CYBERCRIME:

LOCAL POLICE INVOLVEMENT IN CYBERCRIME

By

JAIR TYRELL PARHAM

_____

A Thesis Submitted to The Honors College

In Partial Fulfillment of the Bachelors degree
With Honors in

Criminal Justice

THE UNIVERSITY OF ARIZONA

M A Y 2 0 2 0

Approved by:

_____

Anne E. Boustead, JD PhD
School of Government and Public Policy

Abstract

Cybercrime is a crime that was created alongside the creation of the Internet. Both the Internet and cybercrime have grown at a rapid rate since their conception, but the response to cybercrime has lagged behind. Even though cybercrime has increased, efforts to police it have not followed suit and has led cybercrime to go unchecked at the local level, leaving policing efforts to be mostly on the federal level. This is partially because cybercrime has been plagued with not having a definitive definition, which causes confusion as to what is and is not a cybercrime. This paper will explore if cybercrime is under investigated, what barriers there are to cybercrime being investigated, and what could be done to get through these barriers of investigation.

I. **Introduction**

Cybercrime is a relatively new phenomenon that has become increasingly relevant because of the rapid growth of the internet. Due to how new cybercrime is, many scholars and law enforcement agencies have struggled to come up with a definition of cybercrime. According to the International Association of Chiefs of Police (IACP) and the FBI, “Cybercrime has an expansive definition that includes any crime conducted via the Internet, network or digital device. Capturing digital evidence, such as that found on cellular phones, GPS devices, computers, tablets and network servers, is crucial to investigating and solving cybercrimes” (Federal Bureau of Investigations). Examples of cybercrimes include identity theft using phishing to gain personal information, attacks using viruses or malware to gain information or to damage a website or computer, cyberstalking, and distribution of prohibited content ranging from classified information to child pornography.

After defining cybercrime, the next step would be to find out who exactly commits cybercrime. Because of the evolving nature of the internet, “[t]here is no static "profile" for a cybercriminal, as they take on many forms in their effort to steal, cheat, and destroy.” (Pinguelo 121). The internet is complicated and intangible, which allows for an immense amount of anonymity. With this anonymity, anybody with internet access could potentially be a criminal or a victim. Additionally, the level of expertise involved in solving many cybercrimes and the inter-jurisdictional nature of cybercrime causes many cases to be sent to the FBI. Generally, cybercrime is seen as a problem for the federal government, and the federal government puts the most resources into investigating it. There are many federally funded organizations and agencies that focus on cybercrime,

including the Internet Crime Complaint Center, Cyber Action Team, and National Cyber Forensics & Training Alliance (Federal Bureau of Investigations). While there are state and local police departments that do investigate cybercrime, their role is much smaller in comparison to efforts taken by the federal government due to having less resources available.

The prominence of the federal role in investigating cybercrimes raises the issue of what role local police departments should play in regards to cybercrime. In general, while few argue that local cybercrime units are bad or not wanted, there isn't necessarily an outcry for units to be added. With a lack of onus put on local police departments, some cybercrimes fall under the radar as the FBI can't handle everything on their own. This in particular leads to "[s]tructural and cultural limitations upon traditional policing agencies have resulted in a security deficit in the online world. This security deficit means that many crimes occurring online go unreported or are ignored by law enforcement" (Huey and Nhan 82). We don't know how many people are being victimized, but this doesn't mean there isn't a threat and the potential of crime should be taken seriously. This issue presents itself in non-cybercrimes as well, and has been referred to as the "Dark Figure of Crime" (Doorewaard 1). There inevitably are a large number of crimes that aren't reported; however, when cybercrimes go unreported, it is less likely that it will be observed in other ways due to the technical knowledge needed to be able to uncover specific evidence.

