Team DIRE Research Proposal

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

Mentor: Jon Hoffman

University of Maryland: Gemstone Program

*We pledge on our honor that we have not given or received any unauthorized assistance on this assignment.*

**Abstract**

Team DIRE’s research involves investigating the sociocultural interactions of various sectors of the Dark Internet. This proposal aims to show that the level of anonymity available to the user has a direct correlation between the lingual and cultural differences in interactions between those of the Dark Internet and the public Internet. It also provides a collection of current information about the Dark Internet that has been gathered to justify the need for further research in order to expand upon the relatively small assemblage that exists thus far. Specifically utilizing the Tor Browser, Team DIRE plans to study this correlation by analyzing four subjects of the Dark Internet: Dark Internet traffic analysis, marketplaces, marketplace consumer experience, and Bitcoins. The overarching goal of this paper is to outline the methodology of developing new knowledge about the current sociocultural impacts of anonymity of the Dark Internet.

**Introduction**

As the Internet has increasingly developed as the world’s main source for information and communication, online security of the individual has become all the more necessary. Tor, otherwise known as Onion Routing, is a virtual privacy network that enables the user to operate online under nearly impenetrable anonymity, thereby protecting the identity and personal information of the user by reducing risk of their information being compromised (Goldschlag et al., 1999). Any website that is available on the public Internet that the average person might use everyday is also available on Tor. It should be noted that Tor is a network host on the Dark Internet (sometimes called the Darknet), which is comprised of all of the websites and network hosts that have intentionally been hidden and are accessible *only* through networks such as Tor (Goldschlag et al., 1999).

The Dark Internet’s degree of anonymity results in increased personal privacy and freedom for the user, which facilitates development of a distinctive culture. The Dark Internet has expanded the freedom of Internet users: it provides the ability to surpass censorship by citizens living under oppressive governments, and gives others the opportunity to act as whistleblowers and dissidents that expose corruption, all while maintaining complete anonymity and personal privacy. Economic developments have occurred alongside the expansion of the Dark Internet as well; online cryptocurrencies and expansive marketplaces have flourished, attracting buyers and sellers from all over the world. Despite the progress these economic innovations have made in recent years, little conclusive research has been done on the topic to date, and thus the future of these online marketplaces and currencies and their potential impact on society remains uncertain.

bitcoin, the anonymous cryptocurrency, is becoming increasingly prevalent in mainstream commerce, and has recently become available on many popular public Internet services, despite its shaky history and tendency to succumb to inflation. The Federal Government has shut down some Dark Internet marketplaces for their prevalence in the buying and selling of illegal goods and services numerous times, but to no avail: these marketplaces have simply reemerged soon after their shutdowns, or others have quickly come forth in their place. The Dark Internet economy has proven to be extremely resilient, as it has persistently continued to expand in both size and popularity in spite of major current events that have threatened to undermine its security and existence as an online network and resource.

Team DIRE plans to analyze Dark Internet traffic and its changes after key events, themes prevalent on the Dark Internet, and bitcoin’s use as a form of currency in the Dark Internet market experience. Our research will be conducted through an economical and sociocultural lens, which will allow us to analyze the impact of Dark Internet developments, economic and social, on Dark Internet culture (through analyses of online web forums), and determine the extent of which external current events and social phenomena have influenced these innovations.

**Literature Review**

**Introduction**

The Dark Internet is a form of Internet based in anonymity; the concept of complete browser anonymity attracts a variety of people looking to keep their identities private in any cyberspace transaction. 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 a result of numerous components that contribute to the overall anonymity it provides. One of its most significant features is the Tor browser, the primary method for accessing sites on the Dark Internet itself. Among many other purposes, one of the most popular and notorious uses of the Dark Internet is for the trade of illegal items. The drug trade in particular has been revolutionized by online marketplaces that offer mass accessibility and a comparatively strong level of anonymity for secure transactions. Another important area that should be considered for analysis is the role of bitcoin, the first fully implemented decentralized currency. Its ability to anonymize trade means that it has found natural and widespread usage when used for illegal trade. While the Dark Internet is a 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.

**Background**

**Structure.** Onion Routing was developed in 2003 by the Office of Naval Research as a model for anonymous Internet usage (Dingledine et al., 2004). The idea of the routing was then used by civilians to create Tor, which uses layers of encrypted messages in order to conceal the identities of both the sender and receiver in any Dark Internet exchange. The layers of encryption are used to create circuits that can step from one anonymous source or “node” to another (Dingledine et al., 2004). When using this method of routing, one takes a pathway that goes through the network, building a circuit that will connect from one’s router (or node) to the next, but prevent the ability to identify any other nodes within the circuit (Dingledine et al., 2004). Each time the information reaches a new node in the circuit, a layer of encryption is removed until it is decrypted and ready to be sent to its final destination. This creates a node where the information is fully decrypted, often call an exit node. As such, if someone were to be looking at an exit node, while they would not be able to see who the information was coming from or going to, they would be able to track what that information contained (McCoy et al., 2008). Unfortunately, this first Tor had several setbacks, which established the need for a more advanced anonymous browser, which would be called Tor (Dingledine et al., 2004). Any one dysfunctional node on the original onion routing system could take note of all browser activity and, due to its glitch, expose the position of all nodes in the circuit (Dingledine et al., 2004). To circumvent this, Tor installed a session key that would be used before each "hop" from one node to another (Dingledine et al., 2004). The session key uses encryption to hide any communication between two computers. This means that if one node is compromised it cannot access any user activity from other nodes without the session key. However, the server must first detect whether or not a node is compromised in order for it to withhold the session key. The most efficient way of detecting dysfunctional nodes is called an alert-based approach (Zhang et al., 2008). In this approach, a sensor node is established that can detect certain signals that would alert it to a compromised node, this way the nodes are monitored without being able to track their whereabouts (Zhang et al., 2008).

Though there is existing research into specific facets of the Dark Internet as well as its technical make up, there is not much literature on the Dark Internet as a whole. It should be noted that the Dark Internet is a different entity than the Deep Web, which is better known and researched. In particular, the Deep Web refers to a web server that cannot be found using typical search engines, such as Yahoo or Google (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). While the difference between these two terms is minute, it is a key distinction to make, as it is the Dark Internet, in particular the Onion Network, is vastly under researched. 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.

