The Current State of Cybercrime in Thailand : Legal, Technological, and Economic Barriers to Effective Law Enforcement

Adam Ghazi-Tehrani
University of California, Irvine

ABSTRACT

For the past two decades the rates of online criminality have increased worldwide from year-to-year. Nevertheless, the majority of cybercrime scholarship relies on data collected from the English-speaking world, despite the fact that the majority of Internet users exist within Asia. As the populations of smaller countries in the region, in this case Thailand, become increasingly more active online, there may be barriers to effective law enforcement. This study shows that outdated laws, an understaffed and underfunded law enforcement, and new technology, provide for an over-stressed response. Using the United States of America as a point of comparison, as the number of users continues to grow; Thai law enforcement may be unable to keep up.

INTRODUCTION

The Internet was originally designed to be easily-accessible, open, and used as a tool for research. As web

traffic has shifted from academic purposes to commercial purposes, this openness has proven to be a "double-edged sword" (Liu, Hebenton, & Jou, 2013) with cybercrimes increasing year-to-year and results in worldwide losses numbering in the hundreds of billions of U.S. dollars each year (Nakashima & Peterson, 2014). The first-world has seen a rapid increase in information technology (IT) security services to attempt to provide unfettered business. However, a connected system cannot be completely secure as it relies on users being able to access it. As a result, financial frauds, identity theft, and other hacks have become commonplace (Holt & Bossler, 2008). Recent security breaches at major corporations such as Target (Riley, Elgin, Lawrence, & Matlack, 2014), Neiman Marcus (Zetter, 2014), and Home Depot (Lipka, 2014) have resulted in tens of millions of credit card numbers being stolen and used fraudulently.

Cybercrime is a growing problem, not only in the United States of America, where arguably the "best" security systems are in use, but worldwide in markets without massive IT-security budgets. As a relatively new field of criminology, cyber criminological research has frequently focused on areas where the most cybercrime occurs or where data is most easily available, usually limiting research to the US and other English-speaking countries. For example, Smith et al. (2011) present the most in-depth analysis of cyber-criminal law through a look at the trial and sentencing processes for cyber criminals, but limited their study to the US, Australia, New Zealand, the United Kingdom, and Canada.

Within the past ten years, research has finally begun to break into other emerging cybercrime hotspots, such as former U.S.S.R. satellite states and Asia, which is home to the vast majority of Internet users. In fact, when ranked by "online population," or Internet penetration rate (IPR), three of the top five countries are in Asia (China, India, and Japan) and the top country (China) has more than two times the Internet users of the second place country (the US) at roughly 568 million users to 254 million users (Internet Live Stats, 2014).

What is frequently lost in the literature, then, is research on less-accessible countries, such as those in the Association of Southeast Asian Nations (ASEAN) community, which are: Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. Broadhurst and Chang (2013) draw attention to the challenges that will face the region in the coming years, most notably an increasing online populace. Not only does Asia provide the majority of Internet users, but growth is explosive and will continue to increase. In 2002, for example, 3.5% of China's populace was online. In 2011, that number has jumped 10-fold to 36.3% of the population. There is similar growth in India (0.7% of population to 8.4%), Indonesia (1.8% to 16.1%), and Thailand (5.7% to 27.4%) (Internet Live Stats, 2014).

This study focuses on The Kingdom of Thailand and cybercrime in the unique Thai environment. Thailand experienced rapid economic growth from 1985 through 1996 and, amid constant political struggles, has emerged as a newly industrialized country focusing on manufacturing, agriculture, and tourism (Worldbank, 2014). Classified as a "middle power," Thailand is ranked second in quality of life among ASEAN nations (just behind Singapore) (Fisher, 2013). Thailand's Internet penetration rate (IPR) is currently around 27.4% and the country has invested heavily in providing a growing telecommunications infrastructure with high-speed 10Gbit/second fiber optic lines and 23,000 free public Wi-Fi hotspots nationwide (Fernquest, 2012). While Internet access itself is widely available, online content is censored by the Thai government. Websites that are deemed immoral are blocked nationwide at the ISP level; these include gambling, pornography, and websites critical of the Thai Royal Family (Doherty, 2010).

Though getting quantitative data is difficult, an internal report compiled by the High Tech Crime Unit in 2009 provides a glimpse into the state of cybercrime in Thailand (Prommajul, 2009). According to the Royal Thai Police, between 2006 and 2008, 467 cybercrimes were prosecuted and the majority of the offenses fell into three

categories: defamation, online fraud, and child pornography. Furthermore, the RTP categorize the crimes into three groups (using language directly borrowed from the 2001 Council of Europe's Convention on Cybercrime): (1) offenses against the confidentiality, integrity, and availability of computer data and systems; (2) computer-related forgery and computer-related fraud; and (3) content-related offenses (Prommajul, 2009). Though the first category has the potential for a high amount of damage, the report states the relative frequency of such crimes is quite low. The second category is "the most serious category in Thailand" with simple frauds occurring on a routine basis.

The goal of this study is to describe the current cybercrime landscape in Thailand in order to better understand the challenges facing countries other than the US, the commonwealth states, and Europe. Asia is already the most populous region online and is poised to continue to grow. Asian markets are known for intellectual property theft and other technological crimes, but there remains very little research on law enforcement efforts to combat these types of crime within the region.

