Spring 2016

Law Enforcements' Perceptions and Preparedness to Address Child Exploitation Via Hacking

Jack W. Lightfoot
Georgia Southern University

Recommended Citation

Binford, W. (2015). A Global Survey of Country Efforts to Ensure Compensation for Child Pornography Victims. Ohio State Journal Of Criminal Law, 13(1), 37-65. Botelho, G. (2013, September 27). Arrest in 'sextortion' case involving Miss Teen USA Cassidy Wolf - CNN.com. Retrieved November 8, 2015, from http://www.cnn.com/2013/09/26/justice/miss-teen-usa-sextortion/ CBS news. (2015, April 23). Baby monitor hacker delivers creepy message to child. Retrieved December 2, 2015, from http://www.cbsnews.com/news/baby-monitor-hacker-delivers-creepy-message-to-child/ CBS New York. (2015, April 21). Seen At 11: Cyber Spies Could Target Your Child Through A Baby Monitor. Retrieved January 07, 2016, from http://newyork.cbslocal.com/2015/04/21/seen-at-11-cyber-spies-could-target-your-child-through-a-baby-monitor/ Crewdson, J. (1998). By Silence Betrayed: Sexual Abuse of Children in America. Boston: Little Brown. Department of Justice. (2015a, June 3). Child Pornography. Retrieved January 10, 2016, from https://www.justice.gov/criminal-ceos/child-pornography Department of Justice. (2015b, July 6). Citizen's Guide To U.S. Federal Law On Child Pornography. Retrieved January 09, 2016, from https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography Department of Justice, Homeland Security Announce Child Pornography File-Sharing Crackdown: Law Enforcement Initiative Targets Child Pornography Over Peer-to-Peer Networks. (2004). Epiphaniou, G., French, T., & Maple, C. (2014). The DarkWeb: Cyber-Security Intelligence Gathering Opportunities, Risks and Rewards. Journal Of Computing

LAW ENFORCEMENTS' PERCEPTIONS AND PREPAREDNESS TO ADDRESS CHILD EXPLOITATION VIA HACKING

by

JACK WILSON LIGHTFOOT

(Under the Direction of Adam Bossler)

ABSTRACT

Throughout recorded history, children have been subjected to sexual exploitation. Child predators and pedophiles often take great risk and go to extreme lengths to sexually exploit a child. With technological advancements many individuals became globalized and connected with the invention of the computer, the Internet and its attributes. However, child predators quickly took note of the vulnerability of children as they began to groom them online. The problem quickly evolved as the Deep (Dark) Web and encryption were created. This put great stress upon law enforcement entities as locating and combating these predators became exhausting tasks. It's most often that these predators evolve quicker than law enforcement. Most recently, the use of hacking has become a successful tool in a child predator's arsenal. To better understand this new phenomena, this study will focus on interviewing local, state, and federal law enforcement agents on detection, combating, prevention and direction of this problem. The results suggests that child predator hacking is a very rare crime. In fact, only one of the five agents interviewed for this study had experienced child predator hacking. Instead, child predators use easier techniques such as grooming and manipulation as children are naïve and are consensually giving the child predators explicit material. However, there is still a possibility that child predator hackers were successfully able to blackmail the child and the crime will go unreported.

INDEX WORDS: Predators, Pedophiles, Child Predators, Hackers, Hacking, Webcam, Internet Crimes Against Children (ICAC), Child Exploitation, Child Pornography, Blackmail, Deep Web, Tor, Encryption

LAW ENFORCEMENTS' PERCEPTIONS AND PREPAREDNESS TO ADDRESS CHILD EXPLOITATION VIA HACKING

by

JACK WILSON LIGHTFOOT

B.S., Georgia Southern University, 2014

A thesis submitted to the Graduate Faculty of Georgia Southern University in partial fulfillment of the requirements for the degree

MASTERS OF ARTS

STATESBORO, GEORGIA

LAW ENFORCEMENTS' PERCEPTIONS AND PREPAREDNESS TO ADDRESS CHILD EXPLOITATION VIA HACKING

by

JACK WILSON LIGHTFOOT

Major Professor: Adam Bossler

Committee: Laurie Gould

John Brent

Electronic Version Approved

May 2016

ACKNOWLEDGEMENT

I would like to thank Dr. Adam Bossler, Dr. Laurie Gould, and Dr. John Brent for all of their support throughout this paper.

TABLE OF CONTENTS

Page

CHAPTER 1

INTRODUCTION

The purpose of this study is to better understand child exploitation through the hacking of webcams. Child exploitation through cyberspace has become problematic for law enforcement due to its unregulated nature. This has allowed child pornography to become one of the fastest growing cyber markets which is believed to continue to grow exponentially. As of 2009, the child pornography market is a twenty billion dollar industry (ICMEC, 2006; Edelmann, 2010 & M'jid, 2009 as cited in Binford, 2015). The Internet and its many tools provide a safe and efficient venue for pedophiles and child exploiters to discuss, share, and download child pornography. Additionally, this is the easiest and most effective way for child predators to prey on children. It's no secret that children are vulnerable and naïve within the cyberspace. The cyberspace creates an environment of anonymity and security, a space where adults and/or guardians are often not present, thereby creating the perfect storm. Child predators groom children online by posing as other children and/or other individuals and promise friendship and gifts in an attempt to sexually exploit the child. However, law enforcement quickly noticed this practice and began to combat the matter. Child predators quickly evolved and are able to deceive law enforcement once more. These predators have discovered that children can easily be exploited through the webcam without one's knowledge or consent. This new method of exploitation is achieved through hacking (Muller, 2011; Pitarrio, 2007 & Jewkes & Andrews, 2005).

According to Bruce (1993), "a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment, or to evaluate those weaknesses to assist in

removing them." Hacking has recently taken the spotlight by storm as many corporations and government entities have been constantly under attack and successfully breached. Office of Personal Management, Ashley Madison, Anthem, VTech, IRS, Juniper Networks, and Sony Pictures all fell victim to data breaches that compromised personal, sensitive, and secret information (Lanaria, 2015). However, spies and hacktivists aren't the only ones taking advantage of this tool, as child predators have begun to use the art of hacking to blackmail and exploit children. They achieve this by hacking unsuspecting children's webcams (Muller, 2011).

Within the last few years, these types of attacks have garnered a great deal of media attention. Miss Teen USA, Cassidy Wolf, was a victim of sextortion when she was blackmailed by Jared James Abraham, a former classmate of Wolf. Abraham was able to hack into Wolf's and seven other victims' webcams, where he then proceeded to take nude images and videos while they undressed in their rooms without their knowledge. He then threatened to publish the images and videos online if they refused to send more explicit material and skype with him. Abraham also hacked his victim's social media accounts, a direct contact to their social life. Those who failed to meet his demands had their explicit material posted on their social media accounts. He also changed the passwords to their accounts which locked the victims out. Therefore, the victims were unable to delete the explicit photos and video on their own social media accounts (Botelho, 2013 & Stump, 2013).

Upon being threatened, Wolf scrambled to contact the FBI. The FBI failed to trace an Internet Provider (IP) address because Abraham was using a Virtual Private Network (VPN), a program used to encrypt one's IP address creating anonymity. However, further investigation revealed that Abraham used Darkcomet and Blackshades, programs used to hack and exploit laptop and their webcams. These program's origins or IP addresses were not protected by the

VPN allowing the FBI to successfully locate Abraham. VPNs encrypt users Internet; however it failed to encrypt these programs he installed on her computer. This story received national attention due to Wolf's popularity and fame as Miss Teen USA. She has become the poster child for sextortion. Even though Wolf wasn't underage, it's still illegal to commit sextortion (Botelho, 2013 & Today News, 2013).

Another example of this malicious crime is the hacking of baby monitors to watch and "talk" to children. CBS New York (2015) reports of a father who entered their three year old's room in time to hear a voice over the monitor saying, "Look someone's coming," or "Someone's coming into view." Additionally, the hacker was also able to remotely control the camera. Another hacker in 2013 was able to hack a baby monitor that watched over a two year-old girl. The couple that resided in Houston, Texas described hearing a strange voice coming from their daughter's room. Upon entering the room, they quickly noticed the voice was coming from their baby monitor. The hacker said, "Wake up Allyson, you little slut." The hacker was said to have had a British or European accent and was probably able to obtain her name from the wall decorations within the room. Then, the camera swiveled to the parents where the hacker proceeded to call the father a "stupid moron" and the mother a "bitch." The father unplugged the camera. Ironically, Allyson was born deaf and never head the harassment (Gross, 2013).

IMPORTANCE OF STUDY

This qualitative study is significant and original due to the lack of literature on child exploitation through the hacking of webcams. Because this crime is a new phenomenon, few studies have been conducting in this area. By interviewing law enforcement officers, we can better understand the nature of the threat, the methods used by child predators to commit such acts, law enforcement methods being used to combat this major problem and how children and

parents can take precautionary measures to prevent their child from becoming a victim of child exploitation. Child predators use an array of methods to exploit children within the cyberspace. This study will help us better understand if hacking is in fact a common technique used to exploit children within the cyberspace. Additionally, this study will help us understand how child predators successful exploit a child if the method of hacking is used.

CHAPTER 2

LITERATURE REVIEW

HISTORY

The Department of Justice defines child pornography "as any visual depiction of sexually explicit conduct involving a minor (someone under 18 years of age). Visual depictions include photographs, videos, digital or computer generated images indistinguishable from an actual minor, and images created, adapted, or modified, but appear to depict an identifiable, actual minor. Undeveloped film, undeveloped videotape, and electronically stored data that can be converted into a visual image of child pornography are also deemed illegal visual depictions under federal law" (Department of Justice, 2015a).

Throughout recorded history children have been victimized through sexual exploitation and sexualizing material. Children have often been sexualized through drawings, paintings and erotic literature through objectification. However, this phenomenon has become more prevalent with the invention of the film camera and video camera (Tate, 1990 & Tyler, 1985). Instead of erotic literature, drawings and paintings, child exploiters now have real pictures and videos. With the possession of real physical pictures and videos, child exploiters are able to create and distribute child pornography. However, due to the physical nature of film rolls and prints, law enforcement were easily able to monitor and combat the statutes that it violates and distribution of child pornography and child exploitation. Child pornography was often locally produced, expensive and problematic to obtain. Additionally, law enforcement were able to more accurately identify children being exploited due to the locality of production. This created paranoia among those who exploit children (Crewdson, 1998 & Tate, 1990). Due to the high risk

attributed to the illegal activity and successful monitoring by law enforcement, child pornography became a rare and expensive product around the mid-1980s.

