THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

OBSTACLES IN PROSECUTING TRANSNATIONAL CYBER CRIMINALS

ANDREW C. CLAY
SPRING 2011

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Information Sciences and Technology
with honors in Information Sciences and Technology

Reviewed and approved* by the following:

Donald R. Shemanski
Professor of Practice
Thesis Supervisor

Dr. Rosalie Ocker
Senior Lecturer
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

The process of prosecuting transnational cyber criminals and terrorists is complex and many such crimes are never pursued for many varying reasons, including cultural and legal differences as well as difficulties inherent in the extraterritorial application of a state's domestic laws. This thesis focuses on the evolving process in which transnational cyber criminals and terrorists are tracked and prosecuted. With the help of leading experts in the field I have indentified the key issues facing international cyber crime and have offered suggestions to improve the process.

While there are many technological hurdles to attributing cyber crimes to specific individuals, the main issues facing transnational crimes are cooperation between governments and mutual legal assistance procedures. Treaties such as the Council of Europe Treaty on Cybercrime only have support from certain Western countries and still lack adequate definitions of intellectual property violations. Furthermore, the treaty has often been proven ineffective among member states involved in the Council of Europe. Lack of requirements for points of contact between nations and the lack of effective means to punish those who do not cooperate have made the treaty ineffective at fulfilling the purpose for which it was drafted.

The analysis led to several suggestions. Ultimately transnational cyber crime is an issue of cooperation and diplomacy. The United States alone cannot compel international cooperation; however parties of the Council of Europe treaty could revise the treaty in talks with dissenting nations. There needs to be agreement on the approach of reacting to crimes as they occur, regardless of where the attack is originating. Additionally, there must be an improvement in the process of investigation, as a single point of contact is not enough to properly respond to the high volume of attacks and crimes.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS iii

Chapter 1 Domestic Process 1

Agencies and Responsibilities 1
Technical Issues 2

Chapter 2 Transnational Process 4

Current Issues 4
MLATs, Legal, and Cultural 5
International Efforts 6
TFTP, Swift, and International Cyber Security 8
Background 8
Legal Basis 8
Current TFTP Debate 11
Cyber Warfare 11
Cyber Crime 13

Chapter 3 Analysis 16

Introduction 16
The Issue 18
The Current Process 21
Failures of the Council of Europe 21
Law Enforcement Approach vs. Immediate Military Intervention 23
Proposed Solutions 24
Prosecution Issue 24
Political Issue 25
Public Company Reporting 26
Improve Points of Contact 26
Host Country Trial 27
Leadership Support 28

Bibliography 29

ACKNOWLEDGEMENTS

I would like to thank everyone involved in helping make this thesis a successful and rewarding experience. Without the generous sacrifice of time and effort of these individuals it would not be where it is today:

Don Shemanski – Professor of Practice and Honors Thesis Advisor

Robert Knake – Author and DHS Cyber Crime Expert

Ed Gibson – International Cyber Crime Expert

Rosalie Ocker – Honors Advisor

Chapter 1

Domestic Process

Agencies and Responsibilities

The research that I performed on the topic involved gaining an understanding of the domestic prosecution of cyber criminals before tackling transnational proceedings. Many of the same obstacles exist in both arenas, but domestic prosecution does not require legal cooperation and assistance from a foreign entity. This is a list of the domestic agencies and their responsibilities for fighting cyber crime:

Agency Responsibilities

- The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA).
- FBI - National Infrastructure Protection Center (NIPC.) Fights and Investigates Cyber Crimes
- The Directorate of Information Analysis and Infrastructure Protection (IAIP), part of the Department of Homeland Security (DHS.) Focused on protecting infrastructure against terrorist attack
- The National Cyber Security Division (NCSD) United States Computer Emergency Response Team (US-CERT.) - charged with improving computer security preparedness and response to cyber attacks in the United States. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. US-CERT is the operational arm of the NCSD at the DHS.
- The National Communications System (Department of Defense), which coordinates emergency preparedness for the telecommunications sector. (Megias pg 1)

FinCEN, the Financial Crimes Enforcement Network of the United States Department of the Treasury, is the organization in charge of safeguarding our financial systems and

enhancing the U.S. national security through deterrence of criminal activity. It was created as a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). They act as an important intermediary for banks, the financial industry and law enforcement agencies to aid investigations of crimes and help ensure the security of the financial system. They offer an excellent guide for individuals who feel they have been the victim of an internet crime:

Guide for Victims

- Fraud or Money Laundering Scam: Contact local law enforcement or if a federal crime visit www.stopfraud.gov
- Identity Theft or SPAM: Contact the FTC
- Internet Crime or Scam: Contact the Internet Crime Complaint Center www.ic3.gov
- Stole Credit Card Number: Call issuer of credit card
(FinCEN pg 1)

Often it is not just one of these crimes that have been committed, which further complicates the process of resolution. IC3 recognizes the complexity of these cases, which is why in part they exist. In order to resolve complaints, IC3 first reviews them and based on their judgment refers the cases to the appropriate federal, state, local, or international law enforcement or regulatory agency. If those agencies believe the case requires their attention they may assign an investigator to it, but there is no guarantee that every complaint will be fully investigated. (FinCEN)

Technical Issues

The technical obstacles to prosecuting crime exist no matter domestic or international. Anonymity, speed of attack, increased vulnerability, and lack of evidence

doom many investigations. Furthermore, a lack of confidence by businesses that an investigation would be successful deters sufficient reporting of crimes. **(Krebs)** For individuals, the process is generally confusing as there are many agencies and no clear avenue for prosecution **(Lewis)**. Since the Internet is an instantaneous means of communication, crimes occur instantaneously and evidence can be erased right after it occurs. This leads to a high frequency of crimes committed very quickly that are difficult to investigate; all of these are variables that lead to problems for law enforcement.