▣ THEORY

Properly theorizing cybercrime has proven a difficult task. Most current scholarship has followed one of three popular paths, depending on the population being studied. The first type is one that compares cyber offenders to white-collar offenders based on structures of opportunity. This avenue uses the organizational advantage argument (Benson, Madensen, & Eck, 2009), alternative sanctions argument (Kahan & Posner, 1999), and system capacity argument (Pontell, 1982) to argue that cyber offenders exist within a system where they are given differential treatment (Kshetri, 2013b). Basically, the organizational structure of corporations provides a "shield" from prosecution, higher-class offenders are offered a wider range of available sanctions, and cybercrimes, similar to white-collar crimes (Benson et al., 2009), are difficult to prosecute due to their complexity, which "requires substantial amounts of investigative and

prosecutorial efforts" (Kshetri, 2013b). These three theories complement one another and provide a good argument as to why cyber offenders are seldom caught and punished.

The second type of scholarship compares cyber offenders to deviant subcultures based on learning theories. This scholarship argues that cyber offenses require a special type of expertise that is frequently "passed on" through online forums and chat rooms (Holt & Bossler, 2008; Holt, 2007). Early hacking, cracking, and phreaking began as the exploits and pastimes of a dedicated group of computer enthusiasts who would swap stories and techniques online.

As hacking moved from recreation to profit-seeking behavior, however, it is unclear whether these theories hold as much theoretical weight as they once did.

The final type of scholarship focuses not on the offenders, but on the computers and networks themselves borrowing from routine activity theory. This scholarship compares the physical hardware as targets akin to houses and networks like neighborhoods (Pratt, Holtfreter, & Reisig, 2010; Yar, 2005). Thus, these theories argue the solution to cybercrime is not within the psyche, attitudes, and motivations of the cybercriminal, but in the "target hardening" of the victim computers and networks.

It is unclear at this point which, if any, of these theoretical paths will prove most useful for studying Asian cybercrime. In fact, as Asia is such a large area with such diverse cultures, what is suitable in Thailand may not be suitable in Japan or China. In the meantime, comparing the growing rate of Internet usage and, subsequently, cybercrime of Thailand to the United States is beneficial. As the evidence below suggests, Thailand is experiencing cybercrimes similar to that of the United States fifteen or twenty years ago. For example, the two most common cybercrimes in Thailand are website defacement and small-scale fraud.

The United States hacking subculture grew from the earlier 1970s "phone phreak" movement in which curious individuals studied, explored, and manipulated national telecommunications systems. This

"explorer" mentality persisted as the first computer "hackers" were born in the early 1980s, which was eventually codified as the "hacker ethic" in Stephen Levy's "Hackers: Heroes of the Computer Revolution" (1984). Chief among these were: "1) Access to computers should be unlimited and total" and "2) All information should be free." Thus, the first wave of computer intrusions was motivated by curiosity, not economic interest and the cybercrimes of the time represent this: the majority of intrusions caused minimal damage and were typically done for the interest of learning or as a prank.

It was not until Internet access became widespread in the late-1990s and early-2000s that economic crimes became commonplace, such as eBay frauds. In the year 2000, 43.08% of the U.S. population was online and accounted for 29.65% of all web users. As the U.S. online population grew, so did online crime. The aforementioned Target, Neiman Marcus, and Home Depot hacks have become commonplace and represent multiple millions of dollars of fraud.

As technology in the U.S. has evolved, so have the crimes, while the law and law enforcement are frequently left behind. This study analyzes cybercrime in Thailand to describe the current landscape of Thai cybercrime and, using the United States for comparison, explains what the future may hold for Thailand.

▣ RESEARCH QUESTIONS

- What are the most common cyber offenses in Thailand?
- To what extent are Thai law enforcement agencies able to deal with cybercrime?
- How do legal, technological, and structural factors affect the ability of Thai law enforcement to solve cybercrimes?

▣ METHODOLOGY

There is a marked scarcity of data when it comes to cybercrime. This is due to a variety of factors. First, and most importantly, is the fact that a vast majority of cybercrime victims do not know they have been victimized.

For example, the typical victim of a computer virus is completely oblivious of an attack as viruses frequently appear transparently to the end user; the user might notice their computer running more slowly than usual, but the vast majority do not suspect attack and, thus, fail to report victimization. Second, companies, governments, and other cyber-security-conscious institutions are more likely to detect a "hack," but are unlikely to report it for a variety of reasons, including, but not limited to: a fear of lost profits, issues of national security, and risk of embarrassment. Third, while cybercrimes are occurring at an alarming rate, statistical data on cybercrime is not collected by most police agencies (in the U.S., Thailand, or otherwise) and is not included in the FBI's Uniform Crime Report or in the national crime data for any other country (as of October 2014).

Due to these issues, qualitative methods, through in-depth interviews and observations were deemed to be the most appropriate level of inquiry in this research design. The researcher spent three months in Bangkok, Thailand interviewing relevant government officials and agents at a variety of agencies in order to complete an accurate picture of "cybercrime in Thailand." The subjects of these interviews included six (6) personnel at the Ministry of Justice's Department of Special Investigation's (DSI) Bureau of Technology and Cyber Crime, four (4) personnel at the Ministry of Information and Communication Technology's (MICT) IT Crime Prevention and Suppression Bureau, and four (4) personnel at the Royal Thai Police's High Tech Crime Unit (HTCU), in addition to relevant interviews with one (1) official at the Anti-Money Laundering Office (AMLO) and with the director (1) of the Thai Center for Justice Statistics (CJS). Over three months, sixteen (16) one-to-three hour interviews were conducted for a total of approximately 32 hours of interviews with government workers ranging from the lowest (agent/investigator) to the highest (director) levels of the Thai government.