Just as police had complete control over the child pornography trade, the Internet was born. With the advent of the Internet, people were able to communicate, network, and share information on a global scale (Binford, 2015). Information sharing expanded even more through the creation of social media, blogs and forums. Ultimately, the Internet has fundamentally changed how society interacts. Businesses, videos, pictures, forums for likeminded people, games, chats, and much more have revolutionized society as a whole. We were no longer living in the age of limited communication (Miller & Slater, 2001). Sadly, the ease of communication and information sharing is not all positive, as child predators and pedophiles actively use the cyberspace to exploit children.

The pedophiles and child predators now had a limitless source of communication and networking. This new source of communication and networking allowed the child pornography market to expand to unprecedented levels. With the stroke of a few keys and the click of a mouse, pedophiles and child pornographers had access to unlimited images and video of exploited children. Images and videos were purchased, traded and shared via "websites, email, instant messaging/ICQ, Internet Relay Chat (IRC), newsgroups, bulletin boards, peer-to-peer networks, and social networking sites" (U.S. Department of Justice, 2015b). However, the exploitation of children wasn't limited to pictures and videos. Pedophiles, child pornographers, and sexual predators use the internet to discuss their fantasies, experiences of exploiting children, interests, and their intentions (Holt, Bossler, & Seigfried-Spellar, 2015). With this mass communication between multiple individuals and their similar ideology, these deviants

normalize the physical and psychological damage they cause children by sympathizing with each other.

Additionally, the protection of identities attracted more individuals to exploit children (Department of Justice, 2015b). The extent of this problem can be seen in the available data. Due to laws or the absence of laws in geographic locations, child pornography can thrive without police intervention. It's estimated that there are around 100,000 child pornography websites that are run like commercial businesses which is believed to be a multibillion dollar business (House of Representatives, 2007). This business is thriving within the U.S. and around the world. In fact, "According to the FBI, the United States has seen a 2500% increase in the last ten years in the number of child pornography arrests (Wortley & Smallbone, 2012).

CHILD PREDATORS AND CHILD EXPLOITERS

Child pornography has long been around before the creation of the Internet. However, the creation of the Internet has fueled the encouragement and promotion of child exploitation (Edwards, 2000; Holt, Blevins, & Burkert, 2010; Krone, 2004; Quayle & Taylor, 2002 as cited in Holt et al., 2015). The anonymous nature and protection from social stigma or legal repercussions has allowed the exploitation of children within the cyberspace to thrive (Alexy, Burgess, & Baker, 2005; Durkin, 1997; Durkin & Hundersmarck, 2007; Holt et al., 2010; Rosenmann & Safir, 2006 as cited in Holt et al., 2015). This has allowed child exploiters to create, distribute, and trade child pornography. Additionally, this has allowed child exploiters to develop romantic and even sexual relationships with children online (Durkin, 1997; Jenkins, 2001; Quayle and Taylor, 2002; Taylor, Quayle, & Holland, 2001 as cited in Holt et al., 2015). This has given birth to a pedophile subculture in which individuals seek validation and justification of their sexual orientation and neutralizing the damage that occurred when

exploiting a child. This led to the belief that an adult-child relationship is a positive relationship and that nothing is wrong with their actions (Durkin & Bryant, 1999; Holt et al., 2010; Jenkins, 2001 & Mayer, 1985 as cited in Holt et al., 2015). Some even consider themselves as "child lovers" and claim they're not child molesters or pedophiles. They even condemn those particular groups. They claim only a small fraction abuse children and that child lovers are there to just look (Jenkins, 2001).

There are many types of individuals who present law enforcement with different challenges when combating the exploitation of children. Each type of individual has their own method of behavior. The first category of offenders are known as the "browser." The browser is someone who browses for child pornography. They knowingly save images, but they neither hide their activity nor collaborate with other child pornography users. Their use is an indirect example of child exploitation (Krone, 2004; 2005).

The second category includes "private fantasizer." Private fantasizers are similar to the browsers. However, private fantasizers go a step further by creating their own digital images for personal use. "Trawlers" are also very similar to the browser but they actively seek out child pornography. They also do little networking and take some time to hide their illegal activity (Krone, 2004; 2005).

The next category of offender are sophisticated individuals. The "non-secure collectors" hide in unsecure chat rooms but don't attempt to hide their internet activity. They attempt to collect images and videos of child pornography. These members are actively networking with other child pornography users (Merdian et al., 2013). The continuation of sophistication is present in "secure collectors." These collectors encrypt all of their Internet activity as they are fully integrated into the child pornography network. These individuals collect endless amounts of

child pornography, while they often cross reference and catalog. They also are after very rare and highly prized videos and pictures (Krone, 2004; 2005).

Child exploiters use methods that are both sophisticated and sadistic. These individuals have direct contact with naïve, vulnerable and unsuspecting children. These individuals groom children online by establishing online relationships. Groomers will attempt to win over the child with the promise of money, love and a better life (Prichard et al., 2013). The groomer will also send the child some pornography in an attempt to arouse their curiosity. These individuals are at high risk of detection, because the child may inform friends or family of their online relationship, or the "child" may be an undercover cop.

"Physical abusers" fall under the similar categorization of "groomers." Physical abusers sexually abuse children for their own sexual gratification. They may or may not record their sexual abuse and may or may not share it with other pedophiles. Their security depends on whether the child is willing to speak out. In a sense, physical abusers are very similar to "producers." Producers, however, record their sexual abuse of children with the intent to share it with other pedophiles. Producers may also be "distributors," who are most often interested in the financial gain of the booming child pornography market. However, some distributors do engage in the illegal activity. They have a massive confidential network of pedophiles they communicate with in order to further their profit (Krone, 2004; 2005).

CYBER STALKERS

Much like groomers, the cyber stalker is the birth of a new criminal type that was fostered with the birth of the Internet. These individuals stalk their targets through cyberspace in an attempt to harass, slander, and/or install fear in their victims using a variety of tactics (Pitarro, 2007). The internet is the primary weapon or tool in the cyber stalker's arsenal. This criminal

offender's success thrives off of anonymity, poor legal definitions, poor detection and global reach (Pitarro, 2007). Cyber stalking, a concept that falls under the umbrella of cyberbullying, is "the use of repeated and intense harassing messages that involve threats or cause the recipient to feel fear for their personal safety" (Willard, 2007 as cited in Holt et al., 2015). This fear can be instilled through threatening messages or in the case of convicted cyberstalker Shawn Sayer, posed as his ex-fiancé via Facebook posting explicit pictures and telling those who liked her material to come over for a sexual encounter. However, his ex-fiancé had no idea who these random men were showing up at her house and feared of being raped (Hoey, 2012 as cited in Holt et al., 2015). The cyberstalking actions carried over into reality where people are at-risk of being victimized. Compared to traditional stalking, cyberstalking can be very repetitive and sent messages rapidly, anytime of the day. This can cause much more distress because the messages will continue to come anytime through one's computer, tablet, and/or cell phone (Jones, Mitchell, and Finlcelhor, 2012 as cited in Holt et al., 2015).

Cyber stalkers are similar to traditional stalkers; however, their acts are committed through cyberspace. Many begin their stalking after having a relationship with the victim, perceived or real (Pitarro, 2007). However, the victim doesn't have to have any sort of relationship with the cyberstalker due to the amass amount of information there is of individuals on social media, blogs, etc. (Bocij, 2004). Even though their tactics are similar, the cyber stalker may have more information and sophisticated tools to work with compared to the traditional stalker. Cyber stalkers can access confidential information through social media, brokerage sites and social engineering. Due to the global reach of the Internet, cyber stalkers can target victims from any location. Because of jurisdictional issues, the cyber stalker may have complete immunity (Pitarro, 2007). Another problem that arises when addressing cyber stalking is law

enforcement's perception of threat. Cyberstalking does not involve physical contact. Therefore, law enforcement agencies may not perceive cyber stalkers to be a threat. However, the threats from cyberstalking are just as serious if not more serious than traditional stalking. (Pitarro, 2007 & Bocij, 2004 as cited in Holt et al., 2015).

Even though traditional stalkers often act alone, cyberspace can encourage cyber stalkers to work in groups and plan coordinated attacks. However, if you add the child predator aspect to cyberstalking, a new breed of deviants run rampant within cyberspace. These predators include child predators who can easily target unsuspecting children, especially those lacking parental supervision (Pitarro, 2007).

There are millions of adults and children who have access to the Internet while at work, school or at home. This creates a target rich environment for cyber stalkers. This problem will only increase as the Internet continues to grow. This also creates more cyber stalkers. This has led to a dramatic increase in cyber stalking crimes (Pitarro, 2007).

Email is often a cyber-stalker's primary weapon in their attacks. Cyber-stalkers use email to harass, threaten, send pictures, videos and send viruses in an attempt to infect their victim's computer and address book. The stalker will also use the victim's email to subscribe to obscene websites or use their personal information to make purchases. Cyber stalkers use cybersmearing (known as doxing) to post negative, harmful or personal information about their victim. This information can include false sexual innuendos about the victim in public chat rooms, boards, forums, newsgroups and bulletin boards. This can be very psychologically and emotionally damaging to a victim because they feel as if the whole world is laughing at them. The cyberstalker can post an abundance of harmful information about an individual within a very short period of time. If the information is removed, the cyberstalker can repost it. Facebook,

Twitter, Youtube, etc. are just some of the many ways a cyberstalker can cybersmear a victim (Jones, Mitchell, & Finlcelhor, 2012 as cited in Holt et al., 2015). Cyber stalkers will also belittle (a process known as flaming) the victim in public chat rooms, forums, etc. in order to establish control and harass the victim. Cyber stalkers also use anonymizing emails to cover their tracks of their deviant behavior (Pitarro, 2007 & Hoey, 2012 as cited in Holt et al., 2015).