Innovations in technology have the ability to transform society as a whole because they enable humans to interact in an entirely different way. From the printing press to the Internet to Facebook and Twitter, society has been revamped with every new development (Levy et al., 1999). They all have to do with the dissemination of information, each new breakthrough molds societal interactions. The printing press enabled the everyday person to be both knowledgeable and up-to-date on current events (Silver, 2012). The Internet usurped physical distance to connect anyone and everyone through cyberspace (Levy et al., 1999), Facebook allowed people to share their lives with any friend or acquaintance and Twitter gave every person a voice. Understanding and acknowledging the impact of Twitter, a channel through which anyone can relay their thoughts to a mass audience, can aid in societies’ evolution. Inconsistencies and injustices that occur in real time are discussed and relayed almost immediately on Twitter (Kwak et al., 2010). Twitter gave the restless people under the authoritarian reign of Hosni Mubarak an outlet to express their indignation. This ability to connect to anyone, anywhere through similar interests facilitated the organization of a revolution that overthrew the 30-year reign of Hosni Mubarak in Egypt (Hounshell, 2011). Today, it would be naive of any government not to consider Twitter while making landmark decisions, as many of those affected by such decisions will make their voice heard. It is only natural that this new channel of information, the Dark Internet, will immensely affect society as well. In order to predict and analyze how the Dark Internet will impact society, research into its community as a whole needs to be done. Team DIRE plans to investigate how the Dark Internet affects current forms of exchange, tradewise and culturally, and how use of the Dark Internet has been affected by major current events.

The development of Tor and its ability to connect with other anonymous nodes became the foundation for various projects seeking to create systems that could avoid all forms of censorship, as mere encryption itself does not hide routing information, which contains a user’s browsing trail and previous activity (Dingledine et al., 2004). The Free Haven Project, which began in 1999, aspired to develop a means of anonymous online storage that could not be infiltrated by higher governing powers (Dingledine et al., 2004). The Eternity Service project also looked to create an anonymous storage medium using elements from the concept of Tor (Anderson, 1996). The Office of Naval Research created The Onion Routing as a way to protect any sensitive government information communicated through the Internet, but now is used by anyone preferring to use the Internet without risk of censorship or observance by government officials.

**bitcoin.** The Dark Internet has led to countless groundbreaking economic innovations that have transformed online commerce: a relatively new form of virtual currency called the bitcoin, has bloomed in public usage on the Dark Internet. Since its introduction in 2009, bitcoin has emerged as a major form of capital in the online marketplace, with over thirteen million bitcoins in circulation as of August 2014 (Bartlett, 2014). The bitcoin’s popularity can be largely attributed to it being a crypto currency, which is an alternative to traditional government-issued money. It utilizes cryptography in order to ensure the security of the online transactions, prevent users from spending the same digital notes more than once, and to govern and monitor the supply of these notes in circulation (Luther, 2013). The Silk Road, an anonymous online marketplace that can only be accessed on the Dark Internet, accepted bitcoin as its sole exchange currency until it was shut down in October of 2013 (Christin, 2013). Crypto currencies such as bitcoin effectively allow international online trade to commence with ease, which has led to the creation of numerous marketplaces on the Dark Internet.

**Online markets.** By far the most famous of the Dark Internet’s marketplaces, the Silk Road was initially founded some time in February of 2011. Its operator then went by the alias of “The Dread Pirate Roberts”, and was already well known for possessing strong libertarian and anti-regulation viewpoints. The site acquired notoriety only a few months after it’s founding, when the blog Gawker featured it in an article that emphasized its potential for drug purchasing and trafficking. Not long after this shot of publicity, the U.S. Government began a campaign to shut the website down, and ultimately arrested several drug dealers and purchasers who had been operating through the Silk Road. In October of 2013, the U.S. Department of Justice arrested a San Francisco man named Ross William Ulbricht, alleged to be the true identity of “The Dread Pirate Roberts”. As of this writing, Ulbricht has confessed to none of the charges the federal government has brought against him; his trial is currently scheduled for January of 2015. Simultaneous with Ulbricht’s arrest, the United States government attacked the Silk Road website itself. Throughout 2013, the Federal Bureau of Investigation seized thousands of bitcoin worth millions of dollars from Silk Road accounts, and ultimately shut down the entire website.

While the FBI hoped that the shutdown would heavily diminish online drug sales, it appeared that the opposite had actually taken place. Led by a new pseudonymous Dread Pirate Roberts, administrators from the original Silk Road re-launched the site in November 2013 just a month after its shutdown. This revitalization was named Silk Road 2.0 with the same setup as the original, but also with the promise of improved security. The new site nevertheless had its share of turbulence, most notably in the form of vulnerability in the site’s “Refresh Deposits” function. As a result of this, $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 8. However, Silk Road 2.0 was eventually shut down a year after its development, as a result of efforts by US and European agencies. Its alleged administrator who went under the pseudonym “Defcon” was arrested, and additional markets such as Cloud 9 were also targets of this operation. Although law enforcement agencies sought to publicize their success, numerous other prominent markets such Agora and Evolution were unaffected, likely due to the professionalism of their operations as well as more advanced security. Agora already contained more listings than Silk Road 2.0 before the shutdown with Evolution also expected to overtake Agora.

**Significance.** The 21st century has been a time of exponential acceleration in the growth of technology. These developments include many tools and resources that can improve societies through a wider spread of new knowledge or advanced cyber security. Nevertheless, the amount of information that we are lacking is far greater than the information that we know and comprehend. The Dark Internet consists of 5-25% of the total net - depending on who was asked- and has been increasing at the rate of about 2% each year (Everett, 2009). To date, there are few individuals (including government officials) that thoroughly comprehend the concept of the Dark Internet. The gap in knowledge and current information surrounding the Dark Internet unnerves society and prevents its potential benefits from being explored and exploited thoroughly. For these reasons, it is important that our team research the sociological and cultural interactions of the Dark Internet, especially as it becomes more relevant to daily life.

It is important to note that there are varying levels of awareness of the Dark Internet: (1) people who are completely unaware of its existence entirely, (2) those who might only know facts about it through what has been said throughout the news or when it has been referred to in pop culture and (3) those that have an in-depth familiarity with the Dark Internet who use it regularly. The obstacle that society needs to overcome is their lacking of general knowledge of the Dark Internet. The media mainly focuses on the darker side of the Dark Internet--the side that contains illegal pornography, black market trading and terrorist activity. Despite these criticisms, there are copious amounts of legal reasons that draw people to utilize the Dark Internet, such as personal online security and anonymity.

