January 2016

Anonymity, Cybercrime, and the Connection to Cryptocurrency

Jesse D. Bray
Eastern Kentucky University

Anonymity, Cybercrime and the Connection to Cryptocurrency

By

Jesse Bray

Thesis Approved:

Chair, Advisory Committee

Member, Advisory Committee

Member, Advisory Committee

Dean, Graduate School

STATEMENT OF PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Master of Science degree at Eastern Kentucky University, I agree that the Library shall make it available to borrowers under rules of the Library. Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgment of the source is made. Permission for extensive quotation from or reproduction of this thesis may be granted by my major professor, or in his absence, by the Head of Interlibrary Services when, in the opinion of either, the proposed use of the material is for scholarly purposes. Any copying or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Signature ______________________________

Date 6-24-16

Anonymity, Cybercrime and the Connection to Cryptocurrency

By

Jesse Bray

Bachelor of Science

Eastern Kentucky University

Richmond, Kentucky

2012

Submitted to the Faculty of the Graduate School of

Eastern Kentucky University

in partial fulfillment of the requirements

for the degree of

MASTER OF SCIENCE

August, 2016

DEDICATION

To Keri, for all of her understanding and unwavering support even when it seemed like there was no light at the end of tunnel.

ACKNOWLEDGMENTS

To my committee chairman, Dr. Ryan Baggett, as well as my other committee members, who pushed me to complete this thesis, always had an open door, and time to help. I would like to express my appreciation to my wife, Keri, for her support and patience during the time it took to complete this thesis. Even though there were times when it seemed it would never end you always gave me the motivation to keep going. Finally, I would like to thank my parents, Vicky and David Bray for their continued support.

Abstract

Cybercrime currently poses a significant threat to the infrastructure of the United States. It can exploit vulnerabilities within the Critical Infrastructure or (CI) systems that are increasingly interconnected. Although the increased interconnectedness allows for easier and more efficient communication it creates vulnerabilities that did not exist ten years ago. A lack of a standardized definition of cybercrime has made it increasingly difficult to create policy that will allow for more efficient interagency cooperation and concrete laws regarding cybercrime. Cybercrime thrives on the anonymity of the Internet with the use of specific browsers, The Onion Router for example, to access information not searchable within everyday search engines. In addition, cybercrime thrives with the increased use of peer-to-peer decentralized cryptocurrency. This study will use primary data collected by the principal investigator (PI) to determine if any connection exists between anonymity, cybercrime, and cryptocurrency. The purpose of this quantitative study is to identify whether or not anonymity and cryptocurrency have an effect on the actions of individuals while online. The sample group consisted of 71 students from various majors on the campus of Eastern Kentucky University in Richmond, KY. These participants may be in any year of their respective programs. Participants were identified through a random sample of the entire on campus student body of the Richmond, Kentucky campus of Eastern Kentucky University. The participation of the students was be entirely voluntary. A large amount of the participants valued a high level of anonymity, (35%) of the total sample (n=71) agreed they valued anonymity and (36.6%) strongly agreed anonymity is something they valued. Participants stated that (18%)

agreed with the download of pirated software and (11.5%) strongly agreed they would download pirated software if given complete anonymity.

TABLE OF CONTENTS

Introduction

The United States faces threats from natural disasters, failing infrastructures, cyber-attacks, as well as attacks from foreign countries, groups, or individuals. This attack may come as a physical attack or virtual; with the latter being a relatively new issue that law enforcement has had trouble combating with a high level of effectiveness. Although cybercrime has been pushed to the forefront of the Federal Bureau of Investigation's priorities it still lacks the capabilities to stay current with hackers, individuals attempting to defeat the security defenses of websites, databases, and networks. (Geers, 2010).

As the world becomes increasingly connected through use of the Internet, the possibility of cyber-attacks will inevitably increase. When discussing cyber-attacks, cybercrime, and cyber-terrorism it should be addressed as to what each of these mean, the similarities, and the differences. Unfortunately, the lack of a consistent definition of cybercrime makes creating strategy and policy dealing extremely difficult. Therein lies a major issue with being able to protect personal information online, networks, and infrastructure; as well as having a lack of resources and manpower to combat cybercrime, which may relate to having a lack of an agreed upon definition. In the last decade Executive Orders and Presidential Policy Directives have been issued but it will take time to measure the effects.

There are many cyber related dangers facing the infrastructure of the United States. These can range from Denial of Service, or (DoS) attacks, theft or release of sensitive data, or manipulation of data. The first documented DoS attack occurred in 2000 and was aimed at multiple websites such as eBay and Amazon.com. These were believed to total approximately $1.7 billion in losses. A more serious cyber-attack is believed to have occurred prior to the Russian invasion of Georgia in 2008, this attack disrupted communication and financial systems of the country (James, 2009).

There are many crimes that once were only connected to the physical world but in recent years have moved at least partially into the virtual world with the use of crypto currency and increased online anonymity. One of the most prevalent physical crimes that can now be facilitated through the medium of the Internet is identity theft. Much of the time identity theft can be done with almost complete anonymity, allowing the criminal to remain anonymous and transfer the stolen identities for online currency or "cryptocurrency". Due to the increase in identity theft, the Identity Theft and Assumption Deterrence Act was passed in 1998. This act made it a federal crime to knowingly use another person's identification without their authority. This included all forms of identification, such as, social security numbers, dates of birth, birth/death certificates, bank/credit card numbers, as well as biometric data. Even when applying this act, law enforcement is still not able to produce consistent data on victims and losses. This is primarily due to the lack of a concrete structure on how to label cyber related crimes since each department may classify identity theft crimes differently. Also, since identity theft involves mail fraud, credit card fraud, or other types of offline fraud it will be difficult to assemble statistics relating to online identity theft (Federal Bureau of Investigation, 2014).

Cybercrime has been on the rise in the past decade and becomes a higher priority when exploring the fact that the U.S. infrastructure is increasingly connected with the Internet. This connectivity increases efficiency but leaves infrastructure vulnerable to attack from individuals wishing to do the United States harm, hacker groups that disagree with policies, or even other nations that wish to steal or manipulate data to do harm and/or benefit themselves. By increasing awareness of cyber-crime, creating a clear definition of cyber-crime and when a crime is a virtual crime or a physical crime, the U.S. Department of Homeland Security (DHS) will be better equipped to protect United States citizens and combat cyber-attacks.