Pittaro (2007) describes the four types of cyber stalkers: vindictive cyber stalkers, composed cyber stalkers, intimate cyber stalker, and collective cyber stalkers. Vindictive cyber stalkers are the most aggressive of the four. These stalkers use spamming, identity theft and email bombing to harass their victims. They're also the only stalker type to use Trojans to infect a victim's computer. These stalkers usually have average to above average computer skills and based on the content they send to their victims, are believed to have mental illness. Composed stalkers are calm in their actions. They harass their victims which includes keeping the victim stressed. The intimate cyber stalker is usually obsessed with their victim and their ultimate goal is to establish a relationship with the victim. They may have known the victim or they may have discovered them through cyber space. Lastly, collective cyber stalkers possess advanced skills, and work in a group to harass a target.

In summary, there are many types of individuals who exploit children using indirect or direct methods. Each type plays a significant role in the exploitation of children. In order to survive and thrive, these predators will continue to adapt and take advantage of the latest technological developments available in order to successfully exploit children. A cyberstalker will threaten a child in order to coerce or blackmail them in order to exploit them.

ANONYMIZING PROGRAMS AND SERVICES: ENCRYPTION

During the 1990s, the U.S. Naval Research Laboratory was tasked with developing an untraceable network of communications that was protected from the watchful eyes of enemies of the state. In response, they developed the deep (dark) web. The purpose of the deep web was to protect military communications. The deep web was designed to thwart potential hackers at every stage. First, our enemies would have to find a way onto the deep web. Once this was achieved they would have to intercept the message. However, when they would intercept the message, they wouldn't see any messages but rather encrypted data. This was intended as only the communicators could see the decrypted messages (Tian, Qi, & Liu, 2011; Tor).

In 2002, the Electronic Frontier Foundation funded what is known as Tor (TIAN et al., 2011). Tor, a deep web browser, was funded and created to promote security and privacy among internet users (Tor). "Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site. […] Journalists use Tor to communicate more safely with whistleblowers and dissidents" (Tor). Tor has many great uses such as protection for whistleblowers or safely surfing and communicating on the web without having to worry about being monitored by an oppressive regime. While Tor was created to better society, it has also helped facilitate the exploitation of children.

Accessing the deep web is a somewhat involved process. For one to visit the deep web, you must download the Tor relay as it is the only way it can be accessed. Once the Tor relay is turned on, it will connect to the Tor directory. Tor will obtain multiple IP addresses from the relay. Here the Tor software will route your computer to a random set of Tor relays. Once you

connect to the first relay, your IP address changes that of the first relay. The next relay it connects to will only see the address of the previous relay the computer was connected to and not the actual IP address. No relay knows the entire route of the IP relay connection. Once it is fully connected to the relay system, the computer has access to the deep web. It does not matter what websites that computer visits, its IP address will be the IP address of the last relay connection. These relays are spread across the globe. If someone were to IP trace a specific computer, they'll see it broadcasting out of a random global location and not the computer's physical location. Additionally, every time you visit any new sites, the relay process repeats to ensure complete anonymity. What the relay system is achieving is encryption. The data becomes unencrypted only after it finishes leaving its last relay. This is where your IP address shows up as somewhere in Denmark (Tor). There are Virtual Private Networks (VPNs) that can completely encrypt your data; however Tor does a fine job in doing so (Epiphaniou et al., 2014 & Neilson 2013). Tor will route you through at least three Tor servers before you end up at your final location. You could be routed through a server in Russia, then through Germany and finish in Sweden before you reach your destination (Tor). Your Internet connection cannot be monitored. This anonymizing tool creates a petri dish for criminal activity including hiring assassins, buying illegal firearms, drugs, state secrets and even loose radioactive material (Hout et al., 2013). One has access to all of these illegal services from the comfort of one's home.

Law enforcement is able to effectively trace your IP address on the clear web which is the Internet we use on a daily basis. That is if the user isn't using a VPN. However as previously stated, there are still many obstacles that reside in the clear web. To further compare matters, Tor anonymized all online activity. Additionally, the deep web is approximately five-hundred times larger than the clear web (Tor). With the anonymity of the Internet in a cyberspace five hundred

times larger than the clear web, criminal activity manifests and thrives. Hundreds of thousands of illicit videos and images are just a click away and law enforcement has been unable to stop the production and distribution of child pornography on the deep web.

However, this isn't the final tool that child exploiters use to "safely" exploit children. In fact, there is yet another well-known program freely available to people. After entering either the deep web or clear web, one can take another step to completely wipe your virtually foot print off the web. This next step requires a program also known as virtual private network (VPNs).

VIRTUAL PRIVATE NETWORKS (VPNs)

VPN's, much like Tor, encrypt data to ensure that it cannot be seen or traced back to its original location. VPNs are more commonly used on the clear web by governments, corporations, and individuals living under oppressive regimes. Even if a hacker was able to retrieve data, it would be unusable due to encryption. For example, a Chinese citizen can access YouTube, which is otherwise blocked by their government, by using the VPN's ability to change IP locations (i.e. from China to the United States) (Newton, 2008).

As Newton (2008, PG# 3-4) describes, VPNs can "'relocate' internet users and encrypt network traffic. This has some profound effects on criminality and law enforcement. A natural side effect of the implementation of mandatory government censorship would be to encourage criminals to use VPNs, because the kinds of network activity these people intend to carry out would be inhibited by the censorship system, leaving them with little alternative." Law enforcement's response to cybercrime becomes frustrating because the evidence needed to build a criminal case must be extracted from the encrypted data stream or memory. Given the anonymity of the Internet, the Tor relays, and the complete encryption of data from the final relay by the VPN, it is difficult for law enforcement to achieve any kind of success. Law

enforcement will have to jump the hurdles of anonymity and legality. This inhibits law enforcement's response to child exploitation within the cyberspace.

THE OVER ABUDNACE OF CHILD PORNOGRAPHY WITHIN THE CYBERSPACE

Another major problem that arises when attempting to combat child exploitation in the cyber space is the overabundance of child porn that is produced, distributed, and viewed every day (Jewkes & Andrews, 2005). It is virtually impossible for law enforcement to intercept and track down every single individual who viewed child pornography on the web. Law enforcement agencies are just simply outnumbered. Child exploiters are actually aware that the chances of being caught by law enforcement are very low (Jewkes & Andrews, 2005). Even in cases where law enforcement interrupts a child pornography network, the effect is minimal because there are so many networks out there, child pornography networks are pervasive (Jewkes & Andrews, 2005). What might seem like a big bust turns out to be nothing but a little bump in the road for child exploiters.

UNFOUND DANGERS

The invention of the web camera was a great innovation for the cyberspace. People from around the world use webcams to communicate as the web cam can broadcast live or recorded feeds to the World Wide Web. It can also be used to create and publish images. Webcams are cheap, user friendly and require minimal set up. Therefore, they allow easy access by children/teenagers.

There exists, however, a sinister side to this innovation. Webcams are often placed on top of computer monitors or built within a laptop where they're likely focused on the individual using the computer and/or the surroundings of a room in which the computer sits. This can lead to unknown dangers that stem from the webcam itself. For example, a child's personal life can be

broadcasted to the entire world through this device with or without their knowledge (Muller, 2011).

Yet, children/teenagers are used to broadcasting their life to the cyberspace because the Internet and social media have created a culture in which children fight for popularity and exposure to their peers. It's become common for children to share their daily lives and keep others updated on their adventures, successes and/or hardships (Muller, 2011). Websites such as Facebook and Twitter have likes and shares which fuels this competition for popularity. Because of this, children don't think twice about using social networking sites.

The technological advancements and social media culture creates a very vulnerable and/or a target rich environment for child predators (Laer, 2014 & Arntfield, 2015 as cited in Muller, 2011). These child predators scan webcam sites that unknowingly connect unsuspecting children/teenagers' webcams. This occurs when a webcam is connected to the Internet. It connects to the host server which can be accessed by anyone browsing the site unless protected by a password. They can be viewed by anybody unless a password is created. Once they've located their target, the predator will attempt to groom the child by establishing a "friendship" and/or "relationship." This process happens over an extended period of time as the predator gradually gains the adolescent's trust. Upon success, they will then attempt to convince the child to explicitly expose themselves via the webcam's picture, video recording or the live feed feature. These predators convince unsuspecting adolescents to engage in these activities by promising gifts, money, and love. Sadly, this tactic has proven successful and some victims have self-published their own pornography websites where users can subscribe (Muller, 2011). Children such as these are a product of a successful groom and, unfortunately, this is but one method of child exploitation. With a web camera and a little skill some child predators may

never have to groom another child. Instead, they can exploit a child/teenager in secrecy and then blackmail them with their images and videos.

A protective parent will take precautionary measures in order to ensure their child is safe online by setting ground rules. However, even if they follow the protective guidelines to the best of their ability, children may still be vulnerable to hackers. Hackers are problematic for governments, corporations, individuals, and children/ teenagers. Two recent examples of hacking included the Office of Personal Management (OPM) and Ashley Madison security breaches. If hackers can hack into the United States government, many won't have a problem hacking into webcams.

In the shadows of the cyberspace exist a specific hacking niche, which poses significant challenges for law enforcement. These individuals are what I identify as "Child Predator Hackers (CPH)." These hackers can hack into web cams without the user's knowledge or permission and the process is frighteningly simple. As Muller (2011, p. 8) explains, "There are some webcams that automatically post the URL of the webcam on a website when the software is installed. Even users who do not post their webcams on one of these sites could find their lives being shared with the world. Each webcam has a web address that can be found by search engines, who will then post it among their listings." While these web cams require passwords for access, users fail to change the default password, a password that is known and used by CPHs. Additionally, Trojan horse programs that infect a computer allow hackers to activate a webcam without the user's consent (Muller, 2011).

This combination of child predators and hackers is frightening as child predators can covertly record their victims and exploit them through the use of blackmailing. In doing so the CPH can obtain more sexually explicit material and/or possibly force the victim to engage in

sexual acts with themselves or others. Additionally, if the CPH can install a Remote Administration Tool (RAT), they can obtain passwords and personal information; thereby allowing hacker to access the victim's social media accounts and spread the explicit materials directly to friends, family and/or employers. In short, CPH has complete control over their victim (Muller, 2011).

LAW ENFORCEMENT RESPONSE

Law enforcement has developed many task forces to combat child exploitation within the cyberspace. First and foremost, the creation of the Internet Crimes Against Children (ICAC) "was created to help Federal, State and local law enforcement agencies enhance their investigative responses to offenders who use the Internet, online communication systems, or computer technology to sexually exploit children. The Program is funded by the United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention" (OJJDP, 2016). This task force consists of 61 coordinated task forces that branch out across the United States. These task forces represent over 3,000 local, state, and federal law enforcement agencies. Additionally, prosecutorial agencies also make up the ICAC task force.