The Internet is built on technologies, such as TCP/IP, that were meant for a close looped network where all users could be verified as trustworthy. Security was not the main priority of these early systems but many of the same standards were kept as the Internet boomed. The 2003 U.S. National Strategy to Secure Cyberspace recognized security issues with TCP/IP, Domain Name Systems, and the Border Gateway Protocol. The strategy came to the conclusion that private industry would drive the development of these three protocols towards security without the need for the federal government's involvement. However, as of September 2010, private industry has yet to adequately secure them. **(Knake)**

The federal government is looking into the development of new security protocols. In October of 2009, the **D**efense **A**dvanced **R**esearch **P**rojects **A**gency contracted out to Lockheed and Juniper Networks to develop a new Military Protocol. The idea is to attribute every packet to a person, allow for prioritization of packets, and further encryption technologies. This would be used solely for government purposes and is a long way off from implementation. **(Cyber War)**

Chapter 2

Transnational Process

Current Issues

The current events articles involved in this review all share one common theme; the concerns over our vulnerability as individuals and a nation are growing. President Obama is quoted as saying, "It is now clear this cyber threat is one [of] the most serious economic and national security challenges we face as a nation," "We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness." **(CBS pg 1 p 11)** As quoted by Jim Lewis, CSIS, "In 2007 we probably had our electronic Pearl Harbor. It was an espionage Pearl Harbor," Lewis said. "Some unknown foreign power, and honestly, we don't know who it is, broke into the Department of Defense, to the Department of State, the Department of Commerce, probably the Department of Energy, probably NASA. They broke into all of the high tech agencies, all of the military agencies, and downloaded terabytes of information. The Library of Congress, which has millions of volumes, is about 12 terabytes. So, we probably lost the equivalent of a Library of Congress worth of government information in 2007," Lewis explained. “Some of us call it 'the death of a thousand cuts.' Every day a little bit more of our intellectual property, our innovative skills, our military technology is stolen by somebody. And it's like little drops. Eventually we'll drown. But every day we don't notice," **(CBS pg 1 p 21) (Lewis)**.

MLATs, Legal, and Cultural

Transnational issues have all the technical complexities of domestic issues with the addition of legal and cultural differences. Several of the sources **(Lewis, Krebs, Ultrascan)** point out how the issue is technical, cultural, and governmental. Technically it is very difficult to provide evidence as to who is responsible for a breach. While many of the actions against the US Government would be considered acts of war or treason, it is too difficult to justify retaliation without being able to prove a direct affiliation. While it may be possible to track an attack to a host country it can be very difficult to identify the party responsible. The first step is cooperation by the host country through Mutual Legal Assistance Treaties (MLATs). **(United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Section I.C.7)** If an attack occurs in a country that has an agreement with the victim country, they can work together to identify the party responsible. However, the power still resides with the host country. While many Mutual Legal Assistance Treaties exist, there are still many countries that act as safe havens for cyber criminals and they can choose to not extradite their citizen, especially if the exact crime isn't punishable under their law. Boundaries no longer separate peoples in social or economic markets; however law is still bound by location and culture. **(Secretariat, Twelfth United Nations Congress on Crime Prevention and Criminal Justice)**

International Efforts

While countries have individually agreed to MLATs, there have been conferences to come to a more consensus agreement of international cyber crime. The only widely accepted agreement currently in place is based off the Budapest Convention on Cyber Crime that has been signed or ratified by 46 countries since being drafted by the Council of Europe in 2001. **(Masters)** The UN most recently held a conference in April of 2010 where a UN Cybercrime Treaty was rejected. The main contentions for its ultimate failure hinged on disagreements between the western capitalist countries, including the US and Britain, and developing nations, Russia, and China. Developing nations and Russia have called for a new agreement meant to combat cybercrime while the US and Britain prefer to work from the standing agreement from the Budapest Convention. The main difference and point of contention stems from the Budapest Agreements permission grants for foreign police, "The Budapest Convention sanctions police to cross national boundaries, without consent from local authorities, in order to access servers – with the caveat that the owners of the network systems give permission. Russia has opposed this measure since 2000 when police from the United States gained access to computers owned by Russian men accused of defrauding U.S. banks." **(Masters, pg 1)** While this contention has always existed, Britain has pushed to further review the Budapest Agreement that could possibly result in the broadening of powers. They cite the necessity for this review has to do with emerging technologies, such as cloud computing, that can allow criminals to exist on many systems across many borders.