Purpose of the Study

The purpose of this study is to identify whether the ability of an individual to remain anonymous while online has any effect on their actions online. Additionally the study will help determine if subjects are aware of cryptocurrency, usage, and application of cryptocurrency in the past. There is a gap in knowledge of whether or not anonymity and the availability of cryptocurrency have an effect on potential for criminal activity.

With the following research questions it will be determined if an association exists between anonymity, cybercrime, and cryptocurrency.

1. Does anonymity increase the potential for an individual to commit an act of cybercrime?
2. What role does cryptocurrency play regarding anonymity and criminal activity on the Internet?

Potential Significance

This study will provide current and relevant data on issues involving anonymity while online and the hazards that can result. This study will continue to set a solid foundation for future research of an emerging topic that has the potential to become problematic for policy makers, law enforcement, and the intelligence community. Also, it will determine if there is any association between the need of an individual for anonymity online with the opportunity to commit illegal acts or make illegal purchases. It will unlock a new area of study were very little research currently exists.

Definition of Terms

Critical Infrastructure/Key Resources: "Basic physical and organizational structures and facilities needed for the operation of a society or enterprise." (Collins & Baggett, 2009)

Cyberterrorism: "terrorist activities intended to damage or disrupt vital computer systems." (Cyberterrorism, Merriam Webster, 2014)

Anonymity: "the quality or state of being unknown to most people", (Anonymity, Merriam Webster, 2014)

Terrorist Organization: A group that uses terror as a primary weapon, using any means necessary to inflict damage. Justifies actions with political ideals or religion.

Active Supporter: Individual within a group who participates in day-to-day operations of the group.

Passive Supporter: Individual who is not involved in day-to-day operations of a group but contributes funds or other forms of infrastructure.

The Onion Router, TOR: Software that allows an individual to conceal their location while online.

Payload: Data that can be delivered to an individual, business, etc., may contain code that will damage a network or attack vulnerabilities within a system.

Cryptocurrency, Digital Currency: A medium of exchange that can only be used online, allows for a certain degree of anonymity.

Mining: Process of solving algorithms to collect Bitcoins.

Block Chain: Ledger that stores the address of the digital wallet that transferred Bitcoins to another user, ledger only shows which wallet transferred bitcoins and not the specific person who uses the wallet.

IP Address: “the numeric address of a computer on the Internet.”, (IP Address, Merriam Webster, 2014)

Bitcoin Network: An online medium of exchange that uses the currency known as bitcoin to make transactions.

Literature Review

The following chapter will detail issues pertaining to anonymity, cryptocurrency, and their potential relationship to cyber-crime. There are advantages as well as negatives when using different and/or trading different types of digital currency, such as Bitcoin or Dogecoin. This chapter will also discuss the connection that the cyber-world has with Critical Infrastructure and the potential negative consequences that may arise.

Internet and Critical Infrastructure

A real world example of how a Critical Infrastructure or (CI) system could be hacked would be the Distributed Denial of Service or (DDOS) attack targeting of Estonia in 2007. In April of that year the Estonian government moved a Soviet WWII memorial out of the city center in its capital of Tallinn. This act upset the Russian minority as well as Russia itself. This attack that could have been initiated by the Russian Government or a group of hackers that was sympathetic with the cause. The attack severed all communication with some of the largest banks in the country and since 98% of banking done in Estonia is done online, an immense impact was felt throughout their financial system (James, 2009).

The United States has taken the initial steps in protecting itself against all types of cyber-attacks. This has been through the issuing of Executive Order (EO) 13.636 "Improving Critical Infrastructure Cyber Security" and Presidential Policy Directive (PPD)-21, "Critical Infrastructure Security and Resilience." EO 13.636 acknowledges the problem facing CI and to promote the future national security, safety of the cyber world, and economic security. This EO plans to accomplish this by increasing the degree of information sharing relating to cyber security. This will be accomplished in coordination with the Director of National Intelligence by creating a process that can disseminate, track, and record reports and deliver said reports to the necessary agency or agencies. This order will also increase information sharing between appropriate agencies and security providers, both physical and virtual. Increased information sharing will be assisted with the prioritizing the security clearance process for all applicable personnel tasked with CI protection. Also, information sharing will be increased through the temporary employment of subject matter experts, who will provide input in regards to the type of information CI operators will need in order to provide adequate protection. This order also addresses civil liberties and privacy issues and states that all appropriate agencies will review all activities and programs to ensure compliance with privacy standards. EO 13.636 will identify the CI that is at the greatest risk of a cyber-attack through consultation with Sector Specific Agencies (SSAs) and subject matter experts. The process of identifying at risk CI will be completed on a yearly basis (Obama, 2013).

Through Presidential Policy Directive (PPD-21), security and resilience of the U.S. CI will be improved by refining relationships throughout the Federal Government, increase effective information sharing, and create a function the allows planning and operations decisions involving CI to be better integrated and analyzed. All Federal departments and agencies will identify, assess, and suggest corrective actions for applicable CI and all new programs must follow all privacy and civil liberty requirements. In regards to counterterrorism and counterintelligence investigations the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) will be primarily responsible. The FBI will have the responsibility of operating the National Cyber Investigative Joint Task Force (NCIJTF), which will be the primary agency sharing information that is related to cyber threats. This agency group will have representation from the Department of Homeland Security (DHS), Intelligence Community (IC), and the Department of Defense (DOD) ("Critical infrastructure security," 2013).

The world is increasingly more connected to the Internet, which leaves the United States open to an attack from other nation states, groups, or individuals who wish to the United States harm. Although being more connected allows increased risk, increased connectivity grants CI the ability to react more quickly to emergencies, increase efficiency, and secure and operate facilities more effectively.

The Internet and Terrorism Recruiting

Although the Internet will most likely never replace traditional mediums of terrorism, (i.e. bombings and/or other forms of violence) it allows for easier communication between separate terrorist cells, allows for increased recruitment and/or conversion to the terror groups ideology, and a potentially high degree of anonymity from Law Enforcement (LE) and the Intelligence Community (IC).