Given how complicated cybercrime is, police departments tend to steer away from policing even lower level cybercrimes. As a result, local police departments rely heavily on the federal government to investigate cybercrimes like cyber-related ID theft,

online predators (distribution of child pornography), spam, phishing, malware, cyberbullying, and compromised local business networks (Federal Bureau of Investigations). However, with how fast cybercrime is evolving and expanding, it is quickly reaching a state where the FBI can't handle everything on their own. For example, it could be said that FBI involvement in cyber harassment is a misuse of federal cyber investigation resources, as it is usually a local community issue that could be handled by the police. Other crimes local police could handle are cyber-related theft, spam, and phishing. There is a tendency to think that cyber criminals are notorious hackers that threaten the nation's security with a few strokes of a keyboard, but even if threats to national cybersecurity and hacks aimed at large private business are beyond the scope of local law enforcement, it doesn't mean that local police departments don't have a role to play in making the internet a safer place.

In this paper, I argue that local police should be involved in policing cybercrimes, and specifically that many more local police departments that should have cybercrime units. In the next section, I provide background information on cybercrime, and present an analysis of current cybercrime units in local police departments. I then review why local police need to be involved in the world of cybercrime investigations. In the fourth section, I identify potential barriers that exist to implementing cyber units. In section five, I explore how to potentially overcome those barriers. Finally, I present some concluding arguments and policy recommendations.

II. Background

A. Literature Review

To understand the issue at hand and the arguments that will be presented, it is crucial to review the previously existing literature on the topic of policing cybercrime. According to this literature, “[m]ost attention and initiatives focused on tackling cybercrime have focused upon reducing activities such as child pornography and abuse” (Nykodym 64). Child safety/endangerment is a key aspect of a large majority of police departments. Even if a department doesn’t have a cybercrime unit, they usually have one of their other units investigating child pornography or they have suggestions on how to keep children safe on the internet. Additionally, most police departments give out tips through their website to keep children safe on the internet. A lot of local police department websites also give tips on how to deal with cyberbullying, as that is one of the most prevalent concerns related to children on the internet.

Other commonly investigated cybercrimes are fraud and identity theft. These two crimes are usually investigated by a police department's economic crimes or financial crimes unit. Fraud and counterfeiting investigations being conducted by those specific units makes a lot of sense as they are primarily crimes that deal with money, but identity theft can be more than just a financial crime.

Officers and heads of police departments often believe they don’t have the resources necessary to investigate cybercrimes due to the possible geographic diversity of perpetrators. The internet is expansive, and a criminal committing a crime in the US could be in China, England, or anywhere. However, perpetrators of cybercrimes can also be closer to home. “In fact, data from the Internet Crime Complaint Center (2010) suggests that between 20 and 35 percent of reports of internet based fraud from ten states have both offenders and victims living in the same state. In addition, juveniles are

likely to experience cyberbullying or online harassment from individuals they know in the real world as friends or associates" (Bossler and Holt 167). This suggests that local police could potentially investigate cybercrimes without needing aid from the FBI, although police departments may have to reach out to other departments in their state if they want to catch the perpetrator.

Additionally, some have argued that local police don't have adequate training or technical expertise to investigate cybercrimes. Willits and Nowacki state that, "[p]opular opinion suggests that police are not well prepared to address cybercrime. Dozens of articles are published in major newspapers and magazines each year with titles like 'Police clueless on web crime, says chief' and 'Local level police ill-equipped for cybercrimes, cyber threats'" (Willits and Nowacki 107). Citizens think that local police are not a reliable resource in cybercrime investigations, so citizens often rely on the FBI for their cybercrime needs.

However, relying only on the FBI to address cybercrime just makes things more complicated by creating a backlog as the FBI doesn't have time to be handling the large amount of identity theft cases that occur. This leads to cybercrimes either being unsolved or going unreported as victims don't think they will get help from law enforcement. The lack of local police involvement in cybercrime leads the public to underestimate their capabilities. "[I]n fact, Wall (2008) suggests that public perceptions of cybercrime and cyberpolicing are often erroneous, resulting in a reassurance gap between the public's risk for cybercrime victimization and actual cybercrime activity" (Willits and Nowacki 107). The public's false sense of cybersecurity just makes the job of the FBI more difficult. This causes the public to take more online risks as they go to

unsecure websites and unknowingly giving away information about themselves leads to more people becoming compromised by cyberattacks. In turn, this causes more outrage when the FBI can't handle the large number of cybercrime investigations.