The interviews themselves were semi-structured and open-ended in an effort to allow subjects to freely express opinions on what is important to the subject without imposing

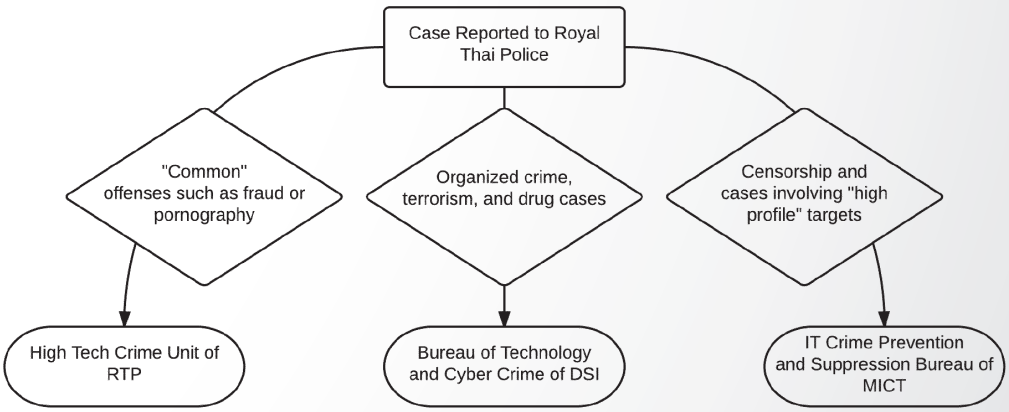
researcher judgments. One particular advantage of a qualitative design using open-ended questions is that subjects are more likely to explain detailed answers reliably. Four (4) interview subjects provided follow-up interviews and this process of multiple interviews ensured consistency and greater validity. Furthermore, consistent answers in repeated interviews with the same subject, as well as consistent answers across different interview subjects, indicates minimal interviewer bias effects. In addition, none of the four (4) interview subjects that supplied follow-up interviews gave contradictory or conflicting answers to previous interviews.

TYPICAL CASES

Cybercrime is a growing threat in Thailand, but it is not yet what one could call "common." In 2002, the Thai Ministry of Justice began tracking crime victimization through a national crime victimization survey (CVS) similar to the NCVS utilized in the US and other countries around the world. While the US NCVS is yearly, the Thai CVS occurs infrequently and has been conducted a few times: 2002, 2007, 2011 & 2013 (CJS Interview #1). The most recent (2013) Thai CVS surveyed 2,000 households for a total of 6,363 people. It found the four highest victimization rates to be: "crimes against persons" at 0.57%, "property crime" at 3.87%, "sexual crime" at 0.14%, and "fraud crimes" at 2.66% (CJS Interview #1).

The only cybercrime question in the Thai CVS concerns "cyber fraud," which is loosely defined as "online monetary frauds" such as fake eBay listings. In 2013, there were 18 victims of "cyber fraud" or a victimization rate of 0.28%. This is much less than the general "fraud crimes" at 2.66%, yet, according to all interviewed sources "cyber fraud" remains the most common cybercrime in Thailand. The other top crimes are: child pornography, "cyber extortion," website defacement, and "victimless crimes" such as accessing gambling and pornography websites (which are illegal and blocked in Thailand) (HTCU Interviews #1-3; MICT Interviews #1 & #2).

The cybercrime investigation process follows a simple hierarchical tree of law enforcement and, similar to street crimes, case investigation begins with the Royal Thai Police (RTP) , which gathers initial leads for a case. If the case involves fraud, pornography, extortion, or any other number of “common” offenses, but is conducted primarily through electronic means, the case is moved from the local police jurisdiction to the “High Tech Crime Unit” (HTCU) of the Royal Thai Police in Bangkok. If the case involves organized crime, terrorism, or drug offenses the case is moved to the Bureau of Technology and Cyber Crime of the Department of Special Investigations (DSI), also in Bangkok. The remaining cases involving censorship or certain high-profile people, such as the King or Prime Minister, may be handled by the IT Crime and Suppression Bureau of the Ministry of Information and Communication Technology (MICT) (see image #1).



It is important to note that the vast majority of cybercrime investigations in Thailand begin only after the victim reports the crime; there is no "active investigation" component within any of the three investigative units described above. The only cases that do not come from a victim's report instead come from other non-Thai investigative agencies; for example, the majority of child pornography investigations begin at the behest of the Federal Bureau of Investigations in the U.S. or from Interpol. In an effort to aid the general public in reporting crimes they've been a victim of, the HTCU has a website (http://www.hightechcrime.org/) where victims can report a crime and give as much relevant information as possible including the offender's phone number, LINE screen name (a popular social networking and messaging application in Asia), email address, and an in-depth description of the crime. In the first 8 months of 2014, over 60 crimes had been reported through this portal (HTCU Interview #3).

What follows are four example cases of the most common cyber-crimes in Thailand according to the interviewees. In some cases, the offender and victim names have been kept confidential and the dates supplied were only general. These omissions were due to the fact the victim or offender was under the age of 18 or because the case involved a high-profile individual that the law enforcement agency wished to protect and their removal should not affect the importance of the case.

▣ CHILD PORNOGRAPHY

Child pornography cases do not have a "victim" in the traditional sense: the abused child is most definitely a victim, but they are unlikely to be aware that pictures or videos of them have been posted and downloaded online and, unlike most other computer crimes, the victim is not the person using the computer unlike, for example, an eBay fraud victim. Since the Thai investigative agencies do not have agents actively monitoring the Internet for child pornography websites, they investigate when cases are reported via outside agencies (HTCU Interviews #1-3; MICT Interviews #1 & #2).