These agencies attempt to be proactive in their investigation, conduct forensics investigations, and prosecute child exploiters (OJJDP, 2016). Since ICAC's creation in 1998, ICAC has helped train 465,000 law enforcement officers, prosecutors, and other individuals who specialized in combating child exploitation within the cyberspace. They have investigated 516,000 complaints of child exploitation within the cyberspace which has led to the arrest of more than 54,000 individuals (OJJDP, 2014). Additionally, in 2014, ICAC was responsible for more than 58,000 investigations as well as 66,000 forensics exams. This led to the arrest of 8,100 individuals (OJJDP, 2014). It is safe to say that ICAC is an effective response to child

exploitation within the cyberspace. ICAC will continue to conduct investigations, forensic exams, prosecute, and train individuals to combat child exploitation within the cyberspace.

Local and state law enforcement entities of Georgia fall under the ICAC umbrella (OJJDP, 2016). Additionally, the Georgia Bureau of Investigation (GBI) and Federal Bureau of Investigation (FBI) are members of ICAC (OJJDP, 2016). The GBI has formed the *Child Exploitation And Computer Crimes Unit* (CEACCU). This unit assists local and state law enforcement agencies in combating child exploitation through developing effective response to child exploitation, forensic and investigation assistance, victim services, prevention, and awareness (GBI, 2016). The FBI has created the *Violent Crimes Against Children* unit. This mission of this unit states, "first, to decrease the vulnerability of children to sexual exploitation; second, to develop a nationwide capacity to provide a rapid, effective, and measured investigative response to crimes against children; and third, to enhance the capabilities of state and local law enforcement investigators through programs, investigative assistance, and task force operations" The FBI achieves this by creating a task force consisting of agents from multiple agencies. With the help of ICAC, this task force can combat child exploitation within the cyberspace that spans across jurisdictional, geographical, and legal boundaries. This can involve national and international cases (FBI, 2010).

In summary, the ICAC was created to combat the unstoppable reach of child exploitation within the cyberspace. By training law enforcement and individuals, conducting investigations and forensics examinations, and prosecuting child exploiters, ICAC is a very effective tool used to combat child exploitation within the cyberspace. The GBI and FBI have developed their own task forces that work with many agencies and ICAC in order to ensure complete cohesion when dealing with this sophisticated matter. Lastly, the FBI often deals with cases that span over many

jurisdictional, geographical, and legal boundaries in order to ensure not only are American children safe but those of foreign countries as well.

CONCLUSION

Child predators have always existed within the cyberspace. Due to the global reach and anonymity of the Internet, child predators are able to successfully groom children within the cyberspace. The invention of the Internet developed many great features such as email, blogs, social media and the web camera. The web camera allowed pictures to be taken, videos to be recorded and the ability to conduct live streams. Child predators were quick to act to use this technological advancement by exploiting children through the web camera. First, it began with grooming children on web camera sites but quickly turned to hacking their web cameras and computers without their consent. CPHs would take pictures, record videos and/or stream live underage children changing their wardrobe. The more malicious child predator hackers escalate the severity of exploitation by blackmailing their victims. If the victim refuses to give into the hacker's demands, the hacker will publish the explicit material online or post it on the victim's social media account. Through this process these predators can obtain sexually explicit material of their victims and further their sextortion. The victims become trapped in a vicious cycle as they can't seek help without risking the publishing of their photos and videos. Therefore, the victim will continue to give in to the predator's demands.

Law enforcement has trouble combating child pornography and exploitation due to the anonymous nature of the internet, anonymizing programs and services, and the abundance of child pornography, exploitation, and blackmail. There is a paucity of research focusing on the hacking subculture of child predator hackers and law enforcement's knowledge, training, tactics, and response to child predator hacking. As such, this study will fill a significant gap in literature.

CHAPTER 3

METHODOLOGY

The study employed qualitative methods to explore the knowledge, training, and tactics of law enforcement in regards to child exploitation through hacking. Local, state and federal law enforcement agents who specialize in child exploitation were interviewed via telephone about child exploitation within the cyberspace and child predator hackers. Their combined experience covered local, state, and federal cases of child exploitation via hacking. Additionally, these individuals are agents who specialize and work child exploitation cases. The study sought to interview anyone who combated child exploitation within the cyberspace. My sample of five agents were contacted through mutual and personal contacts and through the Internet Crimes Against Children (ICAC) commanders contact page. I called and emailed many officers who specialize in child exploitation within the cyberspace. I explained to them the purpose of my thesis and why I would like to interview them. I supplied them with my proposal and consent form. This allowed them to develop a better understanding of the study. A few officers responded wanting to take part in the study. A few officers declined, however, stating they believed they wouldn't contribute or simply didn't want to partake in the study.

The officers interviewed had a combined experience of one hundred and fifty plus years. Two of the officers interviewed were ICAC commanders and would know of any kind of child predator hacking. The officers I interviewed were agents of the following agencies/organizations: a Southeast Sheriff's department, Georgia Bureau of Investigations (GBI), Federal Bureau of Investigations (FBI), a Midwest ICAC state commander, and a South East ICAC state commander. The ICAC commanders are state commanders who oversee all child exploitation within the state. Additionally, they're in constant contact with 61

other ICAC commanders and will know of the latest trends and dangers within the field of child exploitation. The local, state, and federal officers have strong relationships with ICAC and Non-Governmental Organizations (NGOs) such as the National Center for Missing and Exploited Children (NCMEC). Therefore, they're experts of this particular crime.

Upon answering my request, the officers agreed to being interviewed and signed a consent form. An interview date followed. The interviews were recorded using a phone audio recorder. The interviews ranged from fifteen minutes to forty-five minutes. Upon completion of the interview, the interviews were transcribed for data analysis.

The data became saturated due to the strong relationship that exists among child exploitation officers. As previously stated in the literature review, the agents who combat child exploitation work with an interconnected unit called ICAC. This unit allows cohesive communication between agencies, proper training, investigation, and prosecution (ICAC, 2016). The saturated data is a product of this organized unit. Due to their collaboration and efforts to combat any sort of child exploitation within the cyberspace, the agents generally answered the questions similarly because they have been informed on the subject matter and have strong communication ties.

The following questionnaire was administered during the interview to answer the eleven research questions:

RQ: Is child predator hacking a common crime?

1. Is sexual exploitation through the hacking of a minor's webcam a prevalent crime? Where is it most prevalent? Please explain in detail.

By administering this question we can develop a better understanding of the prevalence of this crime. This will determine if law enforcement believes this crime to be a common crime. I

began with this question because it laid the foundation for the questions to follow. If this was a common crime, it allowed me to further dive into it to develop a better understanding of child predator hacking of a minor's webcam.

RQ: Are our current law enforcement entities properly trained in the subject matter?

2. Have you received training on how to respond to a child being exploited by a hacker? What did the training entail? Do you believe its effective training? Due to the ever changing landscape of technology, does the training become outdated? Please explain in detail.

Regardless of the prevalence of this crime, this will determine law enforcement's response to this crime. Law enforcement's reactive response must be quick but properly administered. There are many variables that must be considered and overcome in order to apprehend and convict a child predator hacker. Due to the complexity, law enforcement may have a problem when combating this crime.

RQ: What does the common case display?

3. Have you ever dealt with a case where a child was exploited by a hacker? If so, could you describe the case and its outcome? Please explain in detail.

By asking the officer their personal experiences/cases, this allowed for a better understanding through first hand experiences. If they had experienced such a crime, they would be able to provide details, patterns, and outcomes of their case(s). Each officer may experience something unique or they may never experience such a crime.

RQ: How sophisticated are child predator hackers known to be?

4. What is the most sophisticated child predator hacking crime you have experienced and/or been informed? Please explain in detail.

This question will determine how sophisticated this crime can be. Crimes such as bank heists or hacking crimes can take years to plan as the criminals gather and formulate their attack using social engineering.

RQ: What must law enforcement overcome to combat this crime?

5. What challenging obstacles must you face when addressing and combating this crime? Please explain in detail.

This question will help determine what hurdles law enforcement face with addressing child exploitation via hacking. The sophistication of hacking or the cyberspace may inhibit law enforcement's response.

RQ: What group of adolescence is most at-risk of being exploited by a child predator/child predator hacker?

6. Which group of adolescence is at-most risk of this crime? Please explain in detail.

This question will address the at-risk population of this specific crime. Exploitation of individuals will always involve an at-risk population.

RQ: Are the child predator hackers evolving quicker than expected?

7. Do you see child predator hackers becoming more sophisticated in their acts due to the advancement in technology? Please explain in detail.

This interview question helped us better understand how problematic child predator hacking can be. Child predators are constantly outmaneuvering law enforcement due to their knowledge

of technology and the creation of better technology. Technology has exploded onto the scene which has allowed criminals to exploit people in unthinkable ways.

RQ: What common themes and/or patterns are arise in these particular criminal acts?

8. What occurring themes or patterns have you noticed when addressing and combating this crime? Please explain in detail.

This question helped determine if these crimes are similar in nature. Due to the complexity of hacking, these crimes can occur through many avenues and methods. This will allow, law enforcement, children, parents, and the community to develop defensive matters by watching out for specific tactics used among child predator hackers.

RQ: What must law enforcement and families do to protect their children from these predators?

9. How can we properly address and exterminate this crime? Please explain in detail.

By asking law enforcement this question, we can develop a better sense of the dangers of child exploitation and child predator hacking. Education on the subject matter will decrease victimization and will allow law enforcement's response to be more effective. A program could be developed from this question which can be used in presentations to educate children, parents, and the community.

RQ: Are current practices effective? If not, what needs to be changed?

10. What would you change in order to be more effective in combating this crime? Please explain in detail.

This question allowed us to better understand if the agents believed their current responses were effective. There is a possibility they may be restricted due to protocol, funding, or

jurisdiction. This will present many hurdles because the officers can only do so much even though the criminal might be in arm's reach. This will allow us to better understand what changes are needed to effectively address and combat this crime.

RQ: What does the future hold in regards to this crime?

11. What direction do you see child predators going in regards to hacking? Please explain in detail.

This question will develop a better understanding as to the future of child exploitation and child predator hacking. By foretelling the future, law enforcement, parents, children, and the community can better prepare for what is to come. More education, additional funds, more NGOs, new practices, etc. many be required due to the evolution of technology and tactics used by child predators.