Additionally, patrol officers often don't believe they should be investigating cybercrimes. "[B]ased on the data from a study done on the Charlotte-Mecklenburg Police Department and the Savannah-Chatham Metropolitan police department 39 percent of patrol officers believed that local law enforcement should not be the primary investigator of cybercrime," although 40% of the officers surveyed had no opinion (Bossler and Holt 171). This perception may be based on lack of cybercrime training and experience at the local level: only 1% of the officers actually had training in cybercrime cases, while only 16% of officers had actually handled a cyber case and, of those, 16% the case was over 2 years old (Bossler and Holt 171). While it doesn't appear that patrol officers are against learning how to handle cyber cases properly, they are quite adamant that specialized units should handle those cases, as 72% of police officers surveyed said specialized units should handle them. Additionally, 63% of the officers surveyed believed that cybercrime investigations did not drain valuable resources that should be spent investigating other crimes (Bossler and Holt 174).

Cybercrime is on the increase, creating a need for additional investigators to adapt to handle the case load. "[F]rom 2007 to 2012, the FBI's Internet Crime Complaint Center (IC3) reported a 40% increase in cybercrime complaints. The increased concern about crime, increased reporting of cybercrime, and lack of confidence that the police can manage cybercrime create tremendous pressure for police agencies to adapt their enforcement strategies to these types of offenses" (Willits and Nowacki 107). The

increase in reported complaints obviously doesn't tell the whole story, as not every crime is reported, meaning that there are plenty of cybercrimes either not reported or not noticed. So if the amount of complaints have gone up by nearly half in just 5 years the amount of actual cybercrimes have likely increased much more.

As cybercrime continues to evolve, it has proven difficult to find solid ways to police cybercrime. There has been a model created by Paul Hunton that describes steps to investigate cybercrimes:

> The Cybercrime Execution Stack (see Fig. 1) is aimed at providing an investigator with an objective means of identifying and gaining an understanding of the wider technical and criminal characteristics of cybercrime. The model defines the abstract entities that will directly or indirectly occur in the commission of an offence or other illicit cyber behaviours. In the context of a practical investigation, the model will allow an investigator to consider each element in turn and gain a broader understanding of a potential offence." (Hunton 62)

The Cybercrime Execution Stack was created to standardize cybercrime investigations. The model is also "intended to facilitate increased knowledge sharing and communication between the many investigative roles and varying specialist disciplines necessary when conducting complex technical cyber investigations" (Hunton). The Cybercrime Execution Stack can be compared to criminal intent and Modus Operandi or M.O. (habits of crime) combined, as it takes into account intent and how the crime is committed. Because understanding crime leads to solving crime, Hunton suggests pairing this tool with the model Stages of Cybercrime Investigation, these stages consist of "modelling, assessment, impact/risk, planning, tools, action, and

outcome" (Hunton 63). The combination of these two models is meant to link law enforcement with specialist services, it is also meant to increase communication across cyber investigations. This came out in 2011, but it doesn't seem that it has caught on in either American literature or in American cybercrime investigations. Key components that the models encourage are large amounts of communication between many different organizations and sharing knowledge due to how complex a single cybercrime could possibly be.

B. Data of U.S. cities with and without Cybercrime units

To look at how local police departments are currently investigating cybercrimes, I took a random sample of 1,000 of the largest cities in America and conducted web research to determine whether each city's police department had a cybercrime unit, how the unit was described, the list of crimes the unit investigated, and the services provided by the unit.

I found that only 8 out of the 100 cities I studied had a dedicated cybercrime unit listed on their website. For example, the McAllen Police Department in Texas has a unit called the Forensic Evidence Acquisition and Recovery Unit (F.E.A.R), "responsible for the extraction and recovery of electronic evidence using various forensic electronic tools and softwares. The unit is also responsible for the investigation of internet based crimes" (McAllen Police Department). California's Long Beach Police Department has a Computer Crimes Detail, which "investigates cases where a computer is the target of a crime or an instrument used in the commission or furtherance of a crime. The Computer Crimes Detail is frequently called on to assist other investigative units, as well as federal

and local law enforcement agencies with the seizure and processing of computer-related evidence" (Long Beach Police Department).

