CYBER SPACE: IS THE INTERNET A BREEDING GROUND FOR TERRORISM?

Tiffani L. Hume

Tiffin University, Tiffin Ohio

School of Criminal Justice Administration

Abstract

Across the United States cyber crime has hit all time highs with the advancement of the electronic medium. Such mediums have evolved from the telephone to computers, laptop computers, cell phones, fax machines, I Phones, Blackberries and many more wireless, portable devices that have internet access. This article will focus on the growing trend of cyber crime, the impact cyber crime has on the United States and how exactly cyber crime is impacting the state of Ohio. In addition, this article is concerned with the connection of cyber crime and its possible connection to terrorism.

Introduction

The United States federal government and local law enforcement spend a great deal of time investigating cyber attacks by criminals, foreign adversaries, sexual predators and terrorists. The Director of the FBI has placed the protection of the U.S. against cyber-based attacks and high technology crimes as the number three priority within the FBI. With the grown dependency on computers throughout the nation, people from all walks of life, all ages, cultures and beliefs are now turning to communicate not only locally, but abroad. Such reasons for communication may be to promote their own causes, covertly communicate with others, shop online, or to provide services. With these businesses and individuals conducting business around the clock it is easy for the innocent to be preyed upon by those hiding in the shadows.

The potential damage to our national security from a cyber-based attack includes devastating interruptions of critical communications, transportation, and other services. Additionally, such attacks could be used to access and steal protected information and plans. Law enforcement members spend a vast amount of time attempting to and often successfully preventing criminals, sexual predators, and others who intend on malicious destruction from using the Internet and online services to steal from, defraud, and otherwise victimize citizens, businesses, and communities.

However, something to remember is that the Internet produces an atmosphere of virtual fear or virtual life. People are afraid of things that are invisible and things they don’t understand. The seed of Cyber fear is planted by questions of whether an internet attack can actually bring down airliners, ruin critical infrastructure, destroy the stock market, reveal Pentagon planning secrets, etc.? The truth of the matter is that cyber attacks actually take planning and testing which takes time. With the ongoing immigration problem in the United States, the 14 million or more people who are residing in the United States without proper credentials and those who are residing in the United States illegally that we do not even know of, provides a possible breeding ground for a domestic terrorist attack or even an international terrorist attack physically and even online if they can obtain easy access.

Aside of the concerns listed above; there are many computer scientists and homeland security experts who also have concerns that the internet and cyber space is a testing ground for terrorists and to expand their agenda. The concerns are slightly different than those listed above because they look to terrorist acts that will cause such damage as to effect the nation’s financial network, which may lead to the shut down the flow of banking information located in databases; or possibly effect computer systems that operate water treatment plants as a means to contaminate the water supply; or interrupt networks that control the electrical grids and dams; or even effectuate the facilities that control the flow of information over the internet.

Observing these concerns and assessing terrorism in general, the terrorist themselves cannot necessarily just blast out with a cyber terrorism attacks that cause mass destruction because they need time to achieve their overall agenda and depending on what they are trying to do, they need to *raise money* in order to cause a catastrophic event. If no funding or very little funding is required the terrorist will need to gain the trust of the people and solicit them to support some kind of effort.

Overall, if a terrorist will go to the lengths of doing what is called “dry runs” for terrorist attacks inside the United States whereby they may plant a pseudo bomb in a specific location and wait to see if it goes undiscovered or not (like that of the New York City attempted car bomb), or what reaction they receive, the terrorist will also do the same over the internet. Every single day countless homes and offices across the nation are being broken into through the mediums of laptops, computers and wireless devices simply by hacks and bits of malicious code.

Although, some perpetrators are young teenagers who want bragging rights, the more serious in nature are those who are businesses trying to steal corporate information from another business (industrial espionage). Other types of cyber crimes are international rings of criminals attempting to steal identities and sell their information on the black market. An example of this is where the social security number and birth certificate of a U.S Citizen is stolen and sold to illegal aliens who come into this country and purchase them.