Upon completion of the interviews, the interviews were transcribed for to be analyzed. Each of the eleven questions had five answers. The answers were grouped together per question to identify main themes and patterns. Main themes and patterns were drawn from the data. This data helped formulate the results and discussion of this study.

CHAPTER 4

RESULTS & DISCUSSION

RESULTS

RQ: Is child predator hacking a common crime?

All five of the agents interviewed stated that the hacking of a minor's webcam in order to exploit them is not a prevalent crime. In fact, none of the agents have ever dealt with such a crime. Some officers commented,

> "I have never come across it. It is […] something that is very difficult to do." – Agent 1
>
> "It's not a crime problem I have run into." - Agent 3
>
> "I have not even heard other commanders, there are 61 other commanders ICAC, I have never heard another commander discussing the hacking of webcams being a problem." – Agent 4

As all of the agents explained, a child predator seeks to exploit a child in the most efficient and easiest manner. This includes grooming and manipulating children in online chat rooms, smart phone application chat rooms, and social media. A child predator will trick a child into producing nude photographs or videos by posing as an attractive child of similar age. This "child" will show affection and attention towards their victim in order to gain their trust. Then, the "child" will dupe the victim into sending nude photographs or videos of themselves to the predator. Once this is achieved, the child predator will blackmail or commit 'sextortion' by threatening to release their nude images to the victim's friends, family, classmates, etc. unless they give into their demands. Their demands may consist of additional nude photographs and

videos, performing sexual acts that can become torturous and sadistic in nature on webcam, sexually exploit their sibling(s), perform "cam shows", and/or physically meet so the child predator can sexually abuse the child. Therefore, there is little reason for a child predator to hack a child's webcam.

In order for this to be achieved, a child predator must be knowledgeable of computers and the art of hacking. This requires the child predator to learn a new skill which will take time and effort. There is very little drive for a child predator to learn hacking if they can achieve about the same results by grooming and manipulating children online. This is reflective of the literature review which suggests that grooming is a common tactic used by child predators. Child predators groom children online through the promise of friendship, romance, etc. This allows the child predator to gain the child's trust which will lead to the child to dropping their defenses (Muller, 2011; Pitarrio, 2007 & Jewkes & Andrews, 2005). Thus, there is no demand for child predators to learn the art of hacking.

> "Not so much the hacking of the minor's webcam but what we're seeing is an abundance is that the children are using their webcams either by their phone or on their computer and they're talking to strangers." – Agent 2

> "What we see generally related to sextortion matters is a little bit different. The child is either duped into putting out nude photographs or videos, using a webcam out to somebody they think they can trust." – Agent 3

RQ: Are our current law enforcement entities properly trained in the subject matter?

Two of the five agents received training on how to respond to a child being exploited by a hacker. However, the training was generalized in the sense of sextortion and the hacking of

minor's social media. This is a bit different because the hacker will first obtain nude photographs and videos through the process of grooming and manipulation. Then, the hacker will threaten to publish those photos on their own social media accounts if they don't give into their demands. However, if they don't obtain explicit photographs/videos, they can still bully the child by threatening to post on their social media or harass other children. One officer explained the process,

> "A person takes over their account or locks down their computer and then forces the child to either send explicit images back to the hacker and specifically in those we keep updated online internet technique training." – Officer 2

A hacker who hacks a child's webcam can obtain explicit material without the minor knowing. However, regardless of how they obtain them, they can exploit them using blackmail. Sadly, most of the officers reported that many children are consensually giving these predators what they want. Once they do so, the child predator will now have blackmail material and begin to blackmail the child. One agent commented,

> "Sextortion is usually the child sends the explicit pictures. Hacking is a rare case but sextortion is not." – Agent 2

Of the two agents who received training on the matter, one believed the training to be effective. This agent believed they are keeping up with the latest in child exploitation through constant and updated training. The other felt it quite often was outdated due to the ever-changing landscape of technology. One agent explained,

> "The training is often outdated sooner than later. I would think about every quarter, every three months we receive new information of new techniques in order to get these guys. – Agent 2

Technology is constantly changing, sometimes too quickly. Therefore, it requires a lot of time, money, and resources to constantly keep up with the ever-changing landscape of technology. Once child predators discover law enforcement techniques to combat this crime, they evolve in order to remain undetected. This is amplified through the creation of anonymizing technology and social media. Child predators have begun to use encryption programs in order to hide their online activity and to hide their saved data. Therefore, there is very little law enforcement can do as encryption requires a key in order to crack it.

Law enforcement officers are trained to properly respond to child exploitation, however, not so much to the hacking aspect. This is because child predator hacking is a rare crime from law enforcement's perspective. Therefore, there is little need to train on the subject matter as they can spend time and resources on more urgent matters of child exploitation. The reference to sextortion is repeated within the literature review as child predators exploit children through grooming and sextortion (Muller, 2011; Pitarrio, 2007 & Jewkes & Andrews, 2005). This is a tactic used regardless of how they obtained the explicit material.

RQ: What does the common case display?

Only one of the five agents worked a case where a child was exploited by a hacker, but this case involved social engineering of a social media account and not the hacking of a minor's webcam. As previously discussed, most child exploitation cases involve a child knowingly supplying the child predator with photographs or videos upon being groomed and manipulated.

One agent reported that mistakenly some parents believe their child's webcam or computer was hacked, when in reality the child knowingly supplied the child predator with content. Therefore, grooming and manipulation account for almost all child exploitation cases.

> "They were able to find out the person's email on Facebook and then abuse the child that way by bullying, posting inappropriate stuff. I have worked several of those. […]Pretty much they'll find the password through social networking. Such as they'll have conversation with the child and they'll find out key words such as their mother's maiden name. They will go in and try to reset the account via the reset buttons that require security questions. And they will take over the account." – Agent 2

Therefore, the common case of child exploitation displayed a case of grooming and manipulation. This is because the grooming and manipulation is a very effective and easy avenue for child predators. There is little need to exploit a child through hacking if the child is knowingly giving the child predators what they want.

However, for agent 2, the case of the hijacking of the social media accounts consisted of social engineering. The child predator will social engineer their security questions for their email or social media account. Under definition, this is hacking although it doesn't require coding or breaking past firewalls. Because only one of the five officers experienced a form of hacking, they were not able to provide a proper answer to the hacking of a minor's web cam. This is reflected in the literature review because these child predators target vulnerable children to groom. In doing so, they can obtain their objective with easier means. Children who voluntarily publish their information in search of friendship and popularity are the easiest of targets. Furthermore, these children are also more open to strangers due to attention seeking (Muller, 2011).

RQ: How sophisticated are child predator hackers known to be?

Only one of the five agents heard of a case of child predator hacking into a webcam. This officer did not work this case. This case involved a hacker gaining access to a baby cam and harassing the child. Even though the agent never stated a particular case, he was informed of a case where a hacker was talking/taunting a family through the microphone of the baby cam. This microphone is used so the parent can talk to the child from a distance. However, the hacker used it to harass a family. Apart from this isolated case, officers reported that most child exploitation occurs by luring the child on the Internet through manipulation and grooming. Additionally, when these children perform sexual acts they often do not know they're being recorded. Instead, when the evidence surfaces, they believed they were hacked. Additionally, one agent contacted all of his task force members who have a combined experience of well over 100 years and none of them have experienced this type of crime and therefore little data exists on the matter.

> "For preparation for your interview, I contacted all my tasks force members and these guys, our combined experience is well over 100 years and none of them have experienced that type of crime. And these guys have been doing it forever. A lot longer than I have. – Agent 3

Therefore, the officers described how grooming and manipulation can be sophisticated through the act of social engineering. Children are willingly giving these child predator's explicit material. Consequently, child predators don't exactly need to be sophisticated in their technique. Instead, they just have to seek a vulnerable or naïve child and "befriend" them. It is then that the child predator will attempt to make the child comfortable with them. Therefore, there is very little drive to learn the art of hacking and this will continue if grooming and manipulation are

effective. This may continue to be the case because more and more individuals are being born into the technology age as they become dependent upon their smart phone.

RQ: What must law enforcement overcome to combat this crime?

Two of the five agents believed this crime is under-reported due to the blackmailing nature of child exploitation via hacking. That, in fact, the child predators are successfully hacking children webcams and taking explicit pictures of them without their consent. Then, the child predator will exploit them with this material. One agent explained that child exploitation in general is very frustrating due to the Internet's global reach. Therefore, it's hard to locate the child predator regardless if they're hacking or grooming/manipulating the child. There is a possibility that the child predator could be located in a country that doesn't share extradition powers with the United States or the government of those countries don't consider child exploitation a crime problem.

> "Bunch of the problems is that a lot of the videos and images we encounter are not of children from the US. They're foreign and some of those countries do not cooperate with us. We don't share extradition. They're not going to arrest their citizens because they don't consider it a crime problem." – Agent 3

Additionally, some of these child predators have begun to use the deep web and/or Virtual Private Networks (VPNs) which enables encryption. This not only allows them to hide the evidence but to also hide their digital footprint. Additionally, the child predators want to hide themselves but will slowly reveal their true identity.

> Me: "Do they utilize Deep Web and encryption to hide their activity?"

> Officer: "Yes, absolutely. The reason that is done is because that person is going to hide themselves until they're able to develop some type of relationship with that child. Then once they build the trust in that child then they can start revealing more about themselves. And any type of situation they're never going to reveal to you exactly who they are or where they're at. That's never going to happen. But once they build an online relationship with the child, and they start communication back and forth, the dialog that happens regularly you know these they build that trust and they will start to reveal more and more of themselves to the child and vice versa. The child will reveal more and more of themselves to the predator. It gets to a point where the predator convinces the child he's not a predator but a friend. And wants to then take it to the next level and meet somewhere to talk. Yes, absolutely people hide themselves." – Agent 1

This is a prime example of a child predator using advanced technology to exploit a child. This is just another layer used to remain undetected in their attempt to groom and manipulate a child.

Lastly, one agent stated that in order to overcome the crime of hacking, children will need to change their passwords to more sophisticated ones and protect them. This applies to any kind of cyber security. Passwords that are simple or that can easily be socially engineered put the child at great risk.