The departments with cybercrime units vary in terms of what crimes they actually investigate. Some specify specific crimes investigated by their unit, such as network intrusion, theft of data, theft of trade secrets, dissemination of malicious code software piracy and criminal activity committed via the Internet, including sexual exploitation of children, fraud, identity theft, cyber stalking and terrorist threats. Other departments just say they investigate internet based crimes or cybercrimes.

Additionally, out of the 100 cities surveyed, 15 had cyber forensics units. For example, the Fort Wayne (Indiana) Police Department has the Digital Forensics department that "conducts the examination of any electronic media evidence and analysis. This is typically, but not limited to: computer hard drives, memory cards, CDs, DVD's, cell phones, digital cameras, and video surveillance systems. The Unit also performs cell phone records analysis" (Fort Wayne Police Department). The Santa Ana Police department in California has a Computer Forensics Unit (CFU) "that assists patrol officers and detectives with seizing and examining computers, cellular telephones, digital cameras, and other items containing digital evidence. In 2009, the CFU joined the FBI Regional Computer Forensics Laboratory, which has been involved in over a thousand cases throughout Orange County. Some examinations uncovered the only physical evidence in a case, and sometimes led to identifying additional suspects and crimes. The RCFL also provides digital evidence training and assists with search warrant preparation and service" (Santa Ana Police Department)

Local cybercrime units typically have other functions that are similar to traditional policing, making cyber units versatile in their skillset. For example, the Riverside County Sheriff's Department's cybercrime unit C.A.T.C.H. also helps investigate homicides. The Virginia Beach Police Department's Economic Crimes Unit Investigates computer crimes and "in 2018 had one detective assigned to the FBI Cyber-Crimes Task Force" (Virginia Beach Police Department). The Sioux City Police Department's Property Crimes Unit, "led by Sergeant Tyler Hartwell, routinely investigates internet crimes, burglary, felony theft, identity theft, forgery, arson, and criminal mischief. It also provides polygraph and computer forensic services" (Sioux City Police Department). The Columbia Police Department partners with the United States Secret Service (USSS) "to investigate cyber and financial crimes such as computer hacking and corporate embezzlement. TFOs (Task Force Officers) also work with Secret Service Agents to identify persons involved in the production and distribution of counterfeit currency and merchandise. In addition, TFOs conduct forensic examinations of cell phones and computers involved in criminal cases" (Columbia Police Department).

Additionally, I found that only two of the eight departments have both a cybercrimes investigation unit and a cyber forensics unit. This is important because only two departments have the means to analyze any cyber related forensics found by either the cybercrime investigations or the non-cybercrime investigations making any investigations with cyber related forensics more difficult. The data collection also found that 63 out of 100 police departments had some mention of identity theft: either how to prevent it, where to go for help, or discussion of a unit that investigated it. This leads to the notion that there is a need for police departments to investigate this crime.

C. Case Studies of Police Departments with Cyber Units

Along with exploring 100 different police departments with and without cyber units, three police departments with cyber units were chosen to be studied further in depth. This was done to see how effective these units are and to see what kind of cities had cyber units. Police departments were selected to serve as case studies based on two criteria: the population size of the city and number of officers in the department. These criteria are to see how different sized departments implement cyber units and what role they play in the department. This will give a better understanding of how different departments with different characteristics can implement a cyber unit and the roles that cyber units can play in a local police department.

1. Charlotte-Mecklenburg Police Department

Charlotte-Mecklenburg Police Department (CMPD) spans not only the city of Charlotte (pop. 841,611), but also all of Mecklenburg county - a total population of 1,054,314 people. Mecklenburg county is slightly above the U.S. average in terms of poverty and income. Mecklenburg county has a per capita income of $37,298, which is about $5,000 more than the United States per capita income. Mecklenburg county has about a 12.7% poverty rate while the United States poverty rate is at 13.1%. This jurisdiction has about 36,000 property crimes per year, with larceny heading this category at 27,000 cases, and about 6,900 violent crimes per year.