So how do terrorist organizations make use of the Internet to accomplish their goals? Many terrorist groups have created websites that include information on the history of the organization, prominent members and/or founders, and what the organization intends to accomplish. Depending on the website the group may or may not directly state their goals, primarily they will criticize their enemies and this approach will normally reveal their intentions. Some groups such as Hezbollah and Hamas discuss prior operations that have been completed. These groups will normally give up to date news regarding their “enemies” as well as successful attacks, and numbers of martyrs and enemies killed.

Terrorist organizations facilitate the Internet to address multiple audiences. Individuals who may support the group, enemies, or the general opinion of the public are all most likely targets. Most cites do not encourage direct violence but do offer passive ways to help in the “struggle” that particular group is facing. Although, much of the encouragement is passive when dealing with violence some of the language that is used may be interpreted as encouraging violence. Hamas mentions Jihad numerous times, this word technically refers to a struggle, but could be interpreted as an invitation to violently attack their enemies
(Tsfati & Weimann, 2002)

While the Internet can be used in multiple ways regarding terrorism, bragging of accomplishment, claiming of achieving goals through pacifist means, or posting current news of the group; the most effective use of the Internet regarding terrorism is the recruitment of impressionable individuals to join a group’s cause. There are many ways a terrorist organization may recruit new followers. For example, one may be propositioned face to face to participate in operations. This first example is the most direct route and may be more useful in areas where there is little Internet connectivity. This method would be more likely to succeed in areas of the world that have suffered from the enemy group or have heard one-sided stories stating what horrible acts the enemy group has committed. While this method may be effective when dealing with a small percentage of a population, taking a more indirect method could lead to more success. Optimal recruitment will be possible when both direct and indirect methods are used.

When discussing the indirect methods that can be used to spread propaganda and increase recruitment, these indirect forms can be grouped together as media. Media may come from multiple different sources, such as, newspapers, magazines, textbooks, television, and the Web. A group that uses the Web may use these public channels to connect with likeminded individuals who support the cause of the group and wishes to become an active or passive supporter.

To understand the different methods by which an individual may be recruited each should be discussed. The methods can be separated into four quadrants, the first of which would be public and proximate. This quadrant consists of recruiting that is done face to face or possibly in small groups. These are in full view of authorities within prisons or combat experiences. This method can be very successful since the recruiter has the ability to work face to face with the individual.

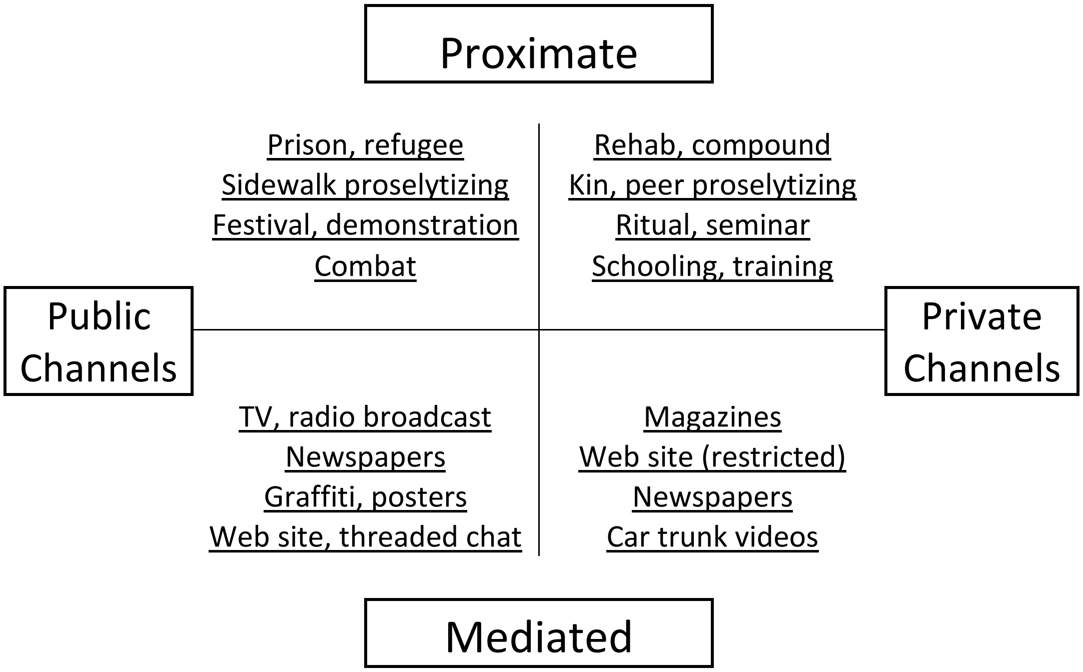

Figure 1: Recruitment Approaches

The second quadrant is public and mediated; the methods within this quadrant primarily use mass media to reach a broad audience. These include such activities as graffiti and non-password protected web sites. The names of the web sites used in these situations are not kept secret and are public. These are more indirect than the methods used in the first quadrant, which leads to less potential effect but will be able to reach further. Some groups, such as al-Qaida will occasionally release videos or make statements to newspapers slamming the United States for their activities in the Middle East.

The third quadrant is private and proximate, these methods relies on recruiting through prayer sessions, paramilitary training, or relatives using peer pressure to influence an potential recruit. This quadrant uses small groups or gatherings to spread their word and is kept away from authorities, especially in regions where the specific group is viewed positively. By using these methods the recruiter is able to directly manipulate the recruit, similar to what can be done in the first quadrant.

The fourth quadrant is the most difficult to combat primarily because of its use of password protected sites that may only be accessed on the Deep Web through the use of specific TOR browsers (The Onion Router). Items that are hidden within the Deep Web range from password protected web sites, restricted chat groups, and many digital videos. In the last 15 years al-Qaida have become incredibly ingenious in the ways they communicate and recruit. Some policy makers have begun to describe this increased use of the Deep Web and onion routers by jihadist groups as a "virtual jihad." The use of new mediums by jihadist groups has made it more difficult for LE and the IC to be able to combat and track the groups. These methods may encounter the same issues has the public mediated quadrant, in the fact that not being able to interact face to face destroys the ability to manipulate a recruit. Although, when this medium is used and an audience that is already sympathetic to the cause then it becomes much easier to recruit. The publishers of the information on the Deep Web also will most likely not have to face attacks from authorities since this area of the web is out of government control for the most part. (Daly & Gerwehr, 2006)

The Deep Web and the Dangers Within

What are the Dark-net and deep-web where much of their propaganda and recruited to done? How do terror groups and potential recruits use this network of primarily benign data and out of use URLs? It is true that the majority of the deep web is harmless but this vast area, that is estimated to several times more information than the standard Internet that we are accustomed to, for illegal activities, which is where dark nets are useful and anonymity is paramount.