When looking at internet crime trying to figure out what the criminal is intending to do and why is often very complex and hardly cut and dried. For example, as we see through this article, it will be clear that crimes such as fraud, non delivery of merchandise or payment and other crimes are being committed, but would you, the reader, connect this to a test run for a future terrorist attack? Sometimes leads fall into place where the investigator least expects them to be, “right under the nose”.

In some instances, innocent people are drawn into the internet because they need something or are looking for something. For example, some people shop online and use their credit cards, some are using social media such as facebook, MySpace, Internet instant messages or they are using dating services or looking for quick fixes to financial help. Whatever the reason, people every day get online and access the internet with some type of computerized mobile or stand alone device. When surfing e-mail or the internet people see pop up messages, advertisements or are doing online searches whereby they may see an advertisement like that of the Haitian earthquake relief website which is an online scam that solicits people to donate money in the aftermath of the earthquake; the money never reaches the victims and the sender becomes the victim of fraud.

Other scams consist of new twists on counterfeit check schemes which target U.S. law firms. Another instance of an online scam is the holiday shopping tips which advertise auctions or other means of buying products which are never delivered, but paid for. The list goes on to include many more scams to take the money out of desperate people who trusted enough to provide a credit card and their personal information. The question still stands, are these scams a test to see if the perpetrator can get away with this type of crime and if so they will make a more global approach with a newer more up scaled idea? Since we are exploring the correlation between cyber crime and terrorist attacks let's take a retrospective approach and use the clues left behind by a specific cyber crimes to develop a specific description of the perpetrators possible motive.

Methodology

This report is based on IC3 statistics from the year 2004 through the year 2009. IC3 has made a number of changes to the way it gathers and classifies complaint data. Beginning January 1, 2009, IC3 implemented a new complaint classification. This system is based on an updated questionnaire, designed to capture data on various aspects of a complaint and generate an automatic classification in terms of the complaint's offense content.

Prompting the redesign of the classification system were criticisms of the previous system's ability to protect validity and reliability. The previous system had as many as 157 complaint categories; many of which were either vague, non-mutually exclusive, or both. The application of these categories produced inconsistencies and classification errors, making it difficult to discern the prevalence of certain types of victimization. The new classification system was designed to minimize such errors.

Results

Globally, the United States was the most heavily targeted nation for cyber crime since their complaints sit currently at 65.4%; The United Kingdom 9.9% is the next highest nation targeted with cyber crime; Nigeria 8.0%, Canada 2.6%, Malaysia 0.7%, Ghana 0.7%, South Africa 0.7%, Spain 0.7%, Cameroon 0.6%, and finally Australia 0.5% (IC3 Internet Crime Report, (2009)). Over all it can be seen by these statistics that the United States is being targeted more than any other nation by foreign and domestic cyber crimes.

With respect to the United States the following states are the top ten states who reported cyber crimes and these are the percentages of cyber crime complaints: California reported a 13.9% cyber crime report rate for the year 2009; Florida 7.5%; Texas 7.3%; New York 5.2% New Jersey 5.0%; Illinois 3.6%; Pennsylvania 3.4%; **Ohio 3.0%;** Virginia 2.9%; and Washington 2.8%.

Taking an interest in specifically the state of Ohio, the following statistics for the years starting from 2008 and moving backward to the year 2004 have been provided to determine the impact of cyber crime on the state of Ohio so that the determination of an increase or decrease in cyber crime has occurred. Further, we will seek to find out if there is any footprint of possible links to terrorist attacks that might be in the planning.

The findings of this study provide that in 2008, the Federal Bureau of investigations computer crimes division known as the IC3, received at total of 7285 complaints from the state of Ohio by itself (Ohio IC3, (2008)). The statistics show that the top ten complaint categories in the state of Ohio are: (1) Non Delivery of Merchandise /Payment 33.6%; (2) Auction Fraud 26.3%; (3) Credit Card Fraud

9.1%; (4) Confidence Fraud 8.3%; (5) Check Fraud 4.9 ; (6) Nigerian Letter Fraud 4.9%; (7) Computer Fraud 3.9%; (8) Financial Institutions Fraud 3.0%; (9) Identity Theft 1.4% and (10) General Threat 1.3%. What is even more interesting about this is that 77.6% of the perpetrators were men and the other 22.4 % were reported to be women with respect to Non Delivery of merchandise/payment and auction fraud. The total median dollar loss for all complaints reporting a dollar loss was $710.00 (Ohio IC3, (2008)).

