://www.nytimes.com/2014/06/27/business/angered-by-nsa-activities-germany-cancels-verizon-contract.html?_r=1

Soska, K., & Christin, N. (2015, August 12). *Measuring the Longitudinal Evolution of*

the Online Anonymous Marketplace Ecosystem. Lecture presented at Proceedings of the 24th USENIX Security Symposium, Washington, D.C.

Spotz, K. (2014, July 16). What I've Learned as an Internet Drug Dealer. Retrieved from https://motherboard.vice.com/en_us/article/what-ive-learned-as-an-internet-drug-dealer

Steinberg, Terrance. (2014, February 19). The Drugs Dilemma at World Economic Forum 2014: Right For Another Reason. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/common-sense-media/what-every-parent-should-know-about-the-dark-web_b_8046106.html

Suler J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior : The Impact Of The Internet, Multimedia And Virtual Reality On Behavior And Society*, *7*(3), 321-6.

Tor Project. (2011). Anonymity online. Retrieved from http://www.torproject.org/ (20.09.12).

Tyler, K. M., Boykin, A. W., Miller, O., & Hurley, E. (2006). Cultural values in the home and school experiences of low-income African-American students. *Social Psychology of Education, 9*(4), 363-380.

Ulbricht, R. (2015) Letter to Judge Forrest, United States District Court of Southern District New York, United States of America v. Ulbricht. Case 1:14-cr-00068-KBF Document 251-1 Filed 05/22/15.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59*(11), 15-17.

Van Hout, M. C., & Bingham, T. (2013). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy*, *24*(5), 385-391.

Vaishampayan, S. (2013). Silk Road drug market handled $1.2 billion of transactions in 2.5 years before FBI seizure. Retrieved from: http://blogs.marketwatch.com/thetell/2013/10/02/silk-road-drug-market-handled-1-2-billion-of-transaction-in-2-5-years-before-fbi-seizure/

Vogt, S. D. (2017). The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. *Santa Clara Journal of International Law*, *15*(1), 104.

Voiskounsky, A. Online Behavior: Interdisciplinary Perspectives for Cyberpsychology. *Annual Review of Cybertherapy and Telemedicine 2016*, 16.

Whitaker, R. (2015, July 14). Why I Had to Buy My Wife's Inhaler on the Dark Web. Retrieved April 3, 2017, from https://motherboard.vice.com/en_us/article/why-i-had-to-buy-my-wifes-inhaler-on-the-dark-web

2016, June 25. Retrieved April 3, 2017, from https://www.reddit.com/r/DarkNetMarkets/comments/4pquar/he_fucking_did_it/

Appendix A
Textual Coding Cheatsheet

Behaviors or Expressions: Each behavior/expression will be assigned a number

1. Movement Expressiveness - rhythm of speech patterns
2. Verve - receptiveness to high levels of stimulus
3. Affect - emotional response to high levels of stimulus
4. Orality - knowledge gained that is passed on through word of mouth
5. Communalism - feeling of duty towards community
6. Individualism - feeling of autonomy
7. Competition - individual's need to do better than peers
8. Object Orientation - person's association of self value with material possessions
9. Cognition - objective and rational reaction to events
10. Bureaucracy Orientation - focus on structure and rules*

Expression Occurrence

(I) Initiation (of a cultural behavior or expression)
(R) Reaction (of a cultural behavior or expression)

Individual Displaying Behavior/Expression:

(U) User
(A) Author/administrator of webpage

Type of Reaction (if applicable, which will appear next to the expression occurrence as a postscript):