> "I guess the biggest thing is children need to protect their password, change them often. If you have routers and modems, put passwords on those. That's how people get into your computers. Easily, if you're not protecting your internet through the modems or routers. With the right software and start packet grabbing and seeing passwords that way." – Agent 2

Therefore, location, anonymity, vulnerable children, and cyber security of social media are the biggest obstacles law enforcement must overcome to combat this crime. This can apply to child predator hacking. Most of the officers, however, couldn't comment on the subject matter because they have never experienced or been informed of the particular crime. This is reflective within the literature review because of the anonymizing nature of the internet and these programs. It allows child predators to operate undetected.

RQ: Which category of children are most at-risk?

There was general consensus among the officers regarding the most at-risk youth. Agents noted that children between the ages of 8 to 16 years old represent the most at-risk group, because these children or their parents are unaware of the dangers of the Internet. This age group is often curious, innocent, and naïve as they're excited to talk with anyone and everyone. Social media helps facilitate communication, and the profusion of social media phone applications afford children with more privacy when using their phones, compared to a computer screen located within a family room. Parents do very little to monitor their children's online activity which provides little to no protection. One agent believed young girls are the most at-risk because they seek validation and acceptance. They're willing to put themselves out there in order to make friends. Another agent suggested single parent homes created at-risk children. A single parent is more likely to be working to provide for their child and will have less time to spend with them. Lastly, youth who are lonely may publish images and attention seeking messages in order to seek friendship. A child predator will immediately become their "friend" in order to exploit their vulnerability. This occurs through social media as child predators can see who's in need of attention (Laer, 2014 & Arntfield, 2015). Some agents stated,

"I would say that your biggest at-risk group would probably be someone between the ages maybe 8 years old up to 16. Characteristics you know it's just most of your kids starting around about the age of 8-9 years old, that group is, they're starting to get, they're starting to really move into the whole technology field and wanting to get into social media. Those are the ones that are most vulnerable. They just don't understand the risks that are out there. […]I think it's just kids that are curious. And the kids that are curious getting online and chatting and being a part of social media. And that's why they are taking advantage of. […] They're just getting on to have fun and talk to people. It's all fun and games to them. It's fun to get on there and talk to people. Talk to with someone in Cali or talk with someone in Sydney, Australia, you know. And that's what really I think, that and just the curiosity of meeting different people and doing different things on the computer, they know they're not supposed to. Doing what most children do, most children are mischiefs and curious. It's just one of those things. A lot of what I have seen in my experience are young boys and young girls who have very little supervision when it comes to social media. And most of this stuff is done with their cell phones at night when they are in their rooms and their parents are in their beds asleep. Sooo..... that's just part of being a curious teenager. They don't realize how dangerous these people out there really are. I could show you videos of this stuff where your mind would be blown of young girls that are doing this stuff. I have countless numbers of them here. Where young girls are setting up their phones and there either masturbating or there doing these types of things because number 1, a lot of them are seeking attention. Looking for attention. They will find it from a child predator. They will. They talk them into doing these things and you know next thing you know they done something and they

uploaded it and sent it to this person because they asked them for it and they took and interests in them." – Agent 1

Agent 2: "Phone apps. Absolutely the children that are being issued these smarts phones are most exploited. The most exploited are the 12-16 year olds. […] They're out there looking for […] acceptability into groups. They're willing to put themselves more at risk in order to be a part of something.

Me: Any other characteristics?

Agent 2: Well the teenage years themselves hold a whole host of problem. Of course these young girls want to be accepted. Why they put themselves at extra risk even with their online friends. They will put themselves out there on the web. Willing to take riskier behaviors such as inappropriate images. I think it will be more the younger girls than the guys." – Agent 2

Agent 3: "Single parent home situation, parent is not monitoring internet usage properly. You know it can lead to those types of problems. Yea, we done presentations before and make it very clear that parents must be very careful allowing their children to have smart phones and not being able to monitor or monitoring properly their behavior. You know, I think that's one of the biggest concerns.

Me: What about children that are lonely, bullied, etc.?

Agent 3: Yes, I have seen that before in children who voluntary put their images out on the internet because they're lonely. They meet somebody in a chat room that person immediately behave like their best friend. Eventually manipulate them into exposing

> themselves on a webcam. Again, it's not hacking. There doing it voluntarily. There being misled into who there actually interacting with." – Agent 3

These at-risk youth are vulnerable and child predators know this. They prey on their neglect, loneliness and naïve nature. This is part of the grooming and manipulation process that allows child predators to exploit children with ease. A child predator will continue to complement them, give them gifts, and listen/talk to them. Sadly, it's the perfect storm for a child predator.

This is a repeat of the literature review in regards to suitable targets. Child predators look to groom children with gifts, friendship and love. The more vulnerable the child is, the easier it will be to win over the child with gifts, friendship and love. The child predator is filling the void that has left the child feeling unwanted, unloved, and worthless (Muller, 2011; Pitarrio, 2007 & Jewkes & Andrews, 2005).

RQ: Are the child predator hackers evolving quicker than expected?

Because most of the agents have never seen this sort of crime before, they couldn't comment on the matter. However, the agents were able to provide information on child predator's sophistication in general. However, it may be awhile before that threshold is achieved. Instead, most child predators use file sharing to share and download child pornography, which does not require them to visit websites and risk exposure to law enforcement. Child predators further protect themselves by using encryption software to hide their location and to encrypt their data. There is a possibility that child predator hacking will become an issue one day but until then, child predators use other innovative techniques to groom and manipulate children. With advancements in technology, crime closely follows.

> "Unfortunately, we are starting to see more encryption. But at this current point the encryption is not being used on the computers as much the encryption of passwords or codes on phones is being used quite often." – Agent 2
>
> "They're very sophisticated uhh what I deal with possessors, disturbers, recipients, are very computer savvy. They know exactly what they're doing. They try to hide it in non-allocated folders. Transfers it from their laptop onto external drives which are a lot easier to hide." – Agent 3

Like other criminals, child exploiters will take advantage of technology to commit their illegal acts. Technology allows crime to occur by using different and innovative methods. This will cause problems for law enforcement because they may not fully develop the new technology and develop a response. Sometimes, technology poses many legality issues due to the U.S. Constitution. Criminals know this as they operate under the cloak of anonymity.

RQ: What common themes and/or patterns arise in these particular criminal acts?

While none of the agents included in this study had worked a case involving child predator hacking a webcam, two officers provided a more generalized explanation of child exploitation. Echoing earlier comments, these officers explained that manipulation and social engineering are the primary tools utilized by child predators, regardless of the method they use to gain initial access to the child. This manipulative technique allows child predators to infiltrate and trick the child into doing something they normally wouldn't do. Additionally, this is the basis for hacking. A hacker usually needs to social engineer their target before they can hack them. Therefore, this next step can easily be applied to child exploitation. Two agents explained,

> "I guess the biggest one if you had to give it a reoccurring pattern would just be the manipulation." – Agent 1

> "A lot of the crimes are occurring through social engineering." – Agent 2

Simply put, child predators will continue to use grooming as their main tool to exploit children. Hacking requires too much attention and effort as it will provide little benefit to child predators. Instead, they'll use the pool of possible victims that willingly and openly publish their personal information on the internet. This will continue as we become interconnected through new venues of social media and our dependence increases upon technology.

RQ: What must law enforcement and families do to protect their children from these predators?

There was broad consensus among the officers that education, community awareness, and parental involvement are key factors in protecting children from these child predators. First, not only do children need to be educated on these dangerous matters but the parents require education as well. Education programs should focus on the dangers of the Internet and how there are evil individuals out there who will exploit a child given the chance. The GBI and FBI already do this; however, they can only cover so many schools and redirect enough resources and agents to educate children on the subject matter. Second, there must be community involvement to inform the community of the dangers of the Internet. With community awareness, neighbors, friends, and family can recognize and combat child exploitation. Lastly, and most importantly, parents need to carefully monitor their children's online activity to ensure that their child does not fall victim to child exploitation. Child exploitation in the cyberspace will greatly decrease if society could practice these three simple concepts. Some agents explained,

"The biggest way to combat this stuff, the absolute biggest way is parents getting involved in what their children are dong. That's the biggest way you can combat it. Concerned parents who are actually willing to go sit down at a computer that these kids are using and go in and starting looking at their histories. See what they're doing and what kind of sites they're going to. […] Too many parents are giving their kids these smart phones such as iPhones. Those children are going to bed in their rooms at night on the opposite end of the house, they're chatting online, they are linked up to the internet, their parents have no idea they're doing this, no idea. So.... it's one of those things where parents get involved and they start regulating what their children are doing online. That is the only way you can combat this other than LE getting involved in it. Usually by the time we get involved with it, it's usually too late. There's already some time interaction between the predator and child. It becomes our job to seek these people out. If you want to eliminate it, my personal belief is parenting." – Agent 1

Agent 2: "Again, I think community involvement is the biggest thing. Spreading the word that these guys are out here as predators looking for our children. […]Children are more than willing to give up their personal info via the web what we ever thought about. We try to protect our social security numbers. These children just don't see that. They let everything out on the web."

Me: "Could the GBI create an awareness/education program?"

Agent 2: GBI is already doing that with the ICAC task force. We have an education component where we go to schools, community forums and provide this info to safe guard their data." – Agent 2

> "Making children aware that there are monsters out there. Community outreach presentations at school all the time. Important to make these children aware that they can be vulnerable if they're not careful who they communicate with." – Agent 3

> "Education is key to addressing and, hopefully, reducing such offenses. Parental oversight of adolescent online behavior is also critical. As long as webcams exist, I see no way to "exterminate" this type of crime." – Agent 5

By educating our youth, their parents, and the community, we can be proactive on the subject matter. Law enforcement can only do so much and they are often a reactive force. The community must be a proactive force by alerting law enforcement of any suspicious activity, watching out for signs of child exploitation or sextortion, and ensuring children know about the dangers of the Internet and how to protect themselves. Even though it isn't directly stated within the literature review, it builds off of literature regarding grooming and suitable targets. Child predators seek to groom these particular children due to their susceptibility (Muller, 2011; Pitarrio, 2007 & Jewkes & Andrews, 2005). If we can educate parents, children, and the community then we can build defenses against groomers. Not only will it be harder to groom a child online but it will also allow children and parents to recognize at-risk youth and a child predator.

RQ: Are current practices effective? If not, what needs to be changed?