In 2007 the IC3 received a total of 5640 complaints from the state of Ohio (Ohio IC3, (2007)). In the year of 2007, the top ten reported cyber complaints were (1) Auction fraud at 37.6% (2) Non Delivery of Merchandise /Payment 25.0% (3) Confidence Fraud 8.1% (Ohio IC3, (2007)), (4)Credit Card Fraud 5.9%, (6)Check Fraud 5.5%, (7) Computer Fraud 3.9% Financial Institutions Fraud 3.8%, (8) Identity Theft 2.5%, (9) Nigerian Letter Fraud 2.4% and (10) Threat 1.0%. In this case, the top dollar loss complaint involved non-delivery and totaled $445,000.00 while reported losses throughout the state exceeded $6.8 million (Ohio IC3, (2007)). In comparison to the year 2008, the total number of men who were perpetrators was 74.2% and the number of female perpetrators was 25.8%.

In the year 2006, the IC3 received a total of 5815 complaints from the state of Ohio and in this case there were nine (9) not ten top complaints. This is significant because as we reflect back we are seeing a lesser patter of cyber crime in the state of Ohio. The first reported cyber crime is Auction Fraud at a 48.2%; (2) Non Delivery of Merchandise /Payment 17.6% (3) Check Fraud 5.8%; (4) Credit Card Fraud 4.4%; (5) Confidence Fraud 2.6% ; (6) Computer Fraud 2.4%; (7) Identity Theft 1.6%; (8) Investment Fraud 1.6% and (9) Financial Institutions Fraud 1.4% (Ohio IC3, (2006)) . The overall dollar amount loss for non-delivery totaled $86,079.00 while reported losses throughout the state totaled nearly $6.6 million (Ohio IC3, (2006)). For the year 2006 the total number of perpetrators that were male totaled 76.2% whereas the female perpetrators totaled 23.8% (Ohio IC3, (2006)).

In the year of 2005, 6148 complaints of internet crime were reported from the state of Ohio. Of those complaints The top 6 complaints reported were (1) Auction Fraud 62.5% ; (2) Non Delivery of Merchandise /Payment 13.2% ; (3) Credit Card Fraud 6.4% ; (4) Check Fraud 2.7% ; (5) Computer Fraud 1.3% and (6) Confidence Fraud 1.0% (Ohio IC3, (2005)). The total dollar amount of damages was $175,000 and the number of male perpetrators totaled 76.2% whereas the total number of female perpetrators totaled 23.8%.

In the year of 2004, the IC3 reported 2115 complaints of internet crime from the state of Ohio. The complaints reported were (1) Auction Fraud at 70.7%, (2) Non Delivery of Merchandise/ Payment at 15.3%; (3) Credit Card Fraud at 5.7% and (4) Check Fraud at 1.9%. The total dollar amount in damages amounted to $196,000.00 and the reported male perpetrators totaled 71.8%, whereas the total number of female perpetrators was 28.2% (Ohio IC3, (2005)).

Discussion

In breaking down the results and taking a deeper look at what has happened from the year 2004 until the year 2008 we can see that auction fraud and non delivery of merchandise /payment have been competing with one another for the last four years in the state of Ohio. This is significant for a couple of reasons: (1) these crimes are continual over four years and have show to be the lead cyber crimes committed so far. This can be that since the percentage of male and female perpetrators are show in the statistics that law enforcement is cracking down on this and at least making some headway in slowing these crimes down or (2) this could show that although the law enforcement agents are making these arrests there may be another higher percentage of fraudulent acts that are not seen. Seeming how these are growing in nature in the state of Ohio based on those agencies who participate in reporting their statistics, there may be cause to bring these crimes to light over a public media and warn the citizens of Ohio not to entertain these types of scams if they should be exposed to them.