(+) Positive
(-) Negative
(n) Neutral

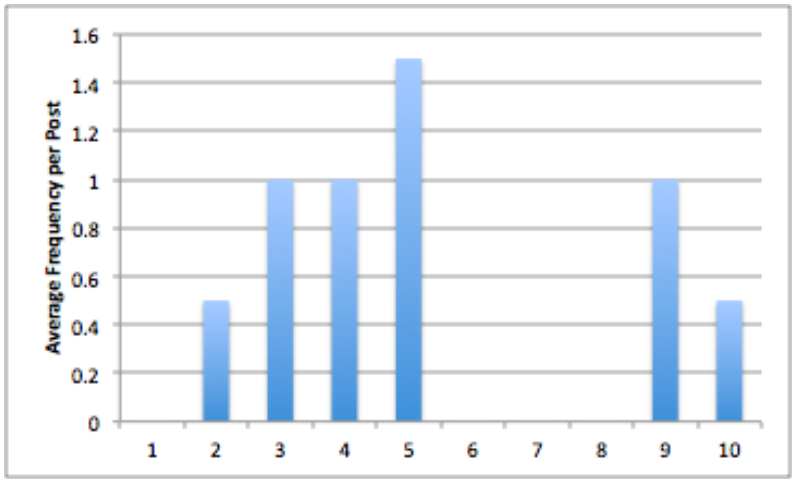
Display Directed towards

(p) Peer/another user
(a) Author

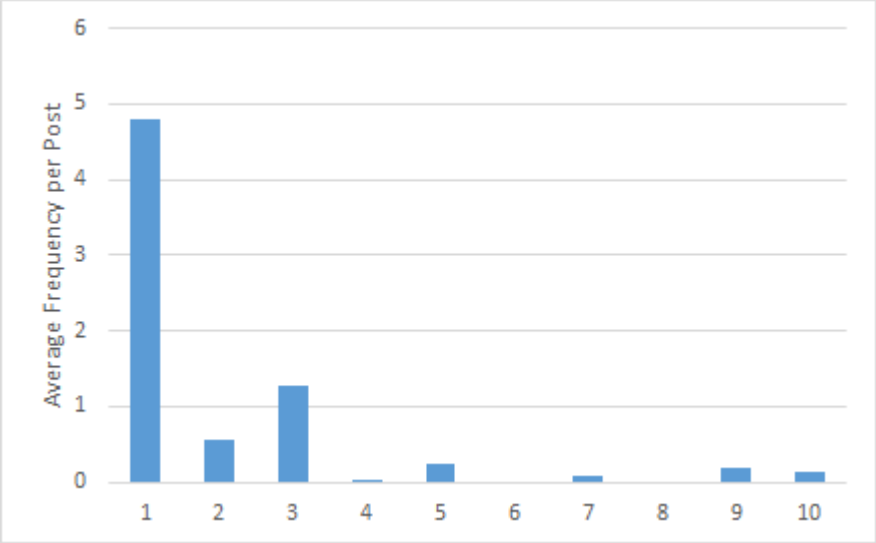
Outcome of Behavior or Expression

(A) Affirmation
(D) Disaffirmation
(N) Unspecified

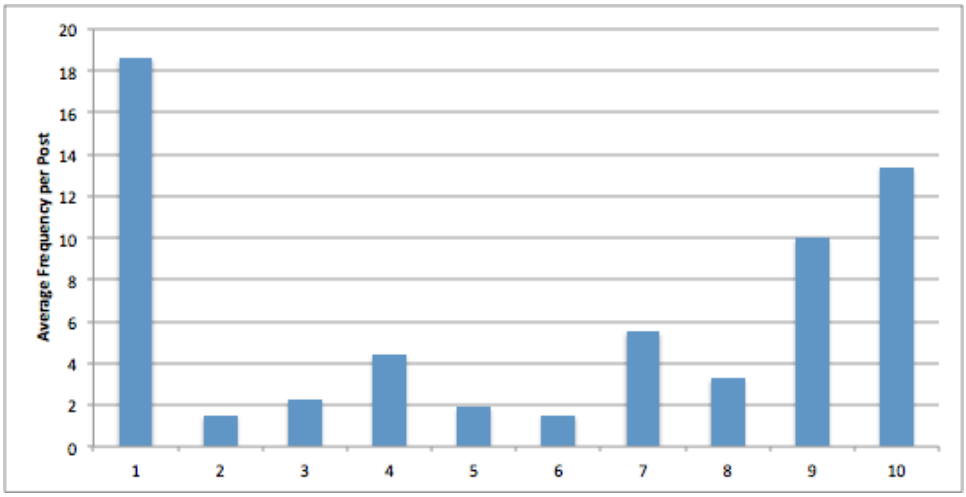
Appendix B
Average Behavior Occurrences for Silk Road