The officers agreed that the current practices are effective but they're a reactive force, and much of their success is driven by money. For example, law enforcement most often becomes involved with a child exploitation case after the child has been victimized. It is rare for law enforcement to apprehend a child exploiter before they commit their crimes. Additionally,

technology is constantly changing and law enforcement must continually adapt and update their equipment in order to effectively combat child exploitation. Technologies such as encryption, mobile apps, etc. require innovative technology in order for law enforcement to effectively respond to child exploitation within the cyberspace. While the officers interviewed for this study believe they receive an ample amount of funding to combat this crime, the community must be proactive, to prevent children from being exploited. A few agents commented:

> "It all comes down to money. How many people can we have and how can we get the info out there? Where are you going to get the money to do the training and distribution of these training programs?" – Agent 2

> "Most of this is money driven. That's the biggest challenge is to buy the equipment to combat these crimes. The technology changes constantly. Quickly, have a laptop state of the art and two years later it's not even close to state of the art its needs to be replaced. Sometimes funding is very difficult; sometimes funding is not. The DOJ allocation of funds is based on crime threat and what is biggest threat out there. For a number of years it was terrorism. That's where most of the funds went. The criminal side of the house suffered." – Agent 3

Law enforcement must be kept up to date on the latest tactics used by child predators. Additionally, if law enforcement cannot receive the required funding, they can no longer keep up with the pace of technological advancement. A state of the art computer will be obsolete within a year. Social engineering is the foundation of child exploitation within the cyberspace and will require the latest and greatest technology to combat it. Lastly, the officers mentioned how they are a reactive force. They would require more proactive presentations on child exploitation

within the cyberspace within schools, churches, youth groups, community meetings, etc. to better spread the message. This is a proactive measure law enforcement can effectively administer.

RQ: What does the future hold in regards to this crime?

All of the officers believed child exploitation via hacking will become a prevalent crime in the future. Unlike older generations, today's youth were born into the smart phone and tablet age. Society's over-reliance on smart phones and tablets has created a target rich environment for hackers as anyone and everyone can become a victim. Furthermore, as the world becomes increasingly connected to the Internet, more child predators and naïve children will dive into the cyberspace. Lastly, people from around the world are becoming more tech savvy which will allow them to hack not only into webcams but banks, emails, etc. This form of criminal hacking is already prevalent and will continue to get worse.

> "I can only guess that the hacking will be more prevalent in order to exploit our children because we're talking real time data being given to them because a child is not going to put down that phone you know very often during the day. And um the phone is a window into their life. Their life is going to be exploited by the hackers of the future." – Officer 2
>
> "As technology advances, to be honest with you it's so easy to get victims right now there is no need for that. These kids go out there and just plainly give these people what they want. So there is no need to go to these extremes right now. […] It's just a generational issue of technology. Exactly, it's scary because children at much younger ages are becoming more sexualized and they're communicating with individual that are clearly strangers online. We have seem to have lost this balance of being afraid of the stranger. […] I don't think, the way we look at it here for instance is public outreach is

> our best prevention. That's got to be our best offense. Getting into the schools, getting with the children and educating them of how to make safer choices online. […] "Yea, I potential see it getting worse and worse only because we can see our victims getting younger and younger." – Agent 4
>
> "Everyone looks to using advancements in technology to make work easier. Child predators are no different. The criminal elements of society will always find a way to exploit technology to advance his or her criminal purpose." – Agent 5

More and more people are connecting to the Internet and social media every day. These new comers will bring a new wave of naïve individuals as they publish personal information for popularity and attention. Much like the current generation, they too will become dependent upon technology which will create a bigger pool of possible victims. Additionally, more individuals are becoming technologically savvy which can possibly lead to more hacking incidents. Hacking requires the knowledge of coding and computers. More and more individuals, however, are learning these skills due to the explosive age of technology. In conclusion, child predators will always have an ample amount of possible victims. As third world countries, like Afghanistan, connect to the Internet, they'll jump into the dangerous world of cyberspace.

CHAPTER 5

DISCUSSION, LIMITATIONS, AND FUTURE IMPLICTIONS

AVENUES OF EXPLOITATION

According to the data collected for this study, child predator hacking is a very rare crime. Evidence suggests that child predator hacking is quite difficult and there are easier methods that yield the same results such as online grooming and manipulation. Grooming and manipulating a child online is a successful technique used by child predators. Innocent and naïve children enter the cyber space looking for friendship, to explore, participate in social media, and meet new people. Child predators know what children want and exploit them through these avenues. These predators will pose as other children, often times as an attractive teenager, seek children who are lonely and are pursuing friendship and acceptance, and/or look for young girls who are looking for validation. These particular children at times often willingly and knowingly send child predators explicit photographs and/or videos. This will evolve into 'sextortion' as they blackmail the child into sending more photographs and/or videos or meeting in person in order to sexually exploit them. Therefore, there is very little drive in a child predator to exploit a child using more sophisticated techniques. This may lead to self-publishing their own child pornography where child predators can subscribe (Muller, 2011).

BLACKMAIL

Even though child predator hacking does not appear to be a prevalent crime at this time, there is a possibility that child predator hacking could be under-reported because it can involve blackmail or 'sextortion'. In these instances, a child could be recorded/photographed without knowledge or consent in an explicit manner. The child predator hacker will then contact the child

with demands and proof of their blackmail. Sadly, the child will believe they have no choice but to give in to the child predator's demand or risk having their explicit photographs and videos leaked to their friends, family, school, community, and the world. This type of crime will likely never be brought to the attention of parents or law enforcement. You can't respond to a threat if you can't detect it. You can take all the protective steps available but there is still a chance a hacker can get into a child's webcam.

CHILD PREDATOR HACKING AND SOCIAL ENGINEERING

Hacking to exploit a child does occur; however, the officers interviewed in this study have only seen it occur through the hacking of social media. Rather than use more technologically savvy methods of hacking, child predators rely on social media in order to obtain sensitive information. Eventually, the child predator will gather enough evidence to correctly answer the security questions to their victim's social media accounts and successfully hijack them. The child predator will bully the child through their social media account and/or threaten to post their explicit pictures and videos directly to their social media accounts which is connected to all of their friends and family.

COMBATING CHILD EXPLOITATION

In order to successfully combat child exploitation, parents, children, and the community must become educated on the subject, raise community awareness, and become involved in their children's online activity. Because law enforcement is a largely reactive force, society must be more proactive. Technology is constantly changing which is allowing children to become exposed to more avenues of danger within the cyberspace. Instead of committing child predator hacking, child predators will groom and manipulate the child in order to exploit them. Groomers

attempt to win over a child with the promise of money, friendship, and love (Prichard et al., 2013). A groomer will use phone apps, social media and chat rooms to exploit a child. Children and parents must understand these innovative and attractive avenues of communication will be used because child predators know children are attracted to these avenues of communication because the Internet and social media have fostered a culture of popularity and exposure to their peers, community, and the world. It's common for children to share their lives on a daily or even hourly basis as they keep others updated on their adventures, successes and/or hardships (Muller, 2011).

Websites such as Facebook and Twitter allow children to publish the most sensitive information to hundreds, thousands, or even millions of people. They seek attention and popularity as they publish anything for attention. This can include lonely children who will often make desperate pleas for help, attention, and/or friendship. As a result, a vulnerable and target rich environment is freely available to child predators. They will know a lot about the child, their family, their interests, their social status, etc. (Laer, 2014; Arntfield, 2015). However, this also displays what a child will do in order to gain attention. They're not just limited to Facebook or Twitter but to chat rooms, forums, blogs, etc. A child predator will then social engineer the child in order to exploit them. This should be a major topic covered when educating children, parents, and the community on the dangers of the Internet and social media. These examples should also be used when addressing parental involvement. A parent should understand that these phones and tablets allow child predators to directly contact their child. Additionally, parents can better monitor what their child is publishing online or deny them access to social media or other websites.

Lastly, the ICAC commander interviewed stated how exposure to the Internet has led to a loss of balance of being afraid of the stranger. Additionally, according to the ICAC commander, children are becoming more sexualized as they're being exposed to uncensored content which is allowing children to become easier targets for grooming. The ICAC commander explains,

> "It's scary because children at much younger ages are becoming more sexualized and they're communicating with individuals that are clearly strangers online. We have seem to have lost this balance of being afraid of the stranger. […] Just because friends you think they're, you know, that's their friend. And becoming comfortable with and the grooming process starts so on and so forth. – Agent 4

Therefore, law enforcement should focus on being proactive through seminars, presentations, commercials, pamphlets, training, and whatever is needed to spread awareness. Law enforcement doesn't believe child predator hacking to be a problem but instead children consensually giving child predators explicit material upon being groomed. This proactive approach will benefit everyone because the awareness will cover the entire spectrum of awareness. This will also allow law enforcement to develop a relationship with the community. In doing so, victims and parents are more willing to come forward to seek help. They will view law enforcement as a friend instead of an incompetent enemy.

However, it must be noted that law enforcement should keep a close eye on child predator hacking. It has and does occur. They should continue to spread awareness and combat the grooming and manipulation but also address what the future holds in regards to child exploitation within the cyberspace. Therefore, law enforcement should develop a D.A.R.E. like program in order to address child exploitation. Education should and needs to be required when the child is at least seven to eight years old. It's around this time that children begin to use and

explore the Internet. If we were to wait until they turn ten, they may already have been victimized or are currently being victimized by a child predator. The young age doesn't deter a child predator. In fact it will make them a more suitable target due to their innocence and naïve nature of a young child.

MORAL PANICS

As the results suggest, child predator hacking is not a prevalent crime. However, many people have begun to tape up their webcams on their computers and fear hackers might one day break into their computers (Muller, 2011). Yet, is this necessary? This may be a result of a moral panic fueled by sensational media coverage, television shows, and the current hacking crisis the United States is experiencing. Cohen (2004, p. 9) defines "moral panics" as,

> "a condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests; its nature is presented in a stylized and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people; socially accredited experts pronounce their diagnoses and solutions; ways of coping are evolved or (more often) resorted to; the condition then disappears, submerges or deteriorates and becomes more visible. Sometimes the object of the panic is quite novel and at other times it is something which has been in existence long enough, but suddenly appears in the limelight. Sometimes the panic passes over and is forgotten, except in folklore and collective memory; at other times it has more serious and long-lasting repercussions and might produce such changes . . . in legal and social policy or even in the way the society conceives itself."