The CMPD has about 1,900 sworn police officers and has been combined to serve the city of Charlotte and Mecklenburg county for 24 years. The current chief of

police has been in office since 2015; before he became the chief, he was in charge of the Computer technology services bureau or the CTS. He has been a leader in making his police department as technologically advanced as possible. Every CMPD patrol officer has body cameras to ensure safety of not only officers, but civilians as well.

Per the CMPD website, the cybercrimes unit was created to “take a proactive approach to crime via Internet before it becomes a major problem”. The leading supervisor of this unit is Sergeant Melissa Kiefer and she has her unit focusing on crimes including “identity-theft through the Internet, computer hacking, theft of intellectual property, Internet fraud, credit card abuse, and Internet child exploitation (solicitation of a child or child pornography) (CMPD).” Due to the nature of the crimes that this unit has to deal with, they have a strong partnership with organizations outside of their police department, including the FBI, IRS Criminal Investigations Division, the U.S. Customs Service, U.S. Secret Service, U.S Attorney General's Office, the North Carolina Attorney General's Office and other local organizations in matters of cybercrime. The CMPD’s cybercrime unit’s involvement with these organizations means they put a lot of emphasis on communication, which is important when investigating cybercrimes.

The CMPD cybercrimes unit is part of the special victims unit inside of the investigative services division. The cybercrimes unit works closely with the department's financial crimes and crimes against children units as the cybercrimes unit takes care of the internet aspect of these units. The CMPD cybercrimes unit’s main function is to be a proactive crime prevention unit. Through their website they have many warnings and links to help keep citizens digital information safe from criminals.

The services provided by the CMPD cybercrimes unit appear to benefit the community. This is because their cybercrimes unit allows them to put in a proactive model towards policing, which is something that many police departments have been trying to implement into their way of policing for decades. In a sense it allows for the chief of police to see not only how police departments can deal with cybercrimes, but how they can implement proactive policing into other areas of the police department.

The experience of the CMPD shows that cybercrime units do not have to divert time and resources away from investigating other more dangerous crimes. A survey done in the CMPD shows that 63% “of the officers believed that cybercrime investigations did not drain valuable resources that should be spent investigating other crimes” (Bossler and Holt 174). However, only 16% of those (from CMPD) surveyed by Bossler and Holt had actually received formal cybercrime training, meaning that the majority of officers don’t know how much time is needed to be qualified to investigate cybercrime. To increase this percent, the unit would need to hire detectives and officers that already had cybercrime training or send them away to get cybercrime training, which would require additional resources.

Other police departments could also learn from the CMPD that the best way to handle cybercrime is to be proactive in policing. The chief of the CMPD, Kerr Putney, has a background in technology so “he helped prioritize and develop plans to enhance and maintain the technological advances of the organization for which the department has become a model around the country” (CMPD). It may take having a leader such as Putney, who has a background in technology, for other departments to implement cyber units. Other departments can also learn from CMPD's partnerships with organizations

like the FBI, Secret Service, and IRS in effort to help smooth the process along for the cybercrimes unit. These partnerships widen the CMPD's reach and makes their cybercrime unit more practical since they have more resources on a grand scale to work with.

However, not every department in the U.S. can realistically move resources into cybercrime. CMPD's approach to cybercrime could be impractical for smaller police departments as the CMPD is one of the biggest departments in the U.S. with over 1,900 sworn officers. Smaller police departments may not have enough resources to send detectives to training, or they may not be able to spare detectives in terms of manpower. The CMPD's partnership with federal agencies also may be difficult for other police departments to obtain as their cities size may get them overlooked.