 One of the fundamental reasons civilians use the Dark Internet is to ensure personal online security (Dingledine et al., 2006). It is a common desire held by individuals to keep their usage on the Internet free from tracking, however, this does not necessarily mean these users are participating in illegal acts. For example, there are times when someone needs to reveal vital information about potentially dangerous parties. These situations can include an individual acting as a “whistleblower” speaking up against his or her corporation, or **e**ven a criminal informant divulging information to a journalist.

Websites such as *The New Yorker*’s Songbox, allow users to exchange secure information without the fear of being tracked (Aked et al., 2013). However, the United States government has demanded control and/or unlimited access to these websites, to ensure privacy and protection of their assets. A momentous example of a recent exchange of secure information was when a former National Security Agency (NSA) subcontractor, Edward Snowden, published mass surveillance programs run by the NSA and the Government Communications Headquarters (GCHQ). Although Snowden later revealed himself to be the source of the leak, he was able to anonymously report information that revealed concerns about domestic surveillance and information security.

Higher authorities are not the only reasons why users might feel as though they are in danger: another major use of the Tor browser is to prevent third parties from discovering individual activity. This is essential for victims of domestic abuse or stalking to achieve a greater level of security from threats. Through anonymity achieved by the use of the Tor Network, victims are able to use the Internet safely without being tracked by potential assailants.

Many people use the Dark Internet as a crucial tool to allow one to safely bypass the censorship that oppressive governments impose on their people. However, the Great Firewall of China (GFC) prevents Chinese users from accessing the public Tor network (Winter & Lindskog, 2012). The chances of bypassing the GFC are minuscule, meaning that those who choose to utilize the Internet are forced to sacrifice their privacy. Personal safety, Internet security and censorship bypass are among many significant examples of how the Dark Internet can be exploited to benefit the general public.

**Gaps in Current Research**

Despite numerous advances in the Dark Internet’s popularity and mainstream usage, specific parts of it remain a great mystery to most. Specifically the online marketplace Agora, bitcoin usage, and the specific traffic patterns (which can be examined through exit nodes) of the Dark Internet have not been studied in depth. 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, including 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 (Rocca 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 previously unavailable by censorship of one’s government, 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.

An exit node, which is the final “jumping off” point for Dark Internet users, would allow our research team to observe the web destinations of Dark Internet users whose servers have been randomly sent to our node, thereby providing a random sample of web destinations of the Tor network as a whole. A plethora of exit nodes exist currently, however, in order to examine the different sites Tor users are visiting, we would need to set up our own. This is something that has not been accomplished by researchers in the past, and by doing this, we could potentially provide useful data about the variety and frequency or sites visited by Tor users.

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 as currency and their overall effectiveness and usage among online marketplace users. As of right now, there are significant studies that have 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 Agora and other 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 been done to analyze specific groups of people such as the case study done on cyber terrorism (Chen et al., 2008), our group could adapt this research 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. Specifically, we hope to research and analyze users on the largest Dark Internet marketplace, Agora. 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 Agora. In order to take it one step further, we can compare the user interactions of Agora to other competitive online marketplaces such as Amazon to see how behaviors on Agora vary from the public Internet where there is no anonymity at all in order to create a bridge between the Dark and public Internet (Christin, 2013).

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 Silk Road have thriving forums where users can congregate to discuss the site and its services.

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 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. However, people that consider themselves a part of a close online group of friends can also feel more comfortable, affecting their behavior online.

**Potential Impact**

The Dark Internet has become a prevalent topic in the United States and has received a substantial increase in attention by major news outlets almost daily, especially as it pertains to the development of online cryptocurrencies. The bitcoin’s emergence as the most widely used form of cryptocurrency has lead to various developments in the Dark Internet; copious amounts of drugs and other illicit materials have been bought on Dark Internet Marketplaces using bitcoins (Levin et al., 2014). Those who profited off of selling these illegal goods have been able to then successfully launder their profits on the Dark Internet using bitcoins. Despite the illegality of much of the online commerce conducted through the use of the bitcoin, the cryptocurrency is projected to continue to grow in popularity and widespread usage (Darlington, 2014).

It is not simply the development of the bitcoin that has brought attention to the Dark Internet; the wide variety of innovative ways for which the Dark Internet can be used (that the public Internet is not capable of) has given it a major boost in media attention. For example, Dark Internet marketplaces such as Agora (and previously Silk Road) have seen an increase in users as of late. After the FBI raid of the original Silk Road, the number of sellers on Silk Road doubled six weeks after Silk Road 2.0 opened (Buskirk et al., 2014). As the Dark Internet continues to develop and expand, the number of different uses it can be exploited for will most likely increase, in addition to the number of users. If significant academic research were to be conducted on the Dark Internet, it would likely gain attention from not only academic circles, but the general public as well. Now is the opportune time for our team to capitalize on the current situation and conduct one of the very first research studies dedicated to the Dark Internet, as it still remains a new and enticing mystery to most.

**Conclusion**

The Dark Internet is a forum for anyone who wishes to maintain privacy and anonymity within the cyber world. The Dark Internet is a steadily growing innovation used for the distribution of information, market transactions, and cultural connectivity, not unlike the public Internet. The distinction between the two is that all these actions may be done in complete privacy of the user on the Dark Internet, which makes all the difference. People are prone to behave much differently under the cover of anonymity. Consequently, studying the Dark Internet can enable our team to view an altered subculture in which people engage in discussion and commerce unlike anywhere else, as many are completely comfortable in their ability to do or say whatever they want without fear of retribution. As Dark Internet usage expands, its shadowy culture that appears foreign and mysterious to us now may soon become customary and indisputably affect society. Therefore, it is of the utmost importance to study the Dark Internet and its users as it stands currently in order to enable our team to draw conclusions and make inferences about the culture as a whole and forecast its future impacts on our society.