The UN Cybercrime Treaty was rejected but only because of a disagreement on the terms and not because countries do not recognize the magnitude of the problem. The main issue facing prosecution of cyber criminals to the UN was the inefficiency of investigations when involving two sovereign nations. There exists an enormous gap between the speed in which a crime can be committed transnationally over the web and the time it takes for a response by governing officials. Along with the speed of the crime itself, they also make the point that evidence on computers can disappear soon after the crime has been committed, furthering the importance of local authorities. The UN considers it vital that existing MLATs become less formal, complex, and time consuming in order to effectively fight cybercrime. **(Secretariat, Twelfth United Nations Congress on Crime Prevention and Criminal Justice)**

After outlining the issues of transnational prosecution, they laid out a short set of recommendations. The main goal of these recommendations was to close the gap on legislative differences, improve outreach to developing nations, and decrease the response time on investigations. The main goal is to improve international cooperation to reduce or eliminate safe havens for criminals. This can only be done with consistency of laws between nations. One of the focuses the UN would like to lead is helping developing countries cope with cybercrime and to aid in investigations within those nations. While much transnational cybercrime is initiated from developing nations, they are also at great risk themselves. Since most do not have the infrastructure in place to protect citizens, the UN will play a vital role in the coordination of local authorities. Most of their goals and recommendations are non-specific in a technical nature, but instead focus on awareness

for governments, authorities, and the public. **(Secretariat, Twelfth United Nations Congress on Crime Prevention and Criminal Justice)**

TFTP, Swift, and International Cyber Security

Background

The Terrorist Finance Tracking Program (TFTP) is a United States government program run out of the Department of the Treasury that utilizes financial transaction information from the SWIFT database in order to find and track terrorist financiers. The program was initiated weeks after September 11th and was said to be limited to people suspected of having ties to Al Qaeda and has been touted as being a strong tool in the fight against terrorism. SWIFT, the Society for Worldwide Interbank Financial Telecommunication, is a Belgian based cooperative that supplies secure messaging services and interface software to wholesale financial entities. **(U.S. Department of the Treasury) (Lichtblau and Risen)**

Legal Basis

The United States government stands by its legal authority to access the SWIFT information, although it has been met with much opposition in Europe. The program's legal standing has been described as a grey area at best and an overreaching exploitation of loopholes that ignores due process at the worst. The United States government bases

its legal authority in the International Emergency Economic Powers Act, which was invoked by former President Bush after the attacks on September 11th, 2001. The letter of the law gives the president a far reaching authority to "investigate, regulate or prohibit" foreign transactions in response to "an unusual and extraordinary threat." The Supreme Court ruled in 1976 that Americans had no constitutional right to privacy for records held by banks or other financial institutions. In 1978, the Congress passed in response to the ruling the Right to Financial Privacy Act, which restricts government access to banking records. The legality of TFTP was initially reviewed by the Treasury Department lawyers with consultation by the Justice Department and the two came to the conclusion that the privacy laws applied to individual banks and not banking cooperatives such as Swift. Additionally, they said the law protects individuals and small companies but not major institutions that route money through Swift on behalf of individuals. Finally, because Swift was a foreign based company but had offices in the United States, the organization was liable to follow both European and US law. **(Lichtblau and Risen) (U.S. Department of the Treasury)**

After this initial legal debate concluded, the United States government felt comfortable enough in their standing to pursue broad access to these financial transaction records. While prior to 9/11 most records of this type would take grand-jury subpoenas or court-approved warrants, since then the F.B.I. more frequently uses an administrative subpoena known as a national security letter. This allows the federal government to bypass the judiciary branch to seize records. In order to enhance the programs legal standing, the Bush administration attempted to pass regulations requiring American banks to turn over records of international wire transfers. **(Lichtblau and Risen)**

The opposition to TFTP can be noted as one of the examples to the complexities facing international prosecution of criminals and terrorists. While the program itself has led to arrests of individuals supporting terrorism and has also had many successes, privacy law differences and lack of trust of America in Europe has fueled the opposition of the program. Many of the programs successes are kept secret and are classified, but the New York Times attributes several events to TFTP. Among them are:

Events Stopped by TFTP

- The capture of Hambali, the mastermind behind the 2002 bombing of a Bali resort
- Provided financial data for investigations into possible domestic terrorist cells and Islamic charities with links to extremists
- Helped identify and convict a man from Brooklyn on terrorism-related charges

(Lichtblau and Risen, pg 3)

After the New York Times published the existence of the program, SWIFT moved most of its data out of the United States, forcing the government to negotiate a deal with Europe to keep the program running. Recently, an agreement has been reached between Europe and the United States to continue the program with the condition that every investigation must operate through an anonymous person appointed by a commission within the European Union. This anonymous person has full control over the investigation and has the authority to refuse any request. The fate of the programs future and effectiveness are still unknown as the resolution is still in the early stages of implementation. **(Rosenthal)**

Current TFTP Debate

The current debate has several sides. The agreement, which was signed on June 24th, 2010 recognizes the program's success and usefulness to combating terrorism. However, the EU believes that un-monitored access to international monetary transactions by the US is unacceptable. Within the EU not all countries are willing to forgo their rights to privacy on international transactions. Additionally, they do not agree with the anonymous person appointment by the commission. While the reasoning for this was to address security concerns and attempt to limit the chance of political lobbying, many European politicians want the process to be transparent. The US has concerns with existence of this person at all and the anonymity that could potentially lead to much less cooperation on investigations. **(Rosenthal) (EurActiv) (Council of the European Union)**