Cohen (2004, p. 8) would describe hackers as the "folk devils." The webcam hacking of Miss Teen USA Cassidy Wolf made national headlines as she was exploited by a hacker. The hacker would wait for Wolf to undress and then take explicit pictures without her knowledge or consent. Due to her popularity, this particular crime became a hot topic among Americans. She even became the poster child for cyberbullying and sextortion.

With the hacks of OPM, Sony Pictures, Blue Cross/Blue Shield, DHS, FBI, CIA, etc., the crime of hacking is on most Americans' minds. They know how vulnerable our information is

within the cyberspace which creates a fear of being hacked. Recently, the show Mr. Robot, a show depicting a psychologically impaired hacker who is the mastermind behind one of the biggest hacks for humanity, displays the power of what hackers can do from the comfort of their own home or through the power of social engineering.

This constant reminder of hacking has created a sudden fear of being victimized. The public looks for legislation, police action, answers, etc. in order to feel safe and protected even if its false security. Therefore, this has led to people believing they may become victims to hacking. Technically, a lot of Americans have already become victims to hacking. It's only a matter of time before they will be victimized again unless cyber security improves. Is it only a matter of time until child predator hacking becomes prevalent? It took a few years for cyber espionage to occur; however, it is now one of our biggest threats to national security (White House, 2016). Will child predator hacking parallel the current hacking crisis? Will this moral panic turn into a real threat? Only time will tell. These "folk devils" may be more of a threat to our children than we may know.

LIMITATIONS

There is little literature that exists on child exploitation via hacking. Therefore, many limitations surfaced. First, generalizability is limited because these data only consists of law enforcement's perception of the crime. This affects my results because the data doesn't paint the full picture. If this study was to be duplicated, it would include data from youth aged 8 to 17, and adults aged 18-25. Secondly, the current study examined one facet of this phenomena. The data collected only paints 1/3 of the picture. None of the data collected addresses adolescence experiences or child predators and their usage of child predator hacking. While the current study addresses a critical gap in the literature, information from victims and predators is needed to

more completely assess the extent of the problem. Again, this affected my results because it only gives me a limited perspective. If this study were to be conducted again, it would include the data from possible victims and child predators.

Other limitations stem from the sample's demographics. The agents interviewed in this study were all located in the southeast United States. The sample size consisted of five agents; those five agent's knowledge and experience covered the full spectrum of child exploitation within the United States. This is achieved through their communication, training and their network of agents. One of the officers interviewed was an ICAC commander of a state. He/she collaborates with sixty-one other ICAC. Therefore, if any sort of child predator hacking of a webcam occurred within the United States, this commander would have been informed of it. Additionally, to ensure I covered all aspects of this crime, I interviewed local, state, and federal officers. Lastly, three of the five officers I interviewed contacted their task force members or other ICAC agents to prepare for my interview. Therefore, their responses cover an array of the spectrum of law enforcement's perspectives. However, this affected the results because it's only generalizable to law enforcement's perspectives within the United States. If this study were to be repeated, it would include interview data of law enforcement officials from around the world. This will allow us to better understand the true nature of this crime on a global scale. Just because it doesn't seem to occur within the United States does mean it will not occur in Europe, Asia, or Africa.

FUTURE IMPLICATIONS

Future research should gather data on possible victims of child predator hacking by conducting an anonymous survey of elementary, middle, high school students, and college students. In doing so, future studies can compare and contrasts the data of law enforcement's

perspectives to possible victim's perspectives, and even child predator's perspectives. This will allow future studies to paint a more accurate picture of child predator hacking. This will allow future studies to determine if this crime is in fact under-reported or if law enforcement detection rate is efficient. If under-reporting is the case, the data will not only help law enforcement better understand and combat this crime but it will also raise awareness and provide educational material.

Lastly, this study was restricted to the United States. Therefore, this study should be replicated in countries around the world to better understand law enforcement's perspectives of the hacking of minor's webcams. In doing so, we can better understand if and where this crime occurs.

Additionally, future research should interview intelligence agencies such as the National Security Agency as they too combat child exploitation within the cyberspace. However, they may withhold sensitive information regarding child exploitation within the cyberspace. Child predators and pedophiles have begun to use Tor and encryption which is where the NSA resides when securing national security. Lastly, future research should interview hackers in general. What do they know about the matter and is it a common crime to hack into somebody's webcam regardless if the motive is sextortion or just for fun? What is the latest talk among hackers? Do they attempt to fight this child exploitation? Do they know if it's commonly used for good, bad, or just for fun?

REFERNCES

Binford, W. (2015). A Global Survey of Country Efforts to Ensure Compensation for Child Pornography Victims. *Ohio State Journal Of Criminal Law*, 13(1), 37-65.

Botelho, G. (2013, September 27). Arrest in 'sextortion' case involving Miss Teen USA Cassidy Wolf - CNN.com. Retrieved November 8, 2015, from http://www.cnn.com/2013/09/26/justice/miss-teen-usa-sextortion/

CBS news. (2015, April 23). Baby monitor hacker delivers creepy message to child. Retrieved December 2, 2015, from http://www.cbsnews.com/news/baby-monitor-hacker-delivers-creepy-message-to-child/

CBS New York. (2015, April 21). Seen At 11: Cyber Spies Could Target Your Child Through A Baby Monitor. Retrieved January 07, 2016, from http://newyork.cbslocal.com/2015/04/21/seen-at-11-cyber-spies-could-target-your-child-through-a-baby-monitor/

Crewdson, J. (1998). *By Silence Betrayed: Sexual Abuse of Children in America*. Boston: Little Brown.

Department of Justice. (2015a, June 3). Child Pornography. Retrieved January 10, 2016, from https://www.justice.gov/criminal-ceos/child-pornography

Department of Justice. (2015b, July 6). Citizen's Guide To U.S. Federal Law On Child Pornography. Retrieved January 09, 2016, from https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography

Department of Justice, Homeland Security Announce Child Pornography File-Sharing Crackdown: Law Enforcement Initiative Targets Child Pornography Over Peer-to-Peer Networks. (2004).

Epiphaniou, G., French, T., & Maple, C. (2014). *The DarkWeb: Cyber-Security Intelligence Gathering Opportunities, Risks and Rewards. Journal Of Computing & Information Technology*, 21-30.

Federal Bureau of Investigation (FBI). (2010). Violent Crimes Against Children. Retrieved May 03, 2016, from https://www.fbi.gov/about-us/investigate/vc_majorthefts/cac

Georgia Bureau of Investigation (GBI). (2016). Child Exploitation And Computer Crimes Unit. Retrieved May 03, 2016, from http://investigative.gbi.georgia.gov/child-exploitation-and-computer-crimes-unit

Gross, D. (2013, August 14). Foul-mouthed hacker hijacks baby's monitor - CNN.com. Retrieved October 26, 2015, from http://www.cnn.com/2013/08/14/tech/web/hacked-baby-monitor/index.html

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. London and New York: Routledge.

Hout, M. V., & Bingham, T. (2013). 'Surfing the Silk Road': A study of users' experiences. International Journal Of Drug Policy, 24(6), 524-529.

Jewkes, Y., & Andrews, C. (2005). Policing the filth: The problems of investigating online child pornography in England and Wales. Policing & Society, 15(1), 42-62.

Krone, T. (2004). A typology of Online Child Pornography Offending:. *Trends & Issues in Crime and Criminal Justice*, (279).

Krone, T. (2005). International Police Operations Against Online Child Pornography. (cover story). Trends & Issues In Crime & Criminal Justice, (296), 1-6.

Lanaria, V. (2015). Here Are The Biggest Hacks And Data Breaches Of 2015: Ashley Madison,

OPM, Anthem And More. Retrieved January 02, 2016, from http://www.techtimes.com/articles/120040/20151229/here-are-the-biggest-hacks-and-data-breaches-of-2015-ashley-madison-opm-anthem-and-more.htm

Merdian, H. L., Curtis, C., Thakker, J., Wilson, N., & Boer, D. P. (2013). The three dimensions of online child pornography offending. Journal Of Sexual Aggression, 19(1), 121-132.

Miller, D. & Slater, D. (2001). The Internet: An Ethnographic Approach.

Muller, M. (2011). The guardians of innocence: A parent's guide to protecting children from pornography (pp. 81-83). Springville, Utah: Horizon.

Newton, M. (2008). Won't Somebody Think of the Adults? 3-4.

Pitarro, M. (2007). Cyber stalking: an analysis of online harassment and intimidation. 1(2): 180-197).

Prichard, J., Spiranovic, C., Watters, P., & Lueg, C. (2013). Young people, child pornography, and subcultural norms on the Internet. Journal Of The American Society For Information Science & Technology, 64(5), 992-1000.

Office of Juvenile Justice and Delinquency Prevention. (2016). Program Study. Retrieved May 03, 2016, from http://www.ojjdp.gov/programs/ProgSummary.asp?pi=3

Sexual Exploitation of Children Over The Internet. (2007, January). Retrieved January 03, 2016, from http://burgess.house.gov/uploadedfiles/subcommittee on oversight and investigations report on the sexual exploitation of children over the internet.doc

Sterling, B. (1992). *The hacker crackdown: Law and disorder on the electronic frontier*. New York: Bantam Books.

Stump, S. (2013, September 27). Miss Teen USA has 'mixed emotions' after arrest of 'sextortion'

suspect. Retrieved November 7, 2015, from http://www.today.com/news/miss-teen-usa-has-mixed-emotions-after-arrest-sextortion-suspect-8C11275299

Tate, T. (1990). *Child Pornography: An Investigation.* London: Methuen.

Tian, J., Qi, W., & Liu, X. (2011). Retrieving Deep Web Data Through Mult-Attributes Interfaces With Structured Queries. International Journal Of Software Engineering & Knowledge Engineering, 21(4), 523-542.

Tor. (n.d.). Retrieved March 28, 2015, from https://www.torproject.org/about/overview.html.en

Tor. (n.d.). Retrieved March 28, 2015, from https://www.torproject.org/docs/faq.html.en

Tyler, R., & Stone, L. E. (1985). Child pornography: Perpetuating the sexual victimization of children. *Child Abuse & Neglect*, 9(3), 313-318.

Wortley, R., & Smallbone, S. (2012). Child Pornography on the Internet: Problem-Oriented Guides for Police: Problem-Specific Guides Series: No. 41. *PsycEXTRA Dataset*.