While the deep net may be primarily full of benign data and old URLs there is a much darker side called the dark net. While using this large swath of the Internet, users feel very safe discussing topics that may have legal consequences if caught. One of the most valuable commodities on the dark web is the idea of anonymity. Anonymity provides safety from LE and the IC while still allowing users to purchase goods and services. The anonymous purchase of goods and services is primarily completed through the use of Bitcoins or other cryptocurrencies. (Ablon, Libicki & Golay, 2014)

There are many items for sale on dark nets; the most prevalent would credit card information and access to social media accounts. Both of these will command different prices depending on the type or the age of the information. A good example of how prices can change depending on the date would be the value of credit card and personally identifiable information (PII) that was gathered from Target in 2013. Prices for cards stolen from Target brought anywhere from $20-$135. Prices for the information also varied depending on what type of card was available, what limit the card had, and expiration dates. The older the data available is then the less likely the card will still be active as well. (Ablon, Libicki & Golay, 2014)

Although many of activities that can be completed on a dark net are illegal it still has a functioning economy. Dark nets can potentially be more profitable than the drug trade when compared to the potential ramifications of drug trafficking. In the online black market much of the goods sold or bought are online based and can be acquired almost immediately.

As deconstructions of dark net sites, such as Silk Road, continue to occur the anonymity of these sites and the cryptocurrency that is used to purchase goods must increase and become less traceable. Administrators of these sites are using multiple methods to keep LE and the IC off their trail. Some black markets only exist in private chat rooms, others only in private forums, some may advertise in one medium but actually conduct business in another, or administrators may create channels to sell goods and then destroy that channel afterwards. (Ablon, Libicki & Golay, 2014)

The dark net contains countless items that can be purchased, much of the dark net functions similar to amazon.com. Some examples of the items and/or services that can be purchased are: hacking tools, which consist of tools that could give a hacker the upper hand in trying to gain access to an individual, commercial, or government target. These tools also contain what is referred to as payloads; payloads can contain different intended effects on a target. A shopper also has the ability to purchase digital assets, information that has already been stolen. The digital assets that can be purchased are primarily financial information, records, bank/credit card accounts, and intellectual property or IP.

A single person or group can also buy certain services from and experienced hacker or group of hackers. These services may offer many of the same goods or tools that are available but the seller will complete the entire cycle of the attack. Adware and spyware are also other services that are available, although now anti-virus software is very well developed and these services may not be as useful. Currently we see increased Distributed Denial of Service (DDoS) attacks against websites belonging to a variety of individuals, companies, and governments (Ablon, Libicki & Golay, 2014). For example, during the Russian invasion of Crimea of eastern Ukraine beginning in 2013 and currently during 2014 hacker groups have used DDoS attacks against websites, defaced others, hacked into private networks and released sensitive information to the public (Carr, 2014). While experienced and talented hackers are still doing much of the advanced hacking, anyone can purchase these services while on the dark net. All a person would have to do if they desired to attack a website, person, etc. is purchase hacking tools or simply purchase a service and the seller would provide the attack. This means that anyone, no matter their hacking ability or lack thereof, is able to buy this service and attack whomever they desire. (Ablon, Libicki & Golay, 2014)

Anonymity and a loss of Self-Awareness Online

The role of anonymity in cyberspace if profound, it allows for individuals or groups to be able to operate in cyberspace relatively undetected from authorities. While operating on the Internet users may feel hidden from other users and not feel like they are constrained from behaviors that are not considered traditional. This loss of self-awareness and self-regulation could potentially lead to behavior that is considered as deviant behavior, although anonymity can lead to negative behavior it could offer benefits. It could potentially allow for more open conversations on sensitive topics or possibly even counseling. These positives cannot help but be compared to the possible deviant activities that can be enacted using anonymity or perceived anonymity (Hinduja, 2008).

This loss of individualization and self-awareness allows someone with deviant tendencies to act on those thoughts due to the perceived anonymity or complete anonymity offered by being immersed online. This is not to say that any person who has the ability to remain anonymous online will simply decide to act in illegal ways, but a person who already has this want to commit deviant acts will be more likely to do so if they are provided anonymity as well as physical and moral detachment from their actions.

The Deindividuation theory states that an individual who is freed from their moral and social responsibilities will lose acute awareness of their identity of self and that of others. This allows someone who believes they are anonymous to lose their self-awareness and regulation. Although this theory leads one to believe that anytime an individual is allowed more anonymity the person would suffer a loss of self-awareness and identity. This may not necessarily be the full truth; the primary individuals who will be affected by the Deindividuation theory will be those who already have a tendency towards deviant behavior and not just the ability to remain anonymous.

Although there are negatives to online anonymity it offers positives to individuals living under repressive regimes and areas where free speech may be discouraged. For example, loss of anonymity and increased censorship is a fact of life for people living in China. Most media within the country is State controlled and many terms are censored and/or tracked online. Any reference to democracy, the Arab Spring, or speech undermining the legitimacy of the Communist government within China is strictly forbidden. The repression of free speech goes farther than simply blocking certain words from use online, the government forbids Western films from being played in theaters or sold legally. This does not stop the illegal copying of Western films for the black market created due to the illegality of the films.

The use of the deep web with the enhanced anonymity that it provides is a popular way of communication countries with repressive regimes. The deep web is a popular way for journalists in repressive countries to express thoughts and communicate with others. This use of the deep web was also important means of communication during the Arab Spring in many countries, especially after access to social media was increasingly regulated or outright blocked from public use.

Cryptocurrency as the Preferred Medium

Cryptocurrency is a digital only version of currency. These types of currency are open source, this means that it is available to anyone, and peer-to-peer or, the ability for data to be transmitted from one computer to another without the need for a central server. Being peer-to-peer allows for shared access among all users, a level of increased anonymity is generated here. There are many kinds of cryptocurrency, but the most widely used at the time of this writing is Bitcoin. Bitcoin is different from other forms of cryptocurrency in the fact that it is totally and completely decentralized. It compares to virtual cash that can be spent or traded online.