In late 2013, Interpol reported a child pornography website being operated within Thailand to the HTCU of the RTP. The agents had little to work with other than a Thai language URL that translated to "Schoolgirls' Pussy" in English. Using the online "whois" command, the HTCU discovered three important pieces of information: the offender's phone number, the offender's email address, and where the website was physically hosted. The phone number was to a prepaid mobile phone that provided no leads. The email address was likewise an untraceable freely created Gmail account, and the website was hosted by a company based in Hong Kong (HTCU Interview #3).

While the Gmail account was not directly linked to a name, the HTCU found that someone who had registered with this email address in an online discussion forum and that this user had provided a secondary email address belonging to a student at a Thai high school. Using this information, the HTCU found that this student was also the owner of the prepaid cellphone number discovered earlier. From start to finish the case took one agent approximately one month to solve, the majority of the time waiting for information from Google, Inc. regarding the Gmail account, the high school regarding the secondary email address, and the mobile phone company that sold the prepaid mobile phone.

With the offender properly identified, the case was handed to the local RTP jurisdiction where the student offender lived. Quickly thereafter the website went dark, but the student was never charged with a crime. Interestingly enough, it appears as if the student has used the funds he made from his illicit website to open a dumpling shop and was profiled in a Thai "young entrepreneur" magazine (HTCU Interview #3).

TWITTER HACK

Social network defacements are the most common non-profit-seeking cybercrime in Thailand and are very rarely investigated by law enforcement as victims usually report their victimization to Facebook, Twitter, or other social networking sites directly, instead. In early October 2011, however, one Twitter hack became national

news: the Twitter account of the (at the time) newly appointed Prime Minister, Yingluck Shinawatra, had been hacked. The hacker posted 8 tweets questioning the new PM's ability to govern, including: "This country is a business. We work for our allies, not for the Thai people. We work for those who support us, not those who differ with us," and "Where are the opportunities for the poor? We use them, give them hope for votes so our own group can benefit." The final hacked tweet mocked, "If she can't even protect her own Twitter account, how can she protect the country? Think about it" (Associated Press, 2011).

The culprit was caught quickly. Aekawit Thongdeeworakul, a 22 year-old architecture student, had made no effort to hide his Internet Protocol (IP) address when he accessed the PM's Twitter account. Twitter, Inc. and the student's Internet Service Provider (ISP) provided the MICT with all of the information needed to find the culprit and the student made an appearance alongside MICT Minister Anudith Nakornthap on October 5th, 3 days after the hack (BBC News, 2011). Mr. Aekawit was charged with "illegally accessing computer data" and faced a 2-year prison sentence if convicted. The case never made it to trial, however, as the student "seemed remorseful" and "was a good person at heart" according to the investigative agents who worked the case (MICT Interviews #1 & #2). Ultimately, the student was given a warning and was able to continue his studies.

▣ CYBER EXTORTION

Cyber extortion cases have become more popular around the world (Anderson, 2013) as the technology behind them has become more readily accessible. In Thailand, however, the cases remain decidedly low-tech. The HTCU revealed that during 2013 it had investigated four cyber extortion cases involving "important people" in Thailand (HTCU Interview #3). One such case began in March 2013. A senior executive at one of Thailand's major banks received a friend request from an attractive female on Facebook. The executive did not know the woman personally, but she was "Facebook

friends" with a number of his female friends. Over the next month, the executive and this woman began a flirtatious relationship. Eventually the woman asked the executive if he had Skype and a webcam on his computer.

The two swapped contact information and the messaging became a daily practice eventually culminating in a number of lewd video chat interactions. After one particular session, the "woman" revealed she was recording their interactions and demanded 20,000 USD to prevent the recordings being posted on YouTube. The executive immediately contacted the Royal Thai Police who put him in contact with the HTCU. Using a program called "Wireshark" to monitor their web traffic, the HTCU contacted the woman-turned-extortionist via Skype pretending to be executive-turned-victim. Wireshark is a "network protocol analyzer" and, through this monitored conversation, the HTCU was able to discover the offender's IP address, which lead to the suspect's name and physical address. The offender was actually male and had been using video recordings to pretend to be female. While this was his first attempt at extortion, the RTP described the practice as increasingly common. They believe most victims simply pay because they don't want to risk the negative publicity or the chance that their families might find out (HTCU Interview #3). The lead investigator describes the extent of the effort behind the extortion:

> The hacker was patient and smart. He knew that the target would be cautious and that is why he began with the target's friends. He spent months talking to these women first because it is easier for a woman to trust another woman. He talked to them about many different things until they were friends. Only after this did he attempt to contact [the victim] and the Facebook profile now appeared real with many posts from people [the victim] knew well. If he had been successful, the amount of work would have been worth it (HTCU Interview #3).

EFRAUDS

The most common type of cybercrime in Thailand is eFraud, cases where goods and services purchased online are never delivered. These cases share a number of similarities:

> The victim can be buying nearly anything. Fraud for big items, like televisions exist, but people are careful when they spend so much. The majority of the cases are for smaller things such as mobile phone minutes or toys. The payer sends the money and never gets the item. Or someone will make many listings on an online auction for the same item, so they can raise the price. Sometimes they make many listings and sell the item once for real and a few more times fake. Since they have the item, they can take pictures of it for proof if a customer asks. We have a website that explains how to buy things online, but these fraud cases remain common (HTCU Interview #4).