**Methodology**

**Introduction**

The Dark Internet is a form of anonymity that boasts complete browser identity protection, leading to private transactions by people looking to avoid observance by governments or major corporations (Brightplanet, 2012). Current research on the subject is very limited as it exists solely as evaluations of the structure of the Dark Internet and analyses of anonymity as a concept (Brightplanet, 2012). Team DIRE, however, plans to analyze Dark Internet traffic and its changes after key events, themes prevalent on the Dark Internet, and bitcoin’s use as a form of currency in the Dark Internet market experience. Team DIRE has divided our methodology into these three sections and will analyze each of the methodologies for these sections in detail.

**Aim 1: Dark Internet Traffic**

**Research Question and Hypothesis.** Our team will attempt to answer the following research question: how do current events affect use of the Dark Internet? We hypothesize that by observing web destinations of Dark Internet users by way of an exit node, we will be able to draw a correlation between changes in Dark Internet web traffic patterns and current events. The Dark Internet has gained increasing attention as it has been tied to many recent events, most notably the FBI seizures of the Silk Road online marketplace in October of 2013 and of the Silk Road 2.0 in November of 2014; these incidents have caused users of those marketplaces to transfer their business elsewhere, creating changes in the overall use of the Dark Internet.

**Sample Information.** The simplest way to acquire this information would be to have direct access to an exit node, be it on campus or not. With access to an exit node, our team would be able to capture some basic information about the destination of a request sent through it (McCoy et al., 2008). With direct access to the machine the exit node is set up on, we will be able to capture, or save, part of the information being sent through the node. In particular, we would be able to save basic information of what is contained within the packet of information (McCoy et al., 2008). Access to one exit node would provide a random sample of the overall web destinations of users on the Tor network. With logs taken at various intervals, our team would be able to obtain a reasonable amount of information as to the traffic trends of Tor network users. Even though this is a small portion of all Tor network users, any significant trends that appear can show a trend throughout the whole network.

 However, as our team’s access to an exit node is pending, we need an alternative to acquiring this information. While the amount of information gathered would not be as large, it is still possible to gleam pertinent information without direct access to an exit node. As the University of Maryland already has a relay node operational, it would be possible to access the Tor network and retrieve some basic information on traffic through those means (Murdoch et al., 2005). We could also use a similar method as with an exit node, capturing IP addresses for the previous and next hop in the circuit (McCoy et al., 2008). These methods would not be the ideal, as the information gleaned would not be nearly as comprehensive as information from an exit node directly.

**Data Collection.** We will begin our data collection by establishing an exit node that will provide us access to observing Dark Internet web traffic. Setting up an exit node on the University of Maryland campus (pending approval by the UMD IT Department) will allow us to observe traffic patterns of Dark Internet users and thus infer the influence of current events on these traffic patterns. A sub-group of Team DIRE members will be organized to set up the exit node and collect its subsequent data for further analysis to be conducted, in part, by all members of the team. Though the Tor network allows individuals to surf the web anonymously, this is not without some limitations: the last node (thereby named the “exit node”) in the encryption process used by the Tor browser through which traffic passes in the network must decrypt communication before delivering it to its final destination. The bytes passing through this server can be viewed by the individual operating the node. As such, an exit node on campus will allow us to track traffic in and out of the network, and thus track more viably the usage of the Tor network (Harrop et al., 2005). The exit node can be considered a chink in the Tor network’s armor, as code that is not protected by cryptographic protocols (namely Transport Layer Security) could be compromised (Dierks & Rescorla, 2008). As such, team DIRE will operate our exit node so as to solely track and record web browsing destinations of Tor users, and not that of their private communications, transactions, and identities in order to conduct our research in an ethical manner. A confounding variable our team may encounter throughout the implementation of this methodology is the inevitable inability to observe and record traffic destinations of Tor users who have employed further security by the use of cryptographic protocols, as their code is encrypted beyond the capacity to be read by an exit node.

 **Data Analysis.** As described previously, our team will gather data from the exit node. However, in order to analyze such large quantities of data, we must make a chart describing frequency of traffic to sites on the Dark Internet per a specified time period that Team DIRE will decide on at a later date, after having observed the amount of traffic our exit node normally receives. Our data gathering will be an ongoing process that will begin immediately after we have established an exit node, or contact with the owner of an exit node.

 After we have been gathering data for at least 2 months, then we can begin our initial data analysis. A time span of 2 months will allow our team to collect a sufficient amount of data in order to observe patterns in web traffic, which could then be analyzed in order to determine if a correlation exists between web traffic trends and major events that occur within these 2 months. In order to analyze the data that we have collected, we will need to have compiled the major events that have occurred during our data collection and the time in which they occurred. Using statistical methods, we will analyze the effect that each major event had on Dark Internet traffic. This analysis will occur through NHST (Null Hypothesis Testing) for each event we wish to analyze. To analyze our results we will establish a null hypothesis (H0), which will predict no change in Dark Internet traffic to a site, and an alternative hypothesis (H1), which will predict any change in Dark Internet traffic to a site (either more or less). We will set α (alpha) to .05, as it is the standard (Wilkinson, 1999).

We will then analyze our results observed using an ANOVA, a statistical analysis test, to initially test whether the current even had an effect on the traffic to various websites based on the average traffic to various website before the event (the population mean) and the average traffic to various websites after the event (the sample mean). This analysis assumes that we are randomly sampling small groups of the population through the exit node with no repeated individuals in the groups before the event and after the event. ANOVA will allow us to see if an event had an effect on the traffic of Dark Internet users before we do more in-depth analysis through the use of t-tests to test the directionality of this change and where it is occurring. Our team will use ANOVA initially because if the test shows that there is no change and we are unable to reject our null hypothesis, then there is no need to undergo the process of multiple t-tests for the various websites testing their traffic before and after the event.

 Our data collection and data analysis will be an ongoing project; data collection will begin once we have established contact with an exit node and data collection will begin approximately 2 months after that. Data analysis will involve the identification of events that occur both inside and outside of the Dark Internet before analyzing each event’s effect. We will be collecting data and analyzing data as we proceed throughout the rest of our project. Data collection and analysis will both cease the summer of 2016.

 **Anticipated Results.** From our research we hope to be able to analyze how events around the world affect the ongoing traffic on the Dark Internet by collecting data on the general traffic of the Dark Internet in order to establish a baseline before major events occur, and determine our ability to chart changes in Dark Internet traffic. The analysis of these results will allow our team to describe the effect that various events have on Dark Internet traffic, such as the changes that occur when a major site such as Silk Road or Silk Road 2.0 is shut down. For example, if the bitcoin were to suddenly increase immensely in value, it is likely that Dark Internet websites selling bitcoin would experience a considerable rise in user traffic. Having successfully observed the relationship between current events and Dark Internet traffic, our team will be able to gain a better understanding of the Dark Internet community and make predictions about future changes in the flow of Dark Internet traffic.