Although Bitcoins are similar to online cash they do not have the ability to be completely anonymous like cash. Bitcoins are stored in a digital wallet once they are collected; this wallet is not necessarily tied to any specific person but it does have a Bitcoin address. The address or public key is recorded in what is called a block chain.

Each public key is recorded a block in this chain and anyone can view the transaction and how many Bitcoins were transferred. The address is tied to a users IP address, although this can be circumvented with the use of anonymizing software like TOR. Bitcoins by themselves are not anonymous but when paired with software such as TOR they become much more difficult to trace by LE or the IC.

The way that Bitcoins are gained is by what is “mining”, this consists of a computer or pool, group, of computers solving increasingly difficult mathematical algorithms. Once an algorithm is solved the user or pool of users is rewarded with a set amount of payout. This payout decreases as more Bitcoins are mined, but will continue until the set cap of 21 million coins is reached.

The goods and services that can be purchased on the dark net must are normally purchased with crypto-currency. Crypto-currencies can provide increased anonymity while on the dark net. Crypto-currencies provide a level of anonymity that traditional currency cannot provide, except for cash which moving large amounts can be very difficult while remaining anonymous. Crypto-currencies such as Bitcoin are able to provide this anonymity by not tracing the transactions back to a specific individual.

The value of a Bitcoin has yet to stabilize, it has shown large swings in value resulting from hacks or stolen Bitcoins. The current value is not tied to anything specific, it is worth the value people assign to it and is traded on an open market. This does show that using Bitcoin, as a type of banking system may not necessarily be a good idea but if they continue to be used a payment method then they Bitcoin economy will become more stabilized.

Bitcoin can be attractive to users or businesses that wish to lower transaction costs, this is possible since the Bitcoin economy has no 3rd party intermediary fees like credit card companies or PayPal charge. Users do suffer a loss of security when peer-to-peer currencies are used instead of traditional currency. There have been instances in the past of Bitcoins simply disappearing from digital wallets or transactions.

Bitcoins are primarily not used for criminal but due to their ability to increase anonymity they are increasingly popular for purchasing illegal goods online. Bitcoins can be used online in the same way that cash is used to make illegal purchases in person, it is simply being done online. Money laundering is another issue that arises when discussing Bitcoins but at this point in time due to the volatility of the digital currency it is not a feasible option.

Bitcoin has many positive uses but still has some of the same legal drawbacks as cash, in that it can be used as a medium to make illegal purchases. This has led to attempts to regulate Bitcoin, although unsuccessful. The regulatory laws currently in use have not envisioned a purely digital currency that has grown to the size of the Bitcoin economy. Bitcoin does not fit into standard definitions of currency or a financial institution though; regulating it has proven difficult due to the currency not being centralized by any specific person or group.

Conclusion

The literature shows that cybercrime has increased over the last decade and that LE and the IC for the most part has been unable to keep pace. Anonymity plays a large role in acts of cybercrime, which can range from pirated software to hacking or acts of cyberterrorism. This increased level of anonymity can be increased with the use of software that can be easily downloaded called TOR or The Onion Router, which allows the user to bounce their IP address over multiple users and access to the Dark Net, tracking an individual using TOR is incredibly difficult at this point. The level of anonymity can be increased with the use of cryptocurrencies, specifically Bitcoin. Cryptocurrencies can be used a medium of exchange online that allows buyers and sellers to remain anonymous when completing transactions. This literature review brings into light the increasing dangers that are faced by the United States. The interconnectedness of the U.S. CI/KR make the United States more vulnerable than ever before and to prevent an attack that could cripple any section of CI all cyber issues must be analyzed and understood. This will allow for policymakers, law enforcement, and the intelligence community to better combat cybercrime and cyberterrorism.

Methodology

Background of the Study

There is a dearth of information regarding cryptocurrency, anonymity and its connection to cybercrime; very little research exists on cybercrime in itself. The scarcity of research on the topics leaves a gap in understanding for law enforcement as well as the intelligence community. This deficiency allows for hackers and criminals to circumvent authorities then attack or steal classified or personal information.

The purpose of this quantitative study is to identify whether or not anonymity and cryptocurrency have an effect on the actions of individuals while online. To begin to understand if a person presented with the opportunity to remain anonymous and resources to do so would take part in criminal activity, ranging from illegal downloading to drug or PII (Personally Identifiable Information) purchasing. A survey should help reveal if these activities are connected with anonymity.

Context of Study

Limited data has been collected regarding types of cryptocurrency and the connection with cybercrime. This study will provide a base for further research in this area. Data was collected regarding whether or not respondents participate in the use of cryptocurrencies and if that respondent has participated in any prior cybercrime. Cybercrime relates to any crime that is facilitated through the use of a computer and/or Internet. It can range from the download or purchase of pirated software to hacking or acts of terrorism.

Selection of Participants

The sample group consisted of 71 students, of a target sample of 1200 students, from various majors on the campus of Eastern Kentucky University. These participants may have been in any year of their respective programs and the participation of the students was entirely voluntary.

Research Questions

This study is designed to determine if a connection exists between anonymity, cybercrime, and cryptocurrency.

The research questions are:

1. Does anonymity increase the likelihood that an individual will commit an act of cyber-crime?
2. What role does cryptocurrency play regarding anonymity and criminal activity on the Internet?

The specific aims of this study are to:

1. Determine whether anonymity increases the likelihood that an individual will commit an act of cyber-crime.
2. Assess the connection between the use of cryptocurrency and involvement in criminal activity in an online environment.

Variables and Measures

The first research question examines individuals who enjoy an increased level of anonymity and the commission of cybercrime. The independent variable for research question one is the level of anonymity that a respondent enjoys while they are online. The dependent variable for question one is the commission of cybercrime. The second research question focuses on what role cryptocurrency plays in criminal activity. The independent variable for question two is the use of cryptocurrency and the dependent variable would the level, if any, of criminal activity. The survey questions were used to determine what level of involvement, if any, the participant had in online activity, use of cryptocurrency, or involvement in cyber-crime.

Research Design

This observational study used primary data collected by the principal investigator (PI) to determine if any connection exists between anonymity, cybercrime, and cryptocurrency.