In looking and comparing the different crimes committed online, it is apparent that other crimes have been tried such as Financial Institutions Fraud in the year of 2006 that had a perpetration rate of 1.4%. It is interesting that this crime has been at a very low rate over the four year period and fluctuates as if perpetrators are testing different methods of attempting this type of crime through computerized mediums. The other possible answer to this is that this type of crime is being diverted through law enforcement measures and better business practices through corporate policy enforcement.

However, the Nigerian Letter Fraud is interesting because it is ranging in the 4.9% area in the year 2008 which is a jump from 2007 which the complaints raged in the 2.4% crime rate. This figure is nearly doubled. This is interesting because it has not show up in previous years in the state of Ohio which indicates that this particular crime is now expanding into Ohio and needs to be publically addressed for the general welfare of the Ohio citizens. In taking a closer look at what the Nigeria Letter Fraud is we can think about how this might be related a terrorist type of activity if at all.

This scam is the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, mailed from Nigeria, offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author, a self-proclaimed government official, is trying to transfer illegally out of Nigeria (Federal Bureau of Investigations (2010)). The recipient is solicited or enticed into sending information to the sender, such as blank letterhead stationery, bank name and account numbers and other identifying information using a facsimile number provided in the letter.

The perpetrator has also been known to send these by regular mail and by email. Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria. In actuality, the millions of dollars do not exist and the victim eventually ends up with nothing but loss. If the individual stops sending money, the perpetrators have been known to use the personal information and checks that they received to impersonate the victim, draining bank accounts and credit card balances until the victim's assets are taken in their entirety (Federal Bureau of Investigations (2010)).

By public awareness this can divert, decrease or even prevent this crime from taking place in the state of Ohio. Another interesting aspect of this is that if citizens of these states participate in a crime like this Nigerian Letter Fraud, they are consenting to assisting in the movement of monies to and from Nigeria and are also consenting to larceny. This would mean that if a person who consents to this believing that they will get to share millions of dollars once the money is transferred out of Nigeria, they can be bribed or recruited to do other things. This is a particularly interesting position because if a person has the propensity to engage in illegal activity such as this type of crime, maybe they could be bribed into giving out passwords or other security information for different things such as computers system that control power grids, hospitals or economic databases etc.

Further, on this issue, Al Qaeda has strong ties to different groups throughout the continent of Africa and Asia which could tie into scams like this to raise money for their cause. Thus, this type of scam needs appropriate attention because it could be a test of ability, strategy and method to plan out future types of attacks on a grand scale by recruitment.

Possible Crime Preventions

Solutions to preventing cyber crime, reducing cyber crime and issue spotting possibilities of terrorist attacks that may be on the rise, the participation of all law enforcement agencies in this matter is critical because as analysts we need to see what states are become more infected with these types of crimes. Once we are able to see the statistics of these crimes, we can begin to educate the public on what exactly is happening and make an overt attempt to protect the public through awareness and education.

Secondly for law enforcement purposes, it is critical to analyze these reports so that these crimes can be watched and evaluated as to whether these crimes are decreasing, increasing, possible an old scam revised and up scaled or if this is a “dry run” for a potential terrorist attack.

The next solution is to get the FBI to engage in adding a cyber crimes publication or television program in comparison with America’s most wanted. This is something that is urged because people are more likely to inform the FBI or local law enforcement of what they see or have heard about or maybe provide tips on suspicious people and activities without having to be identified themselves. If the public is aware of new cyber crimes over the news or on Americas Most Wanted they are likely to get motivated to assist with observing and reporting.

In spotlighting this suggestion, it is contended that this will disinfect potential terrorist homegrown or other by placing them directly into the sun light and exposing them to the world and or U.S Citizens. This will assist in the work of the investigators because leads will be generated that would not otherwise be available without more law enforcement man power. The last suggestion and probably the least expensive solution would be to do a weekly talk show over cyber security and education where the speaker can address one new threat in a 30 minute time frame and then allow callers to call in and ask questions. Further this would generate another option for leads and give the U.S Citizens a feeling of being able to assist instead of being shut out or uninformed.