**Aim 2: Dark Internet Marketplaces**

**Research Question and Hypothesis.** Marketplaces on the Dark Internet provide an extremely unique and valuable opportunity for cultural analysis. Large volumes of illegal items, primarily drugs, are sold through the anonymity provided by Tor and bitcoin. On message boards for these various sites, users can discuss various aspects of the online drug trade from vendor discussion to drug safety. Analyzing the content of forums enables us to learn more about actual users of these marketplaces and the vast drug culture in which they are involved. We can gain valuable knowledge on topics such as the operation and ideals of these sites. As a result, our goal is to answer the following research question: What does the difference in the anonymity levels reveal about Dark Internet user language and culture through prevalent themes on the Dark Internet? We hypothesize that anonymity allows freedom from repercussions; therefore users of the Dark Internet will display different behaviors than users of message boards over the public Internet. Due to the anonymity and the illegal nature of the Dark Internet, it is hypothesized that communication is more trust based than interaction on the public Internet.

**Sample Information.** In order to draw inferences on the culture of the Dark Internet from the interactions of Agora, the current top online marketplace found on the Dark Internet, users we will be employing textual analysis. Agora is the current top online marketplace found on the Dark Internet. Text can be used to gain understanding on the author’s, or in our case the user’s, thought process (Carley, 1994). Thus, textual analysis can be used to understand a person’s mentality. Humans interact through symbols, most notably language; this is what creates a social world and presents the basis of culture (Knorr-Cettina, 1981). Therefore, once we understand the mental model of the user one can move on to draw inferences about the culture that molds this mentality because language facilitates the growth of both cognition and culture (Carley, 1994). The previous text analysis study we are basing our method on uses coding to classify different topics into categories (Carley, 1994). We will modify this method by defining topics that relate to Agora such as drugs or weapons. We will count how often our chosen topics appear and create subcategories within largely used topics in order to understand, more specifically, what users are doing on Agora and why they are doing it. The previous study, (Carley, 1994), also used textual analysis as the means to a different goal than our research, it looked to connect cognition and culture as a relationship that evolves together (Carley, 1994). Our team will use both concepts but instead of attempting to exemplify a relationship between cognition and culture we will be using the information we gather about the users’ mentality to draw conclusions about Agora user culture.

The method of coding different categories has also been applied to the analysis of discussion board postings (Song & McNary, 2011). This study analyzed the online interaction patterns on a discussion board for students in a graduate course. Some areas of investigation were variability in the types of posts and changes in the types of posts over time that may have occurred. These goals are highly relevant to our research in terms of the vast array of topics that can be discussed on Agora message boards. In addition, the study sought to find any difference between students in the frequency and patterns of posts they made. We can also apply this in our data collection by observing the posting behaviors of different users and ways in which communication could be affected.

**Data Collection.** In order to quantitatively analyze the text on forums, message boards, and blogs, we will utilize a computer program to objectively compare the tone of text between varying degrees of anonymous interactions. Specifically, we will use a computer-aided text analysis program, *DICTION* *Software*, to establish a baseline and understand the characteristics of the different interactions.

The software will use specific dictionaries that search text for the following qualities: *certainty, activity, optimism, realism*, and *commonality*. The *certainty* index will search for language indicating resoluteness and inflexibility. *Activity* searches for languages that features movement, change or the implementation of ideas. The *optimism* index will identify language endorsing positive components of the endorsement of a certain person, group or thing. *Realism* finds tangible and immediate language. Finally, the *commonality* index finds language that highlights common values of idiosyncratic modes of agreement (“DICTION Overview”, n.d.).

However, due to the topics of the Agora forums and message boards, we will need to establish an additional, user-defined dictionary to provide definitions for terms that will have alternate meanings on the Dark Internet or online marketplaces. Some definitions that we will need to incorporate include colloquial terms for certain drugs or common terminology for online interactions. The specific unit for analysis is a forum thread, which consists of an initial post and is usually open to replies by the original poster or other users. Attributes such as the title and date of the post can be taken into consideration. Various codes can also be applied to posts or replies based on the topic being discussed. For example, a code “site operations” can be used and expanded into categories such as “vendors,” “payment,” “shipment,” or “security.” A “drug” code could also be used with further categorization into “safety,” “quality,” “prices,” or “laws.”

Our team will conduct a preliminary investigation on the message boards, blogs and forums to catalog the most abundant used terminologies and determine a definition, which we will then assign a tonal value to add to the index. The combination of the *DICTION* *Software* predefined dictionaries and our user-defined dictionaries will allow for a better-coded analysis of the interactions between users. Our team will determine sub-groupings by each member dedicating their use of *DICTION Software* to a single topic and search the topic through the software. The software itself has high processing capabilities and thus, data collection will not take up much of our team’s time, and more time can be spent on the textual analysis of the data collected.

After the guidelines have been set, we will conduct a textual analysis of the forums and message boards on Agora and compare them to the several forums, message boards and blogs on the public Internet. This is similar to a study, conducted by Liyan Song and Scott McNary from Towson University, in which a computer-aided text analysis to compare the tone of face-to-face interactions with those of online interactions (Song & McNary, 2011).

First we will investigate three topics that contain a significant amount of discussion as established by the top selling products of Agora: drugs, weapons and services. These three topics were selected because they can be purchased and have forums on the public Internet. First we will identify sites on the Dark Internet that have complete anonymity (no names or user identifiers and untraceable) that contain conversational text that fall under the three topical categories mentioned before. Next, we will pull text from sites that contains a medium level of anonymity (no user identifiers but traceable) from the public Internet, such as Reddit. Finally, we will analyze text from prevalent sites that holds no degree of anonymity (users must identify themselves using full names). Given the three levels of anonymity, we can compare the correlation between the amount of anonymity and the radicalness or openness of the culture of the Dark Internet.