Data Collection

The collection of data relied solely on information received on the survey that was distributed. The survey was distributed via email with use of Qualtrics software. The survey was comprised of closed ended questions that only allowed for responses of strongly agree, agree, neutral, disagree, or strongly disagree, yes/no, or check all that apply. Respondents were asked to take approximately ten to fifteen minutes to complete the survey. To ensure respondents answered questions as honestly as possible it was stated that no personally identifiable information would be collected and all answers would remain anonymous. Surveys were emailed to respondents who would then complete the survey in a place of their choosing. The survey was accessible between the dates of 01-31-2015 and 02-15-2015. The survey was closed on this date. Approximately 2 weeks after the initial survey was completed a follow up email notification was sent to all who had not replied or completed the survey. See Appendix A for the complete survey.

Data Analysis

First the researcher extracted descriptive statistics from the collected data including mean and standard deviation. Descriptive statistics for demographics were collected and statistics of the use and awareness of cryptocurrency by participants.

A Likert Scale will be used to measure the level of agreement with set questions by providing responses of 5=strongly agree, 4=agree, 3=neutral, 2=disagree, and 1=strongly disagree. There will be a neutral choice to allow for a respondent being unsure or indecision. Other questions will allow for respondents to answer yes/no or check all that apply. Data was summarized using descriptive statistics including means and frequency distributions. Group comparisons were of nominal variables was accomplished by using the chi-square test to determine if an association exists in contingency tables. Data analysis was performed using Microsoft Excel; an alpha level of .05 was used throughout.

Findings and Analysis

There were 71 participants who completed this study. The majority of the participants were female (76%) and between the ages of 18 and 24 (61%). The college to which the participants belonged is split between Justice and Safety (25%), Arts and Science (34%), Education (20%), Business and Technology (14%), and Health Sciences (7%). What participants used the Internet for was split between Social Media (86%), Shopping (85%), News (75%), and Research (74%). Email had the most responses at 93%, Gaming had the least responses at 36%.

Participants statistically stated that they valued a higher level of anonymity with a mean score of 3.99 out of 5 when asked to score the value of anonymity online in the first question. There were not as many participants who valued a higher level of pseudo-anonymity but had a mean score of 2.65 out of 5, although this may have been related to fewer students being familiar with the term. When participants were asked if they would participate in the download of pirated software if given total anonymity the mean response was 2.45 our of 5, most participants did answer that they strongly disagreed with the download pirated software (43%), (18%) stated they agreed with the download of pirated software and (11.5%) strongly agreed they would download pirated software if given complete anonymity. Participants were asked about their feelings toward the purchasing of illegal goods which received a mean score of 1.60 out of 5.The question of hacking personal or business networks had a mean score of 1.40 out of 5. When participants were asked if they felt they had participated in the download of pirated software, music, or videos the mean response was 2.63 out of 5.

When participants were asked if they were familiar with the digital currency Bitcoin the responses were Yes (37%) and No (63%). When asked if digital currencies like Bitcoin would be a good alternative to traditional currency like the U.S. Dollar or Euro the mean response was 2.51 out of 5. When asked if the ability of digital currencies to make anonymous purchases online was a positive concept the mean response was 2.58 out of 5. When asked if the participant would make contributions to controversial groups using digital currency and were given completed anonymity the mean response was 1.94 out of 5. When asked if online hacking posed little threat to United States security interests the mean response was 1.47 out of 5.

Opinions of digital currency and controversial donations

It can be concluded that there is a statistical association between negative views of online digital currency and contributions to controversial groups that participants would not otherwise make if anonymity were not provided (p=. 001). Of those that were indifferent whether or not anonymous purchases were a positive concept, half (50%) were also indifferent about making donations to controversial groups. Of those that agreed that anonymous purchases were positive (15%), of the total sample, (40%) were indifferent and (10%) agreed they would make those same donations. Of the participants that disagreed with the opinion that using digital currency online to make purchases was a positive concept (24% of the total sample n=66), (37.5%) of that sample strongly disagreed that they would make contributions to controversial groups, in addition (43.75%) disagreed they would make those some contributions if given complete anonymity. Of the participants that strongly disagreed with anonymity being a positive statement (18%) the total sample (n=12), all of those participants strongly disagreed (n

=12) (100%) also strongly disagreed they would make donations to controversial groups if given complete anonymity.

Opinions of digital currency and purchase of illegal goods

It can also be concluded that there is a statistical association between the disagreement that digital currencies are a positive concept and the purchase of illegal goods if given complete anonymity (p =. 02). Of the participants that strongly disagreed that the ability of digital currencies to allow an individual to make anonymous purchases online is a positive concept (n=12) (18.75%) of the total sample for this question (n=64), (83%) (n=10) strongly disagreed they would they would engage in the purchase of illegal goods online using digital currency. Among those that disagreed with making anonymous purchases online (n=15), (23%) of the total sample for this question (80%) strongly disagreed they would make illegal purchases online if given total anonymity. Of the participants who neither agreed or disagreed with making anonymous purchases online being a good idea (n=26) of the total sample (n=64), (53%) strongly disagreed they would make illegal online purchases if given total anonymity. Among the participants that agreed the ability to make online purchases was a positive concept (n=10) (15%) of the total sample who answered this question (n=64), (n=7) (70%) strongly disagreed they would engage in the purchase of illegal goods online.

Discussion

This study demonstrates that a large amount of the participants value a high level of anonymity, (35%) of the total sample (n=71) agreed they value anonymity and (36.6%) strongly agreed anonymity is something they value. Participants stated that (18%) agreed with the download of pirated software and (11.5%) strongly agreed they would download pirated software if given complete anonymity. The mean response for the purchase of illegal goods with total anonymity is 1.60 out of 5 and the response regarding hacking personal or business networks is 1.40 out of 5. It should be stated that having an increased level of anonymity online does appear to have a correlation between the commissions of illegal acts online. While (28%) of participants agree that they have engaged in the downloading of pirated software, (37%) strongly disagree that they have participated in any kind of online piracy.

When focusing on cryptocurrency as it relates to cybercrime the statistics do show an association between negative views of using online currency to remain anonymous with (18.75%) strongly disagreeing and (23%) disagreeing, and the use of cryptocurrency to make illegal purchases online (43%) strongly disagreed they would make illegal purchases online if given complete anonymity (p= .02).