Conclusion

Terrorists will go through great lengths to test the ability, strategy and reaction of planning out a test run for a terrorist attack long before they go for the full Monte. If the terrorist will go to that extreme for a physical attack, they will surely be looking for more effective ways to create other types of terror attacks such as using the internet as a medium. The internet is a link to a different form of terrorism which is now known as Cyber terrorism. There is evidence that Ohio is growing in cyber crime each year and the state of Ohio needs to be made more aware of the cyber crimes that are embedding in the state, which can be effected, how the citizens and state can be affected and what they can do to prevent this type of problem from continually growing.

Cyber terrorism can affect the electrical grids which are controlled by computers, it can effect water treatment facilities, hospitals and other areas of public concern that are ran by computers or controlled by computers. Although this takes planning, time and a fair amount of money to accomplish, it still requires the respect and attention of law enforcement as well as the public. In addition, the questions exist as to what type of an attack the criminal or terrorist is planning, will it be costly? Will it be effective in achieving their goal and will the recipient “feel terror”. Based on some of these qualifiers, not all terrorists are going to act in a logical, rational manner and plan so ever carefully a strategic plan. Some terrorists will still carry out the primitive and very culturalistically, trademarked methods of suicide bombings, car bombings and other methods of terrorism.

For the sake of this journal article, it can be concluded based on statistics that fraud scams are very much in the lead as well as non delivery and payment scams where as other types of cyber crimes are less prevalent , but are fluctuating in numbers as if one of two things is happening: (1) the perpetrator is using the internet as a test site to check the ability, strategy and reaction of the crime being committed to commit a simple crime or perhaps upscale the crime into something more nationally or globally broad; or (2) law enforcement is effective enough in those areas that the crime is actually reducing in that particular state.

Although no crime should go ignored, the state of Ohio is now starting to see the Nigerian Fraud Letters penetrate into its jurisdiction as well as other types of cyber crimes. Is this an act of defrauding Americans for a terroristic fund raiser or is the victim actually being solicited for a different cause? The way to combat this is to start making better efforts to inform the public. Strong education of the cyber crimes, scams and alerts should be widely publicized to all residents of every state whether it is through television radio or news papers, there needs to be a better attention getting method to reaching the people, educating them and giving them the power to observe and report.

REFERENCES

Burgess, A.E., Burgess A.W., Douglas, J.E. and Ressler, R.K. (2006) Crime Classification manual: A standard System for investigating and classifying violent crimes 2nd Ed Jossey-Bass, San Francisco CA

Federal Bureau of Investigations (2010) Cyber Investigations
Information retrieved on Tuesday, August 24, 2010 from website:
http://www.fbi.gov/cyberinvest/cyberhome.htm

Federal Bureau of Investigations (2010) Nigerian Letter or 419 Fraud
Information retrieved on Tuesday, August 24, 2010 from website:
http://www.fbi.gov/majcases/fraud/fraudschemes.htm#nigerian

Ohio IC3 (2008) Ohio IC3 2008 Internet Crime Report
Information retrieved on Tuesday, August 24, 2010 from website:
http://www.ic3.gov/media/annualreport/2008/Ohio%202008%20Report.pdf

Ohio IC3 (2007) Ohio IC3 2007 Internet Crime Report
Information retrieved on Tuesday, August 24, from website:
http://www.ic3.gov/media/annualreport/2007/Ohio%202007%20Report.pdf

Ohio IC3 (2006) Ohio IC3 2006 Internet Crime Report
Information retrieved on Tuesday, August 24, 2010 from website:
http://www.ic3.gov/media/annualreport/2006/Ohio%202006%20Report.pdf

Ohio IC3 (2005) Ohio IC3 2005 Internet Crime Report
Information retrieved on Tuesday, August 24, 2010 from website:
http://www.ic3.gov/media/annualreport/2005/Ohio%202005%20Report.pdf

Ohio IC3 (2004) Ohio IC3 2004 Internet Crime Report
Information retrieved on Tuesday, August 24, 2010 from website:
http://www.ic3.gov/media/annualreport/2004/Ohio%202004%20Report.pdf

Pfleeger, C.P and Pfleeger, S.L. (2007) Security in Computing 4th Ed
Pearson Publishing, Upper Saddle River, NJ

Stohl, M (2006) Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? Crime Law Soc Change 46:223-238