LEGAL, TECHNOLOGICAL, AND ENFORCEMENT ISSUES CYBERCRIME LAW IN THAILAND

Though cybercrime offenses were occurring throughout the 1980s and 1990s, national and international governments found themselves constantly playing "catch up" as current legislation proved inadequate for these "new" crimes. Perhaps the primary example of this trend was the response to the "ILOVEYOU" computer worm released on May 5th, 2000 (Seltzer, 2010). The worm spread rapidly through email, infecting computers in Hong Kong, Europe, and the U.S. in less than 24 hours and ultimately causing between $5.5 and $8.7 billion (USD) in damages. The worm was traced to two Filipino computer programmers, Reonel Ramones and Onel de Guzman, but, since there were no laws against writing malware in the Philippines, all charges were dropped (Seltzer, 2010).

While not drafted directly in response to the ILOVEYOU worm, the Council of Europe's (CoE) 2001 adoption of the "Convention on

Cybercrime" (CoC), or Budapest Convention, was an attempt to address growing cybercrime issues, specifically, harmonizing national laws, improving investigation techniques, and increasing cooperation among nations (Weber, 2003). "The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security" (Council of Europe, 2001).

The Kingdom of Thailand is not a member of the CoE and did not sign on to the convention as a non-member (though other nations such as the U.S., Japan, and Philippines have); instead the Thai government chose to borrow heavily from the convention when drafting its own "Computer-Related Crime Act" of B.E. 2550 (2007). The Thai law consists of two parts: Chapter One describes punishable offenses, including "hacking, unauthorized access, distributed denial of service (DDoS), viruses/worms, website defacement, Internet fraud, identity theft, forgery, blackmail, gambling, and pornography" (Thai National Legislative Assembly, 2007). Chapter Two describes "criminal procedure" including how computer offenses should be investigated, who should investigate them, and lays out a variety of operating procedures for computer-related industries, most importantly, a requirement that Internet Service Providers (ISPs) collect and store a 90-day log of Internet Protocol (IP) addresses of its subscribers (Thai National Legislative Assembly, 2007).

While the use of the CoC as the basis for Thailand's Computer-Related Crime Act (CRCA) was a large step forward in securing the Internet in Thailand, there remain two large problems that Thailand, and the East in general, face: (1) the speed at which the Internet and, subsequently, its crimes evolve and (2) an ever-widening "digital gap" between the East and West.

The first issue is apparent when considering the digital "cloud," for example. At the time of the CoC's inception in 2001, most data was

stored either on the user's personal computer and attached hard drives or remotely on a specific server. With the advent of smart phones, wide-spread broadband access, and other recent technological advancements, data is increasingly stored in the figurative ethereal "cloud" that spans various servers across the world. This concept of the "cloud" is not included in the CoC and accessing this data in the course of a modern investigation may result in international legal disputes. This demonstrates that the law is already one step "behind" the technology it is attempting to regulate, a problem for Thailand and the world. The second issue is more relevant to Thailand directly. As the U.S. and other Western nations quickly advance in information communication technology (ICT), some Eastern governments state dissatisfaction with the Western "monopolization of ICT products" which increases "less developed countries' dependence on the West" (Kshetri, 2013a). In 2008, the Shanghai Cooperation Organization (SCO), which includes primarily China and Russia, as well as Thailand through ASEAN's "guest attendance," spoke to this issue directly describing the West's preference for informational "freedom" over "control." In Thailand, online gambling and accessing pornography are deemed immoral and are censored nationwide. Likewise, websites critical of the royal family are blocked and their operators are subject to criminal charges. Western technologies used to circumvent precisely this type of censorship are widely available and protected by the laws of countries such as the U.S. and Australia, which Thai government officials argue weakens Thailand's ability to enforce their own laws (Fox & Carbone, 2014).

In sum, national and international law are frequently "behind" when it comes to regulating technology and Thai law, specifically, is difficult to enforce in an online environment where the infrastructure is controlled by non-Thai governments and their more liberal statutes.

▣ EMONEY

Thailand made international news in late July 2013 when the Thai central bank, Bank of Thailand, announced that Bitcoins were illegal

in the Kingdom of Thailand (Watts, 2013). The Bitcoin ban is just one case in the increasingly complex system of unofficial currencies currently available within Thailand. Since mid-2009, three major "eMoney" systems have arisen in Thailand: True Money, Advanced Info Service's (AIS) mPay, and Total Access Communication's (DTAC) PaysBuy (Pornwasin, 2014). TrueMoney is the largest service with 6 million registered users and while eMoney currently only makes up 5% of Thailand's overall revenue stream, True Corporation expects to see 15% growth in its particular system alone in 2014 (Pornwasin, 2014).

The process of turning Thai currency (baht) into eMoney is simple. TrueMoney, owned by True Corporation, Thailand's largest media conglomerate (the company owns Thailand's largest cable provider, largest Internet Service Provider, and third largest mobile operator), is available at every one of 7-Eleven's 7,651 nationwide stores (as of 2013) (CPall, 2014). The customer simply picks an amount in 100, 500, 1000, 2000 baht denominations, pays with cash, debit, or credit card, and is handed a receipt with a redeemable code. This code can be used to purchase anything from cellphone bills to online gaming "top ups" (Pornwasin, 2014) and, increasingly, child pornography:

> This website looks like it sells ringtones and stickers for Line. The Thai translates to "Super Shop." But if we pick a sticker… see now? If you scroll down past the sticker you see the pictures of the child pornography. This one is two baht. This is smart because that is how much a sticker would usually cost. One or two baht. When you first look at the site the prices and the products seem innocent, but what is really there is you pay for porn. Porn with children. And they only accept eMoney. This site is not hosted in Thailand, but the titles are in Thai and the way you pay is with Thai eMoney. We are attempting to shut this site down now, but it is difficult (HTCU Interview #4).