Cyber Warfare

Offensive and defensive cyber warfare is a reality within governments around the world. Cyber warfare tactics have been employed in several recent conflicts, including the conflict between Russia and Georgia and is suspected to have had a role to play in the Israeli bombings of Syrian nuclear facilities. In February 2007, Estonia was hit by an elaborate DDOS attack originating from Russia and is suspected to have been a state sponsored action. Russia refused to cooperate with Estonia's formal diplomatic request to further investigate the source of the attack, even though Russia was bound by a standing

bilateral agreement. In 2008, as a response to this cyber attack, NATO opened a cyber defense center in Estonia. **(Cyber War)(Knake)**

One of the greatest challenges in cyber warfare is the sovereignty issue. "Speaking to the geography of cyberspace, the strategy implicitly acknowledges the sovereignty issue ("the lack of geopolitical boundaries…allows cyberspace operations to occur nearly anywhere")" **(Cyber War, Page 45)** There exists a focus on government networks with mostly a disregard for civilian systems and networks outside of critical infrastructure. The current main focus of cyber defense is on securing the .gov domain and all federal networks. Businesses and civilians are currently at high risk to cyber warfare attacks; however the federal government has no plan in place to focus on their protection. **(Cyber War)**

Attribution and cooperation are difficult since no government wishes to implicate themselves or their interests. "The attribution problem would persist, however, even in the case of an attack that has already taken place. Trace-back techniques and ISP records may indicate that a particular nation is involved, but they would not usually be able to prove a government's guilt with high confidence." **(Cyber War, Page 248)** There is no current incentive for non-parties of the Council of Europe treaty to police their own citizens. When running intelligence missions or attacks, governments can and have placed blame on patriotic citizens or hacktivists. There is no current legal framework in place to require countries, particularly ones not party to the Council of Europe, to actively seek out and stop citizens from attacking or committing crimes against people in other countries. **(Cyber War)**

Cyber Crime

Today the main agencies responsible for the investigation of cyber crime are the FBI and the Secret service. Additionally, the Immigration and Customs Enforcement and FTC participate when necessary. Most cyber crimes are not investigated since they usually fall below the $100,000 minimum necessary to authorize a federal case. “Today law enforcement in the U.S. does not begin to deter the world’s cyber criminals. Today cyber crime does pay. To make it stop paying, the U.S. would need to make a substantially greater investment in federal law enforcement agencies’ cyber crime capability. We will also have to do something about cyber crime sanctuaries**.” (Cyber War, page 267)** One of the rare diplomatic successes against cyber crime came in the late 1990’s when an order was sent from the major financial powers to the Prime Minister of the Bahamas to pass a law criminalizing money laundering or face a halt on all local currencies and financial transactions with their banks. This private action worked as crime was greatly reduced and the Bahamas was no longer considered a major sanctuary. This is an approach that the Cyber War author believes could and should be applied at the diplomatic level. **(Knake)**

The United States is falling behind international powers when it comes to guiding the development of Internet governance and infrastructure. Non-democratic nations such as Russia and China are using their influence to promote the use of national networks that are heavily controlled by the government. **(Knake)** Robert Knake suggests in his CFR report that the United States should hold countries accountable for cyber crime and attacks that originate within their borders, regardless if they are performed by citizens or

government. The US should also lead by example by investigating and prosecuting criminals that attack foreign victims. There is also a belief among experts that we should move on from the Council of Europe because it is too contentious for non-western nations to agree with. This could be done by establishing new international cybercrime organizations and developing real-time mechanisms for investigatory collaboration and enforcement. Leadership at the highest level in the United States is ultimately necessary in order to push forward these agendas.

"Cyber crime damage to the global economy is estimated at more than $1 trillion each year" **(Knake, loc 150)** Defense and reduction of cyber crime are crucial to the global economy, however some nations interests, such as China and Russia, are more about furthering state control than of protection. Knake fears that if these nondemocratic nations take control of the International development of the Internet that U.S. interests of freedom and democracy would be harmed. He believes that in order to avoid this outcome and keep the Internet as a, "mechanism for economic exchange and efficiency" that the U.S. needs to cooperate with the international system in order to influence other nations to move away from authoritarian approaches and to develop means by which cyber crime can be curbed.

On the Council of Europe Convention on Cyber Crime treaty, some experts believe that many countries will not ratify the treaty simply because it was developed under the Council of Europe. There is also the belief that the treaty does not reasonably do enough to reduce cross-border cyber crime. The treaty focused primarily on bilateral agreements for prosecuting criminals but had very little on coordination of efforts to stop

attacks as they occur and how to investigate them after. “The convention has served a purpose in laying out a legal framework for harmonizing national laws on cyber crime and for providing cross-border mutual assistance, by adding signatories to this particular document is neither necessary nor sufficient for reducing cross-border cyber criminal activity.” **(Knake)**

Knake mentions in his CFR report that there should be the creation of an intergovernmental body developed under the model of the Financial Action Task Force (FATF) in order to aid countries in the development of legal structures to investigate and fight cyber crime. He believes that these countries have an inherent motivation to comply with these structures since cyber criminals living in their country will not only target foreigners but local citizens as well.