A majority of the sample (n=45) (63%) was not familiar with cryptocurrencies, in addition the majority of the sample from Eastern Kentucky University does value anonymity, (n=25) (37.8%) strongly agree and an equal number (n=25) (37.8%) agree they value anonymity online but that many are not aware or are unfamiliar with cryptocurrency in general. This shows that a majority of the sample was not familiar with crypto currencies but still valued their anonymity online.

Complete anonymity online, using cryptocurrency to anonymously purchase illegal goods online, and hacking pose a significant threat to the security of the critical infrastructure of the United States and it only takes a few determined individuals with the right capabilities to cause significant damage. It should be noted that online anonymity does not necessarily end with negative results. Activists, journalists, and many others use The Onion Router or TOR to remain anonymous while reporting atrocities in war torn or oppressed countries. This allows individuals to report without being noticed and is currently being done with steganography to hide information inside messages and pictures. Steganography can be used to circumvent firewalls and government censors. In the past this method has been used via Twitter and Flickr to distribute information to other activists inside and outside the country. This method of hiding information allows activists or other citizens to fight repressive regimes. Unfortunately it also gives criminals other methods of smuggling illegal digital items without being detected. Law enforcement still has difficulty combating the transmission of large amounts of digital currency. If a criminal was using $200,000 in cash to purchase illegal weapons he would be very easy to catch as transporting this large amount of cash would be difficult and using traditional money transfers would be easy to trace. This same person who uses a digital currency to purchase the same goods online will be much more difficult to trace since any individual may have an unlimited number of digital wallets to store their digital currency without any of these tied to a specific person.

Technology like digital currency, TOR, online anonymity, steganography, and other ways of remaining anonymous allow for people in repressive regimes like China, North Korea, and Iran to spread their messages to other activists with a smaller chance of being caught. It also gives new ways for criminals to distribute illegal items like pirated software, personal information, financial information, or classified information. It will be a constant battle to keep criminals from distributing illegal items or services that are using the same methods as activists use spread information in repressive countries.

The future of the digital currency that allows for purchases made online to have a high degree of anonymity is ever changing and ambivalent. There are constantly new types of digital currency that rival one another. With the anonymity involved in using digital currency there have been individuals who take advantage of this and steal from others online with little to no chance of retribution.

The United States is looking to place increased regulations on companies that transmit digital and anonymous currency. At this time the Financial Crimes Enforcement Network or "FinCen" has fined "Ripple", a company that facilitates payments between individuals and other and allows the trading of hard currency for digital currency and vice versa, $700,000 for not registering as a money services business and not following rules to prevent illegal uses online and violating the Bank Secrecy Act. The Bank Secrecy Act does not allow any transactions by anonymous accounts and would mean these exchanges that previously marketed that the anonymity they provided for users in the past would now be forced to collect information about customers. (Richards, 2015)

The Bank Secrecy Act, which does not allow any transactions by anonymous accounts, would force exchanges, such as Ripple, to collect information on the exchanges but the regulations would not apply to the vendors and customers using the digital currency outside of the United States. So it appears that these proposed regulations may not be enough to satisfy opponents of the cryptocurrency and would allow buyers and sellers to continue to operate in secrecy for the time being just outside of the United States in countries with more relaxed regulations. Criminals would still be able to operate illegal businesses, buy, and sell goods electronically with the medium of cryptocurrency without the threat of law enforcement when based overseas. (Richards, 2015)

With the continued creation of new versions of digital currency they become more and more complex. This additional complexity will undoubtedly gain attention from more regulatory bodies, governments, and hackers that are looking to gain the upper hand and find weaknesses within the currency. This additional issue makes it unclear whether or not a digital currency could ever replace the fiat currency that is used currently all over the world. Also, the instability of digital currencies makes them unlikely to replace any fiat currency any time soon.

Aside from the illegal implications of using cryptocurrency and the risk of losing currency to hackers, fiat currency has a value that in most cases does not vary widely. Digital currency does not offer this same promise and will extensively fluctuate; comparing it to tradition currency may prove very difficult.

Limitations

Currently there is little information regarding cybercrime and due to a lack of concrete definitions of cybercrime there are few statistics and reporting is inconsistent. The findings of this study may not apply to all respondents, not all actions resulting from the use of digital currency or online anonymity are negative. Some within the sample group may not have been completely truthful of their knowledge or actions committed online due to perceived repercussions. Although a target sample of 1200 students, only 71 students responded (response rate of 6%). In addition, only more tech savvy students may be aware of the concepts discussed throughout the survey, as many who are not familiar with the topic may not have an opinion on the subject. This study also only focused on a portion of a single university within the United States, this study would only reflect the views of a small section of the region. An expanded study would be much more helpful in determining the likelihood on criminal activity across other regions. This study did not separate individuals without a criminal history from those with a criminal history, which would be incredibly helpful for future research.

Further Research

Due to this being such a novel topic very little research has been completed at this time. Further research opportunities should include deviant history of individuals, as this could be a predictor of future acts cybercrime or other illegal activity. Future research should also focus on different regions within the United States as well as socio-economic classes. Additional studies should focus on the uses of cryptocurrency itself and what is being purchased with all digital currency. Further research should be done into the dark web itself to discover what may be purchased and how this side of the Internet functions. Research would also need to be completed on the effects of increased regulation for digital currency and what implications would result.

References

Ablon, L., Libicki, M., & Golay, A. (2014). *Markets for cybercrime tools and stolen data*, ix-15. Santa Monica: RAND Corporation. Retrieved from https://www.hsdl.org/?abstract&did=751108

Anonymity. (n.d.). Retrieved August 6, 2014, from http://www.merriam-webster.com/dictionary/anonymity

Carr, J. (2014, March 25). *Rival hackers fighting proxy war over crimea*. Retrieved from http://edition.cnn.com/2014/03/25/opinion/crimea-cyber-war/index.html?iref=allsearch

Ceresa, A. (2005). The impact of 'new technology' on the 'red brigades' italian terrorist organisation. *European Journal on Criminal Policy & Research*, *11*, 193-222. Retrieved from http://link.springer.com/article/10.1007/s10609-005-5664-y

Collins, P., & Baggett, R. (2009). *Homeland security and critical infrastructure protection*, 5. Westport: Praeger Security International.