**Data Analysis.** Each site that is collected to be analyzed will be assigned a level of anonymity. Level 1 will contain sites that have little to no amount of anonymity. Level 2 will contain sites that have a medium or mixed amount of anonymity. Level 3 sites will contain sites that are completely anonymous. Once an Anonymity Level has been applied to the sites, the data produced from the *DICTION Software* undergo descriptive calculation statistics including means, standard deviations, medians and ranges based upon the program’s indexes. Separate analyses will be conducted for Level 1, Level 2, and Level 3 site types. Finally, a Pearson Product Moment correlation coefficient will be calculated to determine the relationship between anonymity levels and radicalism of culture.

**Anticipated Results.** As a result, we anticipate that the anonymity levels of sites dealing with common themes such as weapons, services, and drugs will provoke radical speech. This will provide positive correlation between anonymity and radical language of users. For example, through *DICTION Software*, the certainty index would show that users are more steadfast and resolute in their opinions (“DICTION Overview”, n.d.). The activity index would show that topics are consistently changing and fluctuating as time progresses. Through these sites such as forums and messages boards, we expect that users will be more optimistic in their specific word choices providing positive comments and feedback on situations and groups. Through realism, we anticipate to find certain aspects of these sites that can be incorporated into reality and daily life. Lastly, through commonality, we can determine a unified culture based on the idiosyncrasy of the linguistics.

**Aim 3: bitcoin and Consumer Experience Analysis**

**Research Question And Hypothesis.** Our team will be attempting 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? We hypothesize that using a bitcoin on the Dark Internet will show many similarities to the use of using real money in traditional online transactions. However, we hypothesize that there will be distinct differences unique to the bitcoin that sets it apart from traditional currencies. These distinct differences will show how bitcoin greatly affects transactions on the Dark Internet.

**Sample Information.** In order to acquire information pertaining to our research question and hypothesis, as a team we will purchase a bitcoin and then proceed to make purchases on the Dark Internet. State Grants or any other source of State funding cannot be used to purchase a bitcoin, so our team must acquire the funds to purchase the bitcoin on our own. In order to accomplish this, we will fundraise by advertising to multiple sites on the public Internet. In the past, both Kickstarter and Reddit have showed promise in online fundraising. Kickstarter has been previously used to completely raise essential funds for a plethora of different causes. Since the founding of Kickstarter in 2009, there have been at least 875 theatre projects completely funded (Boeuf et al., 2014). This only represents a small portion of a wide variety of projects successfully funded using Kickstarter. Reddit specifically has multiple user-created subsections of its website dedicated to the Dark Internet and different online cryptocurrencies that we could potentially reach out to for funding.

Once we obtain this bitcoin, we will use it to further our research goals by purchasing something with it on the Dark Internet. Since the bitcoin will be purchased with non-State funds, the only restrictions on what we will be able to purchase are legality and price. We do not wish to break any laws, so we will not purchase any illicit materials. And depending on how much we are able to fundraise, the price of our purchase will be limited to a few hundred dollars. But beyond that, we can buy whatever we choose. By doing so, our team seeks to compare the process of purchasing a product or service on a Dark Internet marketplace using bitcoin with traditional online shopping on the public Internet using dollars, specifically by way of popular online shopping destinations such as Amazon or eBay.

**Data Collection.** In order to actually purchase the bitcoin, there are many different sites that we can use to make the purchase from individuals or companies, 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. We can also sell this bitcoin back to many of these sites to receive payment in USD in return. During the time that we possess a bitcoin (or part of a bitcoin) it will be contained in a digital “wallet” installed on a teammate’s computer, ensuring that we will be the only ones with access to this bitcoin (Parthemer & Klein, 2014). 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.

The amount of bitcoin that we buy will totally be dependent on the amount of money that we are able to fundraise. Our team’s goal is to fundraise enough money to buy at least a single bitcoin, but we can accomplish our goal of becoming a consumer on the Dark Internet with less than that. We cannot be certain about whether or not we will be able to purchase a full bitcoin, due to the fact that the value of bitcoin changes very rapidly. Since the founding of bitcoin, one bitcoin has reached a peak of $1200, and as of July 2014, it is $650 (Parthemer & Klein, 2014). Because the value of a bitcoin constantly fluctuates, it is very possible that our bitcoin will not be worth as much as it was when we first purchase it. We must be prepared to lose the money we fundraise and subsequently use to purchase the bitcoins. It is also possible (but unlikely) that we will see an increase in the value of the bitcoin we purchase.

As for where we will make this purchase, we have several options available. Numerous sites accept bitcoin, including Newegg and PayPal, but for the intents and purposes of our project we will use Agora, the popular Dark Internet market. Our current plan for how we will use our bitcoin is to hire the services of a ghostwriter to write a mock methodology paper for our Gemstone project.

There are several confounding variables that we may encounter and have to work through. Primarily, it is possible that we do not fundraise an amount of money that can be used to a significant amount of bitcoin. Hopefully this does not happen, but if it does, we will need to seek other methods of collecting money, likely through obtaining a private grant. Secondly, many of the markets on the Dark Internet have been seized and shut down in the past (In Brief, 2014). This could possibly happen to Agora, and if it does, we will need to find another market where we can make our purchase. Lastly, although unlikely, it is possible to not be able to find a reliable writer on Agora. If this happens, we can either seek out writers on other markets or choose another legal product to purchase.

**Data Analysis.** Throughout the whole process of buying and keeping track of the value of our bitcoin, we hope to gain experience and insight on the process of buying and owning bitcoin and being a consumer on Dark Internet markets. Besides 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 emphasize the experience and insight we gained during the process. Using a bitcoin on Agora will allow us to gain a better understanding of the purchasing process on Agora and Dark Internet markets in general. This first-hand experience and the familiarity that this experience will best enable us to gain a better grasp of using bitcoin and acting as a consumer on the Dark Internet (Scott, 1991).

We will analyze the paper we purchased using the textual analysis techniques described on pages 8 and 9 of this paper. Additionally, we will enlist a professional (possibly from the University of Maryland Writing Center) to grade this paper, and determine its validity, quality, and worth as a piece of academic literature. This will give us an idea of the overall quality of our purchased paper, and determine the quality and effectiveness of the service we had purchased through the Dark Internet. Our team will further our analyses of the experience by enlisting a ghostwriter to perform the same task from a comparable service on the public Internet, such as Academic Ghostwriting, and comparing the experiences and quality of the purchased services.