Chapter 3

Analysis

Introduction

The data collection for this thesis consisted of ongoing interviews and consultations with leading authors and experts within the field of international cyber security. The three experts consulted included Robert Knake, Ed Gibson, and Don Shemanski. Since most of the approaches to solving the issues surrounding international cyber crime are still emerging and being developed, it was necessary to go to those who are helping to shape these policies or have had experience working with foreign governments on similar issues. The interviews were conducted via telephone, email, and in-person meetings throughout the course of the semester and past year. This included bi-weekly meetings with Don Shemanski and several correspondences with Robert Knake and Ed Gibson via telephone and email. The sensitive nature of their work does not allow me to quote them directly, however their contribution to this thesis has been paramount.

Robert Knake: Currently, Mr. Knake is Special Counselor for the National Protection and Programs Directorate of the Department of Homeland Security. Knake's most recent works related to this topic include co-authoring "Cyber War: The Next Threat To National Security and What To Do About It" and as an international affairs fellow at the Council on Foreign Relations wrote a special report "International Institutions and Global Governance Program." He holds a master's degree in

international security studies from Harvard University's Kennedy School of Government and has written on security issues for the Boston Herald, the San Antonio Express-News, and other publications.

Ed Gibson: Currently, Mr. Gibson is a Director in Forensic Technology Solutions for PricewaterhouseCoopers. He previously has held the positions of Chief Cyber Security Advisor for Microsoft Ltd – United Kingdom, Federal Bureau of Investigation Special Agent and U.S. Embassy-London FBI Assistant Legal Attaché, and Corporate Counsel for Amway Global. Gibson was inducted into the Infosecurity Europe "Hall of Fame", London in April 2010. He has contributed to many published works such as an editorial titled "The End" in SC Magazine and has participated in many live radio and television appearances about cyber crime and risk management. Along with his extensive professional work experience, Gibson holds many industry recognized certifications:

- CISSP (Certified Information Systems Security Professional)
- FBCS (Fellow, British Computer Society, United Kingdom), # 990186084
- Member: State Bar of Michigan, U.S. (Lawyer 1981 - Present), # P32485
- Member: Law Society of England & Wales (Solicitor 2003 - Present)
- FBI Certified International Instructor, White Collar Crime, 1999 - 2005
- FBI Certified Legal Advisor 1989 - 2005

Don Shemanski: Mr. Shemanski is currently a Professor of Practice in the College of IST at Penn State University. Shemanski previously served 23 years as a diplomat with the United States Foreign Service. Before joining IST, Shemanski served as Counselor for Global Affairs at the U.S. Embassy in Berlin. Along with other high-priority policy issues, he was responsible for counter-terrorism and international judicial assistance. "He has had a number of postings in Washington and abroad, including tours

in Italy, Pakistan, Cyprus, and Germany. His assignments have included serving as coordinator for State Department refugee assistance programs for the former Yugoslavia, delegate to the U.S. Delegation to the Vienna CSCE Follow-up Meeting, Deputy Special Envoy to the Afghan Mujahedin, and Alternate U.S. Delegate to the foundation, "Remembrance, Responsibility, and the Future," which administered payments to former World War II-era forced and slave laborers of the Nazi regime."**(IST)** Before his diplomatic work, Shemanski worked as an associate attorney for the international law firm Walter, Conston & Schurtman.

The Issue

Globalization, including the spread and reliance on the Internet throughout our world, has required governments to interact with each other on an unprecedented level. Rapid global adoption of Internet connected devices has raised many difficulties for applying nation state laws bound by traditional geographical boundaries to the internationally-connected Internet. Governments have been slow to adapt to the paradigm shift where anyone from anywhere can interact on nearly every medium of communication. Industrial markets, financials, global commerce and critical infrastructures rely on Internet connectivity and the means by which people use these technologies is changing faster than laws can keep up with. The emerging reality of state-sponsored cyber attacks, as seen in Russia's attacks on Georgia and the U.S. establishment of the United States Cyber Command in 2009, has further complicated the issues of international cooperation for prosecuting cyber criminals across borders. It is

the intention of this thesis to explain the issues surrounding international cooperation on cyber crime issues and outline potential solutions.