If the customer purchases eMoney with cash, the resulting eMoney becomes effectively untraceable and, because of this, these alternative currencies have become the preferred choice for Thailand's growing population of Internet criminals. Child pornography websites in Thailand are increasingly using eMoney to collect payment from their purveyors (HTCU Interviews #3 & #4). While the problem remains small at the moment, as mentioned above, eMoney only accounts for 5% of Thailand's overall revenue stream; the explosion of prepaid mobile phone use in Thailand serves as a possible sign of things to come.

PREPAID MOBILE PHONES

Introduced in Portugal in 1995, prepaid mobile phones served to solve a problem with mobile phone customers: since mobile phone operators charged their customers on a "postpaid" basis, the companies were missing out on a large part of potential customers: customers with poor credit ratings (Portugal Telecom, 2014). Prepaid mobile phones were able to fix this problem by allowing those with poor credit ratings to pay before using their phone, though usually for slightly higher per-call and per-text premiums.

These prepaid phones are available with no contract and very few countries require the phones to be registered to customers for use (the countries with this requirement are mainly countries within the European Union). Due to this, the phones have become popular with criminals as they are both cheap to acquire and allow the caller to remain anonymous. In the United States, prepaid phones have become colloquially known as "burners" that can be used for an illicit function and quickly discarded or "burned." While these phones are preferred by criminals, their overall use in the United States remains low at around 23% (as of 2011) (Chen, 2012). In stark contrast, prepaid mobile phones make up over 90% of the market in both Thailand and the greater Asian area (Farivar, 2012).

In the past, the widespread use would have simply meant investigations into street crimes would have had one less piece of evidence: a phone number. As mobile phones become more and more akin to miniature personal computers, however, cybercrimes are being committed via these untraceable phones. These "burner" mobile phones allow for cybercrimes to be committed in a similar manner to that of stolen cars providing difficult-to-trace getaway vehicles.

Since 2010, the number of Thai mobile subscribers has exceeded the country's population at 106.6% (Sakawee, 2013). As of mid-2013, there were approximately 90 million cell numbers in operation for approximately 69 million people. An officer explained:

> The phones are just too cheap. I have one phone for phone calls and another for texting. The texting phone was my primary phone, but I got the newer phone with a deal on minutes and the earlier phone had a deal on texts. It is cheaper for me this way. An offender might have a second phone for crime or might just have a second phone already. It makes finding them more difficult (HTCU Interview #2).

INTERNET PENETRATION RATE

The "Internet penetration rate" (IPR) is the percentage of a population with Internet access. China, the US, and India are the top three countries in overall Internet users, but are 102nd, 28th, and 164th in Internet penetration rates, respectively (Internet Live Stats, 2014). While the countries with the highest IPRs (Falkland Islands, Iceland, and Norway) are not known to be hotbeds of cyber-criminal activity, they are not hotbeds for street crime, either. Generally, the more people online the more cybercrime that occur because, simply put: a larger pool of potential offenders and a larger pool of potential victims results in more crime.

Thailand is currently ranked 132nd in the world with 17.7 million Internet users or an IPR of 27.4%. As mentioned in the Methodology section of this study, the main cybercrime investigative authorities are the Ministry of Justice's Department of Special Investigation's (DSI) Bureau of Technology and Cyber Crime (BTCC), the Ministry of Information and Communication Technology's (MICT) IT Crime Prevention and Suppression Bureau, and the Royal Thai Police's High Tech Crime Unit (HTCU). The DSI's BTCC has a 12-person staff, MICT has a 6-person staff, and the RTP's HTCU also has a 6-person staff. As of 2014, Thailand has 24 people devoted to not only solving all domestic cybercrimes, but to assist in international investigations as well.

At Thailand's current "low" IPR of 27.4%, the organizations tasked with solving cybercrimes in Thailand have already hit system capacity:

> We simply do not have enough staff to solve all of the crimes that are reported. The new website was developed to make reporting crimes easier for the public, but, for us, it serves as a method of triage. When we look for a new case, we look to see if there are any cases that appear to have a common offender. We look at phone numbers, emails, and Line IDs. If there does not appear to be a repeat offender, we simply pick the case with the largest dollar[1] amount. Sometimes these cases are more than ninety days old and become nearly impossible to solve (HTCU Interview #1).

Most interviewees agreed that the average case takes approximately one month to solve. As investigators accumulate a backlog of cases they

[1] *Cases on the HTCU website can be reported in either Thai Baht or U.S. Dollar. The majority of reported "eFraud" and cyber extortion cases are reported in U.S.D.*

run into the 90-day legal limit on connection logs stored by Thai ISPs as set by the Computer-Related Crime Act of 2007. Without growing staff sizes to counteract the increasing Internet Penetration Rate, it is unclear how much longer law enforcement can continue to be effective:

> We do not actively seek cases. There are not enough people to. Gambling sites and pornography are widespread, but we have been forced to consider them victimless crimes. Without a large enough staff to solve all the reported frauds already, I cannot hope to begin to stop online gambling. And I do not think the public would want us to (HTCU Interview #2).