**Anticipated Results.** bitcoin is a currency almost unlike any other on Earth; its backers claim that it offers perfect anonymity for those who purchase with it, which makes it a natural fit for most of the Dark Internet’s users (Levin et al., 2014). As of 2014, however, it remains a fringe currency at best, and many of its detractors point to its the murkiness and unreliability of bitcoin-backed purchases (Levin et al., 2014). A scholarly analysis of the reliability of bitcoin purchases are on the most anarchic section of the Dark Internet - a place where there are theoretically *no* authorities and few ways of rendering merchants accountable - would greatly help our analysis of the benefits and drawbacks of online anonymity. The overall report could very well predict whether in the future, official and natural currencies will begin to emphasize anonymity as the public grows increasingly determined to protect its privacy and increasingly knowledgeable about how the Internet might help them.

**Limitations to data collected**

 Team DIRE’s aims to gather data on various aspects of the Dark Internet, however our methods of data collection will not be without their problems. The data we will be collecting for the analysis of the Dark Internet will have its limitations based on the amount of time we have available to collect the data after gaining access to an exit node. Our successes in analyzing changes to Dark Internet traffic will depend on the random samples that are collected by the exit node as well as the occurrence of events that affect Dark Internet traffic during the time we have available to collect data on Dark Internet traffic. Our marketplace analysis will be limited based on the amount of data collected by the software we use, how we choose to have the software analyze the data, and where we choose to pull our data from. If we choose only certain forums to analyze with our software, we run the risk of missing information. Analysis of bitcoin and the consumer experience on the Dark Internet is limited to our team only experiencing the purchase of one item from the Dark Internet. Due to the time limitations of the span of the Gemstone Program, unfortunately our team is unable to conduct an effective longitudinal study of the fluctuations in bitcoin value, despite the valuable information such a study would provide, and the lack of need of our team to purchase a bitcoin at all to do so. As it is impractical, as well as illegal in certain cases, to try to purchase a little of everything from a Dark Internet market, we will be missing data on the consumer experience of those products and will only be able to speak to our experience in hiring a ghostwriter as well as the quality to the product provided.

**Conclusion**

Team DIRE’s research will delve into the relatively unexplored topic of the Dark Internet and the cultural phenomena surrounding it with the purpose of demonstrating its uses and functionality, the resulting impacts of current events on these, as well as its practicality as a source of economic trading processes through the use of anonymous online markets and bitcoin. Our team will undertake a methodology comprised of researching three principal categories: Dark Internet Traffic, Dark Internet Marketplaces, and bitcoin and Consumer Experience Analysis. These methods will allow our team to gather and analyze both qualitative and quantitative data surrounding the Dark Internet in order to explore its cultural and economic developments. Team DIRE will organize into several sub-groups and be assigned to different tasks under the methods described in our three chief areas of research, which will allow our team accomplish the goals of our team within the scope of our research program.

 The Dark Internet has become an increasingly publicized topic in the mainstream media while still lacking meaningful research on the subject; Team DIRE believes that by being among the first to work as an organized force to explore the subject in depth, opportunities for the sociocultural developments and economic advancements provided by the Dark Internet can be identified and exploited for public use.

**Conclusion**

Most of the knowledge collected throughout the media and academia only scrapes the surface of what composes the culture of the Dark Internet. Even though the Tor Network has become a larger part of today's online society, there is a lot that society needs to understand of the impacts of the security provided through varying degrees of anonymity. Anonymity is provided to the users of the Dark Internet through several layers. First, a user's IP address is routed through heavy encryption. Then, a user is allowed to make purchases through cryptocurrencies in order to not connect any purchases to a personal account. Additionally, the forums and blogs on marketplaces do not require any form of identification, giving users the freedom to speak without their identity becoming known.

All of these subjects can be considered common knowledge, however the impact and the sociocultural differences between the Dark Internet and the public Internet is not known. Team DIRE aims to develop a deeper knowledge on these topics by analyzing: (1) Dark Internet traffic and comparing it to current events; (2) the cultural implications of Dark Internet marketplaces; and (3) the experience of using bitcoin to undergo a consumer's experience on a Dark Internet marketplace compared to the public Internet. Hopefully, the anticipated results will show that anonymity will provoke an increased level of radical speech, relative to the public Internet. Additionally, the results might reveal a correlation between the public Internet media's exposure and the traffic patterns on the Dark Internet.

Due to the increased importance of Internet security in modern day society, the results of this project will create new knowledge on an expanding part of Internet culture. This knowledge will be able to show a better understanding of what draws users to the Dark Internet and how the specific society of the Tor Network is unifying across cultures.

**Appendices**

**Chronological Timeline**

 **Spring 2015.**

* Proposal Defense
* IRB Exemption Form
* Begin fundraising for ghostwriting services (bitcoin)
* Exit Node access by the end of this season
* Software access for textual analysis by the end of this season

 **Summer 2015.**

* Begin exit node data gathering

 **Fall 2015.**

* Reach our fundraising goal
* Begin finding terminologies for textual analysis software
* Begin making documents of forums for textual analysis software
* Begin running textual analysis software
* Purchase bitcoin
* Purchase ghostwriting services from both Dark Internet and public internet (to be received late fall/ early spring)
* Junior Colloquium
* Begin detailed outline for final thesis
* Begin drafts of chapters 1 and 2 of final thesis

 **Spring 2016.**

* Present at Undergraduate Research Day
* Begin drafting chapter 3 of final thesis and revising all three chapters
* Conduct our purchase experience analysis
* Conduct our product quality analysis with the assistance of the UMD English Department
* End exit node data gathering
* End textual analysis software use

 **Summer 2016.**

* Begin data analysis

 **Fall 2016.**

* Senior Orientation
* End data analysis
* Draft chapters 4 and 5 of final thesis
* Revise final thesis
* Prepare draft of presentation
* Submit names of at least 5 experts for thesis conference

 **Spring 2016.**

* Senior Thesis Conference Rehearsal
* Senior Thesis Conference

**Budget**

|  |  |  |
| --- | --- | --- |
| **Item** | **Description** | **Cost ($)** |
| Laptop | Acer Aspire E1-572-6870 | 580 |
| One (1) bitcoin | Cryptocurrency | 351\* |
| External Hard Drive | 500 GB | 50 |
| DICTION Software | Student Edition | 219 |
| Total |  | 1, 200 |

**\***The value of one bitcoin varies depending on the market. The value in U.S. dollars is the price of one bitcoin as of December 10, 2014.