As a globally connected community, we now have to grapple with a number of issues that were unknown in the past. Cyber crime has emerged as a lucrative way for criminals to make money at a very low risk. Hackers can live within safe haven countries that have weak laws against cyber crime and that look the other way when they attack foreign entities. An individual's presence on the Internet in the age of cloud computing can mean he/she are everywhere but nowhere specific at the same time. Terrorists have taken to the Internet to further their reach in all parts of the world. They are seeking individuals susceptible to becoming radical and news ways to bolster financial support for their cause. While the freedom, connectivity, and openness provided by the Internet have brought many great things to our world, it is also necessary to recognize the issues that have arisen from this phenomenon. For instance, e-commerce has redefined the way the world does business in less than 15 years. While this has brought great benefits and increased revenue, it has also exposed consumers and businesses to a greater number of threats. According to Krebs and the FBI's published bank crime statistics, in the 3rd quarter of 2009 traditional bank robberies in the U.S. accounted for $9.4 million dollars. Comparatively, in the same quarter, online banking fraud involving the electronic transfer of funds accounted for $120 million dollars. This trend has been on the rise since 2007 and in many cases the federal government is powerless to stop it. **(Krebs)**

The Nigerian 419 Advance Fee Fraud scammers are an example of a long running and highly profitable fraud ring based out of Nigeria that has expanded in operation because of the advent of new technologies. First discovered during the 1970's, the

Nigerian 419 scammers have evolved from simple mail fraud to using modern technologies such as email, telephones, auction sites and even Internet gambling. One of their most common scams involves the sending of fraudulent emails meant to lure victims into sending or wiring money with a promise of higher returns. This has always been a lucrative business, but the use of the Internet has increased their target base and exponentially increased their profits. In 2009 alone the Nigerian 419 scammers stole an estimated $9.3 billion dollars. (Ultrascan Advanced Global Investigations) One of the main issues that we face is that the sheer volume of these crimes committed is impossible to keep up with. Government resources for prosecuting cyber crimes are sparse, especially when pursuing ones committed across borders. The lack of resources forces the investigators to only go after the biggest threats and by doing so allow most small cases to go unnoticed. The increasing number of individuals connected to the Internet has produced a situation where the most susceptible individuals are closer, in “virtual” terms, to criminals than ever before. Global connectivity provides motivated criminals with the ability to cast a wide net and have more targets. They can enjoy the comfort of anonymity and safety behind the obstacles to investigation and prosecution. As a global community we now face the challenge of strengthening cooperation in order to reduce the crime rate and pursue the offenders.

The Current Process

Failures of the Council of Europe

Currently international cooperation operates primarily under the Council of Europe Treaty on Cyber Crime and existing bilateral Mutual Legal Assistance Treaties. The Council of Europe Treaty is the only widely accepted agreement currently in place and is based on the Budapest Convention on Cyber Crime that has been signed or ratified by 46 countries since being drafted in 2001.

The Council of Europe Treaty has, unfortunately, been universally rejected outside of its current member and affiliated states. South America, Africa, developing nations and countries such as China and Russia have been adamant in this rejection. Russia continues to oppose the treaty, "The Budapest Convention sanctions police to cross national boundaries, without consent from local authorities, in order to access servers – with the caveat that the owners of the network systems give permission. Russia has opposed this measure since 2000 when police from the United States gained access to computers owned by Russian men accused of defrauding U.S. banks." (Masters) According to my sources many of the dissenting countries will not ratify the treaty since it was drafted and agreed upon by mostly Western countries aligned with Europe. This is simply because of traditional political tensions between them. They view the United States as an international bully with selfish interests. Furthermore, there are profound disagreements on the protection of intellectual property rights and how they should be handled across borders. There also exist significant differences in the direction these dissenting nations have taken in regards to control over Internet access within their

countries. China is the leader in state-controlled Internet access, having established ultimate authority over incoming and outgoing connections as well as which content can be viewed by citizens.

While many of the reasons behind the rejection of the treaty have little to do with the substance and more to do with the politics between nations, there also exists a lack of faith in the effectiveness of the treaty to accomplish its intended goal. My sources and I agree that there are major shortcomings in the process outlined by the Council of Europe. First and foremost there is no real punishment for not following the terms of the treaty for all parties involved. Secondly, the treaty is ineffective at requiring a reasonably prompt response to investigation requests. There exists an enormous gap between the speed with which a crime can be committed across borders over the web and the time it takes for a response by governing officials. Official correspondence between nations inquiring on cyber-related offenses tends to only go through one channel and not all countries have that point of contact available at all times.

One of the prime examples of the shortcomings of the Council of Europe Treaty failing is the Gary McKinnon case. Gary McKinnon is a Scottish hacker who publicly admitted to breaking into US Military networks and NASA. The alleged hacking occurred over a period of time between February 2001 and March 2002 and as a result of a criminal investigation into his activities, his computers were seized by British police in March of 2002. Since that time the McKinnon case has become largely a political matter, with McKinnon currently having been fighting extradition to this day. Even between two of the closest international allies extradition can be a lengthy, difficult, and complicated matter. Furthermore this case was considered to be very serious because it involved the

US Government. The lack of progress on such a high profile case gives little hope to smaller victims that seek justice.

Lastly, the experts have said that the Council of Europe Treaty only broadly gets into digital rights protection use and not at all into the illegal obtaining of intellectual property. One of the main obstacles to prosecuting cyber criminals is the differences in cyber laws that exist between nations and the lack of diplomatic discussions meant to come to an agreeable consensus with respect to those differences.

Law Enforcement Approach vs. Immediate Military Intervention

One key issue with respect to transnational cyber crime is whether or not it is acceptable to take immediate action against attackers as the attack is happening. Described during the literature review was the Law Enforcement Approach, where governments collect as much evidence as they can in order to trace the attack and inevitably must request the aid of a foreign government to continue the investigation. As the experts have pointed out this often leaves the trail cold when operating with outside parties of the Council of Europe. Even existing parties have a difficult time retaining evidence of attacks given the nature and speed in which cyber attacks and crimes can occur. This has cast doubt on the efficiency of a law enforcement approach.