Perhaps the most chilling of all, "Child pornography is a very large problem and the user is not the victim, but the offender. We try to solve all the cases referred to us by INTERPOL or the FBI, but since they're not reported like stalking or website defacement, the majority of it, I think, continues easily" (HTCU Interview #1).

HARDWARE AND SOFTWARE

While law enforcement staffing has hit system capacity, it is also clear that the various agencies have also hit some technological roadblocks as well:

> In order to follow the law and maintain proper [evidential procedure], the technicians make block-to-block copies of the offender's hard drive. That way we can have a copy for use in court and they get their computer back. We do not have the ability to look inside encrypted hard drives… this is also a problem with newer phones, too. This software is old and cannot access the data in many new phones. Like the iPhone 5S or new Samsung Galaxy. We cannot afford the new software. It costs many thousands of dollars (MICT Interview #3).

The DSI and HTCU explained that they both had updated software and could access these newer phones, but that they, too, were months-late in updating. While certainly a problem, it might not be as large an issue as it sounds:

> Most of the crimes in Thailand, crimes online, are for money. The people with the newest iPhone are usually not the ones who are committing these crimes. I, obviously, would like to be able to get into every phone collected, but, so far, even if my tech cannot get into a phone, there is more than enough evidence on the laptop or something else. Most people do not think they will get caught and do not try to hide much (DSI Interview #6).

DISCUSSION

This research demonstrates that much can be learned by studying cybercrime outside the traditional theater of the English-speaking world. While this is an introductory study, many conclusions can already be drawn. First, profit appears to be the preliminary motivator for Thai cybercriminals, but the scale of such crimes is on a much lower level than in more developed countries. Stories of millions of credit card credentials being stolen in the U.S. have become commonplace, whereas relatively "simple" eFraud reigns supreme in Thailand. Thai cybercriminals skew toward a younger and male-dominated demographic, which is similar to the West, though the response by law enforcement seems to differ at least anecdotally. For example, the "Twitter hack" of the Thai Prime Minister shares many qualities with the "email hack" of the Vice Presidential Candidate Sarah Palin in the U.S. (Zetter, 2010). While both cases involved prominent political figures, an online communication service being hacked, and young, male college-enrolled offenders, the Thai offender was released after making a public apology while the American offender spent one year in prison (Zetter, 2010).

Theoretically, this study suggests that system capacity issues will be the most significant problem facing law

enforcement in Thailand. Multiple factors contribute to this beyond the standard staffing and monetary issues present for most law enforcement agencies worldwide. First is the unique mobile phone market in Thailand. The sheer number of phones, more than one per person, and the fact that many of these phones are prepaid makes using mobile phone numbers much more difficult to find cybercriminals. The added layer of untraceable eMoney systems combines to a nearly "perfect" environment for aspiring cybercriminals. While the DSI, MICT, and HTCU are still solving cases around the clock, every interviewee admitted that the majority of the solved cases involve offenders that were not entirely careful. A determined offender could easily slip through the cracks by fully utilizing the crime-promoting technology available in Thailand.

The financial and technological issues facing Thai law enforcement compound into a pro-crime environment that is further enhanced via a legal framework that appears outdated and strained. The 90 day log limit, while arguably a positive thing for privacy advocates and the Thai public in general, results in an artificial timeline for law enforcement where a cyber-offender does not have to become completely untraceable online, simply difficult enough to take longer than 90 days to catch.

Compared to the U.S., Thailand is still in "cybercrime infancy" where the most frequent online crimes are small-scale and usually involve a handful of victims. While the Thai economy will remain a fraction of the U.S. economy and thus a less desirable target for the "mass hacks" of larger retailers, it is not implausible to say that if such a hack did occur, the law enforcement agencies in Thailand would be beyond strained to solve the case. As the IPR of Thailand increases, so will the cybercrime rate and, unlike the U.S. during its "cybercrime infancy" period, the technology of the mid-2010s is much more advanced than the technology of the mid-1990s.

Future research may focus on specific areas of cybercrime within the ASEAN community, for example, the online habits and usage patterns of Thai cybercriminals. This introductory study has not unearthed enough information to determine which

theoretical backgrounds are applicable, though evidence of system capacity abounds. Limitations of the current research design include an over-reliance on interview (qualitative) data and language barriers that may make some of the precise and technical language become lost in translation.

Reference

Anderson, N. (2013, March 11). Meet the men who spy on women through their webcams. Retrieved September 15, 2014, from http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/

Associated Press. (2011, October 2). Thai prime minister's Twitter feed hacked to produce mocking messages. Retrieved September 10, 2014, from http://www.theguardian.com/world/2011/oct/02/thai-prime-minister-twitter-hacked

BBC News. (2011, October 5). Arrest over Thai PM Yingluck Shinawatra's Twitter hack. Retrieved September 10, 2014, from http://www.bbc.com/news/world-asia pacific-15185082

Benson, M. L., Madensen, T. D., & Eck, J. E. (2009). White-Collar Crime from an Opportunity Perspective. In S. S. Simpson & D. Weisburd (Eds.), The Criminology of White-Collar Crime (pp. 175–193). New York, NY: Springer New York. Retrieved from http://link.springer.com/10.1007/978-0-387-09502-8_9

Chen, B. (2012, August 2). Prepaid Cellphones Are Cheaper. Why Aren't They Popular? Retrieved September 4, 2014, from http://bits.blogs.nytimes.com/2012/08/02/prepaid-phone-plans/

Council of Europe. (2001, November 23). Convention on Cybercrime. Retrieved from http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm

CPall. (2014). CP ALL PUBLIC COMPANY LIMITED - Home. Retrieved September 4, 2014, from http://www.cpall.co.th/Home#csr-news

Doherty, B. (2010, October 21). Silence of the dissenters: How south-east Asia keeps web users in line. The Guardian. Retrieved from http://www.theguardian.com/technology/2010/oct/21/internet-web-censorship-asia

Farivar, C. (2012, June 15). Die, contracts! Prepaid mobile phone use surges. Retrieved September 4, 2014, from http://arstechnica.com/business/2012/06/prepaid-mobile-phone-users-in-america-hit-record-high/

Fernquest, J. (2012, May 2). Bangkok's free internet: 23,000 hotspots. Bangkok Post. Retrieved from http://www.bangkokpost.com/learning/learning-from-news/291478/bangkok-free-internet-23000-hotspots

Fisher, M. (2013, November 5). Want to move abroad? This map shows the best and worst countries to be an expatriate. The Washington Post. Retrieved from http://www.washingtonpost.com/blogs/worldviews/wp/2013/11/05/want-to-move-abroad-this-map-shows-the-best-and-worst-countries-to-be-an-expatriate/

Fox, J., & Carbone, M. (2014, June 17). Flying the coup: Circumventing censorship in Thailand [Blog]. Retrieved from https://www.accessnow.org/blog/2014/06/17flying-the-coup-circumventing-censorship-in-thailand

Holt, T. J. (2007). subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. Deviant Behavior, 28(2), 171–198. doi:10.1080/01639620601131065

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. Deviant Behavior, 30(1), 1–25. doi:10.1080/01639620701876577

Internet Live Stats. (2014). Internet Users by Country (2014). Retrieved from http://www.internetlivestats.com/internet-users-by-country/

Kahan, D. M., & Posner, E. A. (1999). Shaming White-Collar Criminals: A Proposal for Reform of the Federal Sentencing Guidelines*. The Journal of Law and Economics, 42(s1), 365–392. doi:10.1086/467429

Kshetri, N. (2013a). Cybercrime and cybersecurity in the Global South. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan.

Kshetri, N. (2013b). Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. Crime, Law and Social Change, 60(1), 39–65. doi:10.1007/s10611-013-9431-4

Levy, S. (1984). Hackers: heroes of the computer revolution (1st ed.). Garden City, N.Y: Anchor Press/Doubleday.

Lipka, M. (2014, September 18). 56 million accounts at risk in Home Depot hack. CBS. Retrieved from http://www.cbsnews.com/news/56-million-accounts-at-risk-in-home-depot-hack/

Liu, J., Hebenton, B., & Jou, S. (Eds.). (2013). Handbook of Asian Criminology. New York, NY: Springer New York. Retrieved from http://link.springer.com/10.1007/978-1-4614-5218-8

Nakashima, E., & Peterson, A. (2014, June 9). Report: Cybercrime and espionage costs $445 billion annually. The Washington Post. Retrieved from http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html

Pontell, H. N. (1982). System Capacity and Criminal Justice: Theoretical and Substantive Considerations. In H. E. Pepinsky (Ed.), Rethinking criminology (pp. 131–143). Beverly Hills: Sage.

Pornwasin, A. (2014, March 6). E-wallet key service as True Money eyes 15% growth. Retrieved September 4, 2014, from http://www.nationmultimedia.com/business/E-wallet-key-service-as-True-Money-eyes-15-growth-30228473.html

Portugal Telecom. (2014). General FAQ's. Retrieved September 4, 2014, from http://www.telecom.pt/InternetResource/PTSite/UK/Canais/Investidores/FAQS/Gerais/

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. Journal of Research in Crime and Delinquency, 47(3), 267–296. doi:10.1177/0022427810365903

Prommajul, S. (2009). The Criminal Justice Response to Cybercrime: Thailand (pp. 87–97). High Tech Crime Unit, Royal Thai Police. Retrieved from www.unafei.or.jp/english/pdf/RS_No79/No79_13PA_Prommajul.pdf

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014, March 13). Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. Businessweek. Retrieved from http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Sakawee, S. (2013, August 16). Thailand internet report: mobile penetration has exceeded its population. Retrieved September 22, 2014, from http://www.techinasia.com/thailand-internet-report/

Seltzer, L. (2010, April 28). "I Love You" Virus Turns Ten: What Have We Learned? PC Magazine. Retrieved from http://www.pcmag.com/article2/0,2817,2363172,00.asp

Smith, R. G., Grabosky, P. N., & Urbas. (2011). Cyber criminals on trial. Cambridge: Cambridge Univ Press.

Thai National Legislative Assembly. (2007, July 18). Computer Related Crime Act of B.E. 2550. Retrieved from http://www.prachatai.com/english/node/117

Watts, J. (2013, July 30). Thailand's Bitcoin ban is not quite what it seems. Retrieved September 4, 2014, from http://qz.com/110164

Weber, A. (2003). The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal, 18(1), 425–446.

Worldbank. (2014). Thailand Overview. Retrieved from http://www.worldbank.org/en/country/thailand/overview

Yar, M. (2005). The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407–427. doi:10.1177/ 147737080556056

Zetter, K. (2010, November 12). Sarah Palin E-mail Hacker Sentenced to 1 Year in Custody. Wired. Retrieved from http://www.wired.com/2010/11/palin-hacker-sentenced/

Zetter, K. (2014, January 24). Neiman Marcus: 1.1 Million Credit Cards Exposed in Three-Month Hack. Wired. Retrieved from http://www.wired.com/2014/01/neiman-marcus-hack/