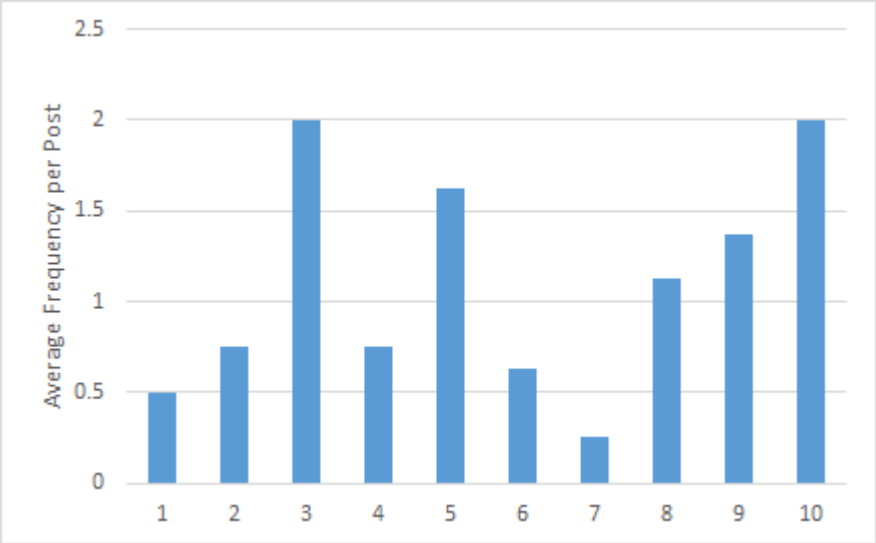
Appendix C
Average Behavior Occurrences for The Hub



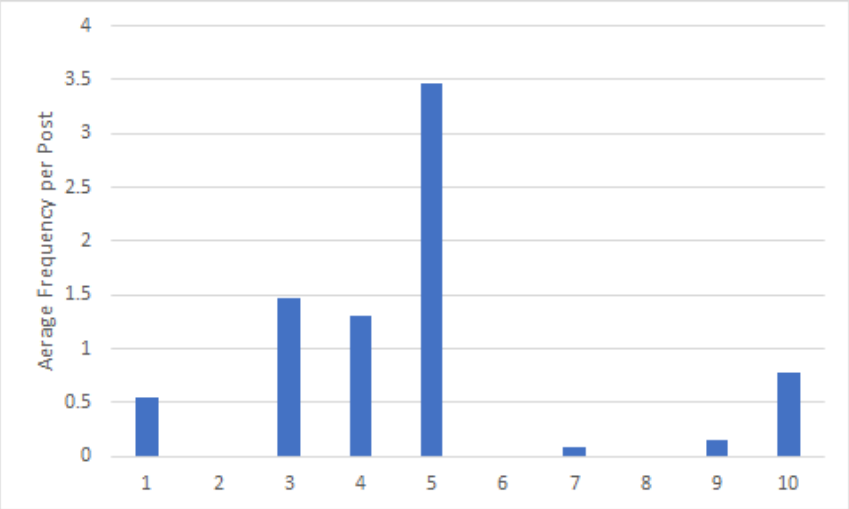
Appendix D
Average Behavior Occurrences for Intel Exchange



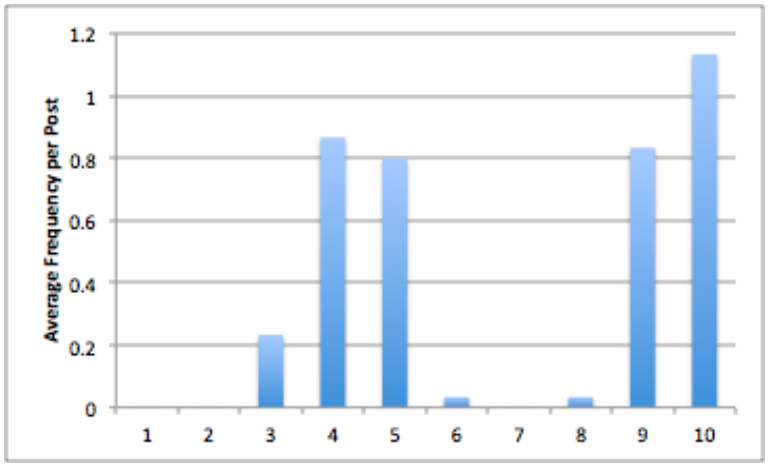
Appendix E
Average Behavior Occurrences for Reddit



Appendix F
Average Behavior Occurrences for Wired



Appendix G
Average Behavior Occurrences for Motherboard



Appendix H
Average Behavior Occurrences for Huffington Post