The second emerging approach is the immediate military intervention approach. With this the US military would knock any server offline that is initiating an attack regardless of where the host server is located. This would help stop attacks early but is a very new and controversial idea. The problem with this approach is that it could be

viewed as an attack by a nation state onto another country even if intended as a form of "anticipatory self-defense." It also has the potential to destroy crucial evidence needed to defend the act. Destruction of evidence and diplomatic issues are not the only points of failure that threaten the adoption of this approach. One of the main issues that permeate throughout cyber crimes and attacks is that even though they may have the same effect as a physical attack, they lack the public perception as being one and the same. If a foreigner entered a country and stole money physically from a bank, there would be public outcry for the defense against that act or at least prosecution. When the same act occurs online it often goes unnoticed, is written off as a loss, and is seen as not worth pursuing.

Proposed Solutions

Regardless of a $1 trillion loss per year to global economies, there is still no solid direction towards curbing the accelerating rate of transnational cyber crime. Not only does this highlight that the significant issue has not been given enough public attention, but it also shows that current efforts up to this point have not worked.

Prosecution Issue

The Council of Europe Treaty has put forth a good set of guidelines for which countries can agree with respect to combating cyber crime and it has helped start an international dialog on the topic; however it does not go far enough in improving the

actual prosecution of these crimes. Furthermore, it is crucial to have the support of all countries not party to the treaty, including important players such as China and Russia. Aside from the issues within the document itself, it is seen as merely a gentlemen's agreement essentially lacking in legally enforceable commitments. This is where diplomacy must play a role in the process. In order to curb transnational cyber crime there must be incentives for countries to hold themselves accountable. Safe havens for cyber criminals should not get a free pass.

Political Issue

Part of this issue is simply political. The United States has had a difficult time tracking and prosecuting cyber criminals that exist within its own borders. Many criminals operate within the U.S. and target foreigners, but even a country with a well evolved domestic cyber crime process faces difficulties to success. Part of the reason nothing is done is because it would be very expensive and there is no current obligation to track and prosecute them. In the current political and budgetary climate, it would be very difficult for a politician to propose extensive spending increases to combat an intangible threat that most citizens do not perceive. While the outcome of increased spending on curbing transnational cybercrime could be very positive and profitable for the United States and others, it is no guarantee that money spent would solve the issues. The U.S. Federal Government has instead left the burden of responsibility on the private industry. While private industry has produced many great things, their ultimate goal is not on the protection of citizens. The government's current focus is on protection of

government networks first, critical infrastructure second, and citizen's computer systems and networks are not considered. It is because of this that the first important factor towards curbing cyber crime is public knowledge and support. Much of the crime that occurs is in very low amounts, which has allowed criminals to cast a wide net and avoid attracting too much attention. Larger scale individual crimes are rarer and usually involve a well resourced entity, like a financial institution, that has the ability to fight back.

Public Company Reporting

One step that could be taken in order to curb transnational cyber crime would be to require publicly owned organizations to report losses resulting from cyber related crimes or attacks. Currently, most organizations refuse to report such information to the police or public because it is seen as embarrassing or pointless. By requiring public organizations to report this information the public would be able to see the extent of the damage cyber related crimes cause. This could also act as an incentive for businesses to increase their security. This in turn could help bring awareness to the overall damage and potential damage cyber crime can inflict and may sway public opinion in favor of taking action against it.

Improve Points of Contact

There also needs to be a reworking of international agreements on cyber crime. It is imperative that cross-border cooperation for investigations improves. Aside from major

disagreements with countries like China, cross-border cooperation also often fails among even the closest allies. Many investigations go stale once handed from one country to the next and the resources appropriated to these points of contact are not sufficient.

Nation state sovereignty is the biggest point of contention among negotiations on transnational cyber crime. Many countries benefit from Internet connectivity but few feel it necessary to police their own citizens, including the United States. Even if the Council of Europe were to add more signatories and provide a framework for developing nations to apply cyber laws, this would do little to incentivize those countries to enforce the laws. The treaty has been in place for 10 years and transnational cyber crime has continued to increase. Regardless of its failures, it still could be a good starting point for improvements. The treaty should be amended to include requirements on increased cooperation and resources dedicated to responding to investigation requests.

Host Country Trial

There should also be included a new clause that states that if an investigation leads to the finding of criminal activity, that the offender will be tried in their host countries court system. Extradition has been proven to be an ineffective deterrent and highly resource intensive. By allowing criminals to be tried in their own countries more crimes can be responded to and there will be less political tension involved with extradition. While this may not be the most desirable for victims it is also the new reality. With the small number of crimes that have actually led to investigation even fewer have led to proper extradition. The first step is to agree with countries that have not ratified the

Council of Europe Treaty on what constitutes a cyber crime and the next should be to have the individual properly tried by the host country.