**Glossary**

**· Agora -** current online marketplace favored by the Dark Internet community after the Silk Road 2.0 shut down by the government

**· bitcoin -** a digital currency that uses state-of-the-art cryptography, can be issued in any fractional denomination, and has a decentralized distribution system

**· Dark Internet -** program that allows browser anonymity by bouncing IP addresses so that the user is anonymous

**· Nodes (Exit and Relay) -** points of interest that IP address is bounced through when using the Dark Internet. Relay nodes specifically apply to points where IP is bounced before proceeding to another relay node or an exit node. Exit nodes are the last point that an IP address is passed before proceeding to the final destination (the website).

**· Silk Road -** online marketplace favored by the Dark Internet community until shutdown by government. It was then replaced shortly by Silk Road 2.0, until government shutdown that caused it to be replaced by Agora as the top online market.

References

Aked, S., Bolan, C., & Brand, M. (2013). Determining What Characteristics Constitute a Darknet. SRI Security Research Institute.

 R. Anderson. (1996). The Eternity Service. Proceedings of the First International Conference of Theory and Applications of Cryptology (Pragocrypt 96), *Czech Tech. Univ. Publishing House*. 242–252.

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

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

Boeuf, B., Darveau, J., & Legoux, R. (2014). Financing Creativity: Crowdfunding as a New Approach for Theatre Projects. *International Journal Of Arts Management*, 16(3), 33-48. ISBN:1480-8986

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

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/>

Carley, K. (1994). Extracting culture through textual analysis. *Poetics*, *22*(4), 291-312.

DICTION Overview. (2014, January 1). Retrieved from: http://www.dictionsoftware.com/diction-overview/

Chen, H., Chen. C, Lo, L., Yang, S.C. (2014). Online Privacy Control Via Anonymity And Pseudonym: Cross-Cultural Implications. *Behaviour & Information Technology* 27.3 (2008): 229-242.

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). International World Wide Web Conferences Steering Committee.

Cook, J. (2014, November 6). FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0. Retrieved from: <http://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11>

Darlington, J. K. (2014). The Future of bitcoin: Mapping the Global Adoption of World’s Largest Cryptocurrency Through Benefit Analysis. *University of Tennessee Honors Thesis Projects.* Retrieved from:<http://trace.tennessee.edu/utk_chanhonoproj/1770>

Dierks, T & Rescorla, E. (August 2008). The Transport Layer Security (TLS) Protocol, Version 1.2. RFC 5246. Retrieved from: <http://www.rfc-editor.org/info/rfc5246>

Dingledine, R., Mathewson, N., & Syverson, P. (August 2004). Tor: The Second Generation Onion Router. In Proceedings of the 13th USENIX Security Symposium,

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

Everett, C. (2009). Moving Across to the Dark Side. National Security, 2009(9), 10-12. [doi:10.1016/S1353-4858(09)70099-6](http://dx.doi.org/10.1016/S1353-4858%2809%2970099-6)

Greenberg, A. (2013, November 6). 'Silk Road 2.0' Launches, Promising A Resurrected Black Market For The Dark Web. Retrieved December 10, 2014.

Greenberg, A. (14, November 5). 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/

Goldschlag, D., Reed, M., & Syverson, P. (1999, February). Onion routing. *Communications of the ACM*, *42*(2), 39-41. doi: [10.1145/293411.293443](http://dx.doi.org/10.1145/293411.293443)

Harrop, W., & Armitage, G. (2005, January 01). Defining and Evaluating Greynets, Sparse Darknets. *Proceedings,* 30,344-350. doi: [10.1109/LCN.2005.46](http://dx.doi.org/10.1109/LCN.2005.46)

Hounshell, B. (2011). The revolution will be tweeted. *Foreign policy*, *187*, 20-21.

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

Knorr-Cetina, Karin (1981). The Manufacture of Knowledge: An Essay on the Constructivist and Contextual Nature of Science. Oxford: Pergamon Press

Kwak, H., Lee, C., Park, H., & Moon, S. (2010, April). What is Twitter, a social network or a news media?.*Proceedings of the 19th international conference on World wide web* (pp. 591-600). ACM. doi: [10.1145/1772690.1772751](http://dx.doi.org/10.1145/1772690.1772751)

Levin, R. B., O’Brien, A. A., & Osterman, S. A. (2014). *Dread Pirate Roberts, Byzantine Generals, and Federal Regulation of bitcoin*. Journal Of Taxation & Regulation Of Financial Institutions, 27(4), 5-19.

Lévy, P., & Bonomo, R. (1999). *Collective intelligence: Mankind's emerging world in cyberspace*. Perseus Publishing.

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

McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008). Shining Light in Dark Places: Understanding the Tor Network. *Proceedings of the 8th International Symposium on Privacy Enhancing Technologies,* *5134*, 63-76.

Murdoch, S.J.; Danezis, G., (May 11, 2005). Low-cost traffic analysis of Tor. *Security and Privacy, 2005 IEEE.*, vol., no., pp.183,195. doi: 10.1109/SP.2005.12

Parthemer, M. R., & Klein, S. A. (2014). bitcoin: Change for a Dollar?. *Journal Of Financial Service Professionals,* 68(6), 16-18. ISSN: 1537-1816

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

Scott, J. (1991). The Evidence of Experience. *Critical Inquiry*, 17(4), 773-797.

Silver, N. (2012). The signal and the noise: Why so many predictions fail--but some don't. New York: Penguin Press. ISBN: 1594204111.

Song, L., & McNary, S. W. (2011). Understanding students' online interaction: Analysis of discussion board postings. *Journal of Interactive Online Learning*,*10*(1), 1-14.

Wilkinson, L. (1999). Statistical methods in psychology journals: Guidelines and explanations. *American psychologist*, *54*(8), 594.

Winter, P., & Lindskog, S. (2012, April). How China is Blocking Tor. *Technical Report*. Karlstad University.

Zhang, Q., Yu, T., & Ning, P. (2008). A framework for identifying compromised nodes in wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, *11*(3), 12.

Zhou, Wanfeng & Olivari, Nick. (2013, October 01).bitcoin Buzz Grows Among Venture Investors, Despite Risks. Reuters. Retrieved from: <http://www.reuters.com/article/2013/10/01/us-markets-forex-bitcoin-id>