Cyberterrorism. (n.d.). Retrieved August 6, 2014, from http://www.merriam-webster.com/dictionary/cyberterrorism

Daly, S., & Gerwehr, S. (2006). Terrorist selection and recruitment. In *McGraw-Hill homeland security handbook* Vol.5, 73-89. Retrieved from http://www.rand.org/pubs/reprints/RP1214.html

Federal Bureau of Investigation. (2014, May 03). *Identity theft*. Retrieved from http://www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview

FEMA (2013, Oct 25). *Dam ownership in the united states*. Retrieved from http://www.fema.gov/dam-ownership-united-states

Geers, K. (2010). The cyber threat to national critical. Journal of Digital Forensic Practice, 3, 126. doi: 10.1080/15567281.2010.536735

Hinduja, S. (2008). Deindividuation and internet software piracy. *CyberPsychology & Behavior*, *11*(4), 391-398. doi: 10.1089/cpb.2007.0048

IP address. (n.d.). Retrieved August 6, 2014, from http://www.merriam-webster.com/dictionary/IP address

James, R. (2009, June 01). A brief history of cybercrime. Retrieved from http://content.time.com/time/nation/article/0,8599,1902073,00.html

Lewis, J. (2005). Aux armes, citoyens: Cyber security and regulation in the united states. *Elsevier's telecommunications Policy* , 2-3. Retrieved from http://csis.org/files/media/csis/pubs/050825_cybersec_and_regulation.pdf

Obama, B. Office of Press Secretary (2013). *Executive order -- improving critical infrastructure cybersecurity (EO 13.636)*. Retrieved from The White House website: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Plassaras, N. (2013). Regulating digital currencies: Bringing bitcoin within the reach of the imf. *Chicago Journal of International Law*, *14*(1), 377-407. Retrieved from http://eds.b.ebscohost.com.libproxy.eku.edu/ehost/detail?sid=37c66d2a-

0c59-4f52-9eb5-289c40216540@sessionmgr113&vid=7&hid=107&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl

Richards, C. (2015, July 05). FinCEN Examinations of Digital Currency Businesses 'Will Drive Innovation Overseas' Retrieved April 11, 2016, from http://cointelegraph.com/news/fincen-examinations-of-digital-currency-businesses-will-drive-innovation-overseas

Tsfati, Y., & Weimann, G. (2002). www.terrorism.com:. *Studies in Conflict & Terrorism*, (25), 317-332. doi: 10.1080/1057610029010121 4

White House, Office of the Press Secretary. (2013). *Critical infrastructure security and resilience*. Retrieved from website: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Appendix A:

Importance of Anonymity Online Survey

Importance of Anonymity Online Survey

1. What is your age?
   a. 18-24
   b. 25-29
   c. 30-34
   d. 35+
2. What is your gender?
   a. Male
   b. Female
3. What is your race?
   a. African American
   b. Hispanic
   c. White
   d. Other
4. To which college do you belong?
   a. Justice & Safety
   b. Business & Technology
   c. Arts & Sciences
   d. Education
   e. Health Sciences
5. I value anonymity while online.
   a. 1=strongly disagree
   b. 2=slightly disagree
   c. 3=undecided
   d. 4=slightly agree
   e. 5=strongly agree

6. What types of activities do you engage in online? (Check all that apply)
   a. Social Media
   b. Shopping
   c. News
   d. Email
   e. Gaming
   f. Research
7. I value pseudo-anonymity (ability to assume a different identity) while online.
   a. 1=strongly disagree
   b. 2=slightly disagree
   c. 3=undecided
   d. 4=slightly agree
   e. 5=strongly agree
8. If given complete anonymity I would engage in the download of pirated software
   a. 1=strongly disagree

   b. 2=slightly disagree
   c. 3=undecided
   d. 4=slightly agree
   e. 5=strongly agree

9. If given complete anonymity I would purchase of illegal goods
   a. 1=strongly disagree
   b. 2=slightly disagree
   c. 3=undecided
   d. 4=slightly agree
   e. 5=strongly agree

10. If given complete anonymity I would hack personal or business networks online.
    a. 1=strongly disagree
    b. 2=slightly disagree
    c. 3=undecided
    d. 4=slightly agree
    e. 5=strongly agree

11. I have engaged in the download of pirated software, music, or videos.
    a. 1=strongly disagree
    b. 2=slightly disagree
    c. 3=undecided
    d. 4=slightly agree
    e. 5=strongly agree

12. Online Hacking is relatively harmless and poses little threat to United States security interests.
    a. 1=strongly disagree
    b. 2=slightly disagree
    c. 3=undecided
    d. 4=slightly agree
    e. 5=strongly agree

13. Are you familiar with digital currencies such as Bitcoin?
    a. Yes
    b. No

14. Digital Currencies, such as Bitcoin, and others are good alternatives to hard currency. i.e. Dollar, Euro, Yen
    a. 1=strongly disagree
    b. 2=slightly disagree
    c. 3=undecided
    d. 4=slightly agree
    e. 5=strongly agree

15. The ability of digital currencies to allow an individual to make anonymous purchases online is a positive concept
    a. 1=strongly disagree
    b. 2=slightly disagree
    c. 3=undecided
    d. 4=slightly agree
    e. 5=strongly agree

16. If given complete anonymity through the use of digital currency I would make contributions to controversial groups to whom I would otherwise not contribute.
    a. 1=strongly disagree
    b. 2=slightly disagree
    c. 3=undecided
    d. 4=slightly agree
    e. 5=strongly agree

Appendix B:

Frequency Distributions of Demographic Characteristics

Frequency Distributions of Demographic Characteristics

Variable	N	%
Sex		
Male	17	23%
Female	56	77%
Race/ethnicity		
African American	44	60%
Hispanic	14	19%
White	3	4%
Other	12	16%
Age Range		
18-24	44	60%
25-29	14	19%
30-34	3	4%
35+	12	16%
College		
Justice & Safety	18	25%
Business & Technology	10	14%
Arts & Science	25	34%
Education	15	21%
Health Sciences	5	7%
Social Media Usage		
Social Media	62	86%
Shopping	61	85%
News	54	75%
Email	67	93%
Gaming	26	36%
Research	53	74%