Leadership Support

Ultimately there needs to be support from leadership. It is impossible to push aside the profound issues that have arisen from the attempt to apply nation state laws to a realm that is supranational such as the Internet. While development of key technologies may have been born from the private sector, there is a duty of governments to protect their people. This has not and will never be the focus of the private sector. My sources believe this has become a largely diplomatic issue and if so it requires support from the highest offices of governments. The lack of agreement and effort towards international cooperation has been very costly. Leaders need to make the extent of damage known to their citizens and take proper steps in a movement resolve the issues.

Bibliography

CBS. Cyber War: Sabotaging the System. 8 November 2009. 1 February 2010 <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565_page3.shtml?tag=contentMain;contentBody>.

Clarke, Richard A and Robert K Knake. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins e-books, 2010.

Council of the European Union. Council Decision on the conclusion of the Agreement with the USA on TFTP. 24 June 2010. 30 September 2010 <http://register.consilium.europa.eu/pdf/en/10/st11/st11222-re01.en10.pdf>.

EurActiv. EU to launch anti-terror finance tracking plan. <http://www.euractiv.com/en/financial-services/eu-launch-anti-terror-finance-tracking-plan-news-376447>.

FinCEN. Resources for Victims. 2010. 30 September 2010 <http://www.fincen.gov/help4victims.html>.

Harley, Brian. A Global Convention on Cybercrime? March 23 2010. 8 September 2010 <http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/>.

IST. Faculty Bio: Don Shemanski. June 2008. 18 April 2011 <http://ist.psu.edu/ist/directory/faculty/?EmployeeID=527>.

Knake, Robert. "Internet Governance in an Age of Cyber Insecurity." Council Special Report No. 56. 2010.

Krebs, Brian. Cyber Crooks Leave Traditional Bank Robbers in the Dust. 9 March 2010. 30 March 2010 <http://www.krebsonsecurity.com/2010/03/cyber-crooks-leave-bank-robbers-in-the-dust/>.

Lewis, James. Securing Cyberspace for the 44th Presidency. December 2008. 26 November 2009 <http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf>.

Lichtblau, Eric and James Risen. "Bank Data Is Sifted by U.S. in Secret to Block Terror." 23 June 2006. The New York Times. 10 September 2010 <http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=1&_r=1&ei=5094&en=18f9ed2cf37511d5&hp&ex=1151121600&partner=homepage>.

Masters, Greg. Global cybercrime treaty rejected at U.N. -SC Magazine US. 23 April 2010. 8 December 2010 <http://www.scmagazineus.com/global-cybercrime-treaty-rejected-at-un/article/168630/>.

Megias, Alain. Cybercrime Investigation: Cybercops. 3 August 2010. 1 September 2010 <http://www.i-policy.org/2010/08/cybercrime-investigation-cybercops.html>.

Rosenthal, John. Terrorist Finance Tracking Program Re-Starts under Anonymous European Oversight. 20 September 2010. 30 September 2010 <http://www.weeklystandard.com/blogs/terrorist-finance-tracking-program-re-starts-under-anonymous-european-oversight?page=2>.

Secretariat, Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime. Online Document <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf>. Salvador, Brazil, 2010.

U.S. Department of the Treasury. Legal Authorities Underlying the Terrorist Finance Tracking Program. 21 September 2010 <http://www.ustreas.gov/press/releases/reports/legalauthoritiesoftftp.pdf>.

—. Terrorist Finance Tracking Program. 23 June 2006. 21 September 2010 <http://www.ustreas.gov/press/releases/js4340.htm>.

Ultrascan Advanced Global Investigations. 419_Advance_Fee_Fraud_Statistics_2009. 28 January 2010. 1 February 2010 <http://www.ultrascan-agi.com/public_html/html/pdf_files/419_Advance_Fee_Fraud_Statistics_2009.pdf>.

United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." 2002.

VITA

Andrew C. Clay

2015 Buttonwood Lane
Huntingdon Valley, PA 19006
clay.andrew@gmail.com

Education: Bachelor of Science Degree in Information Sciences and Technology, Penn State University, Spring 2011
Minor in Security and Risk Analysis
Honors in Information Sciences and Technology
Thesis Title: Obstacles in Prosecuting Transnational Cyber Criminals
Thesis Supervisor: Donald R. Shemanski

Related Experience:

IT/Project Manager for Cumberland Dairy
Supervisor: Carmine Catalana
Summer 2009, 2010

IT Manager for National Realty Corporation
Supervisor: Nicole Robinson
Summer 2008

Network Administrator for La Salle College High School
Supervisor: Peter Sigmund
2003-2007

Relevant Academic Work:

SRA 211 Threat of Terrorism and Crime

IST 445H Globalization Trends and World Issues: Included a trip to CSIS where we participated in current events lectures and a policy making scenario

HS/PO355 Perspectives on Northern Ireland: Lecture Series: Included an extensive dossier of students own research. Included meeting with former terrorists and politicians in interview settings.

HS/PO360 Northern Irish Troubles: 1969-1999

HS/PO365 Conflict Resolution: Comparative Case Studies and Approaches: Included studies of conflict resolution in the Northern Irish Conflict as well as the Palestinian Israeli Conflict.

Awards:

Dean’s List

Presentation/Activities:

Learning Assistant for IST 421: Advanced Enterprise Integration
Lived and studied abroad in Dublin, Ireland.