2. McAllen PD

The city of McAllen is one of the closest cities to the Mexican border in Texas. It covers 58.3 square miles and has about 141,000 residents. Due to being so close to the border, about 76% of the population speaks Spanish. The per capita income in McAllen is about $22,000, which is $10,000 less than the United States per capita income. The poverty rate in McAllen is about 25%, nearly 13% higher than the United States poverty rate. For people in McAllen, the educational attainment for graduating high school is about 75%, which is 12% lower than the national average. McAllen is a highly poverty stricken area where employment is hard to come by.

McAllen Police Department's most prioritized and prevalent crime is drug trafficking as the border is so close to the city. In 2019, the McAllen PD seized about

266 lbs. of marijuana, 11 lbs. cocaine, and 3 lbs. of Methamphetamines. Being a border city, another crime that the police department has to be well equipped for is human trafficking crimes as well, which are investigated by their Special Investigations Unit. Drugs are the primary concern of this police department, but they also investigate many violent crimes as well. According to the 2019 McAllen Uniform Crime Reports (UCR), property crime dropped 6%, while violent crime increased 14% from 2018 to 2019. Also according to their UCR, "McAllen PD has 298 sworn officers, which puts them at ... 2 officers per 1000 population".

McAllen's cyber unit is called the Forensic Evidence Acquisition and Recovery Unit or F.E.A.R. According to their website, "[t]he Forensic Evidence Acquisition and Recovery Unit is responsible for the extraction and recovery of electronic evidence using various forensic electronic tools and softwares… [as well as] the investigation of internet based crimes". F.E.A.R's primary duty is to extract information electronic evidence, but they are more than just a cyber forensics unit as they also investigate internet based crimes.

F.E.A.R. gets help from the department's FBI task force: officers who are given FBI training and act as an intermediary between the FBI and McAllen PD. These officers tend to do most of the investigating, while F.E.A.R. does the extraction. F.E.A.R. also gets help from other departments, most inclusively the support division as this division has an identity theft investigator. F.E.A.R. appears to be heavily reliant on other entities to help get investigations done, perhaps due to the fact that the unit was initially set up to be a supportive unit. However, with the increase in cybercrimes, the unit has become more investigative.

One potential criticism of this unit is that it takes resources away from investigating trafficking, either drug or human. Considering the proximity of McAllen to Mexico, it seems that reinforcing such an important unit such as their SIU would take priority over F.E.A.R. The benefits of the unit appear to include tracking deals made on the internet.

A lesson that could be learned from McAllen's approach is that combining cyber forensics and cyber investigations could save money and resources. This approach could also be used by smaller police departments that don't have the means to create both as separate units. It also causes there to be less miscommunications as information doesn't have to travel between different units. Combining cyber investigations and cyber forensics is an easy way to simplify the chain of information and considering how both units would be communicating with each other on a regular basis if separate, the combining of the both units could be a positive thing for other departments.

The lessons learned from McAllen's cyber unit would apply to Police Departments that lack funds, but see enough cyber complaints to warrant a cyber unit. Police departments with a large minority base and low funds can apply McAllen's more cost effective approach to cybercrime. McAllen also has a decent population, but not too big so cities with around 70,000 to 200,000 people could probably implement this model depending on how well off economically the people in the city are.

3. Perth Amboy Police Department

Perth Amboy is a small city in New Jersey with a population of 51,832 with about 76% Spanish speaking residents. Perth Amboy covers about 4.7 square miles meaning that buildings and housing are in close proximity with each other. The per capita income in Perth Amboy is about 21,000, which is about 11,000 dollars less than the US national average. The city also has an 18.3% poverty rate, which is high in comparison to the US national average of 11.7. In terms of educational attainment, Perth Amboy has a 70.4% high school graduation rate, which is 17.3% lower than the graduation rate of the United States. It appears that the most common crime in Perth Amboy is property crime, more specifically theft.

The Perth Amboy Police Department (PAPD) is a small police department with only 135 sworn-in officers so there is about 1 officer for every 384 people. PAPD has four divisions: the Support Services division, the Operations Division, the Investigative Division, and the Office of Professional Standards. The investigative division is primarily responsible for investigating crimes, and is composed of an ID Bureau, Special Investigation Bureau, Juvenile Aid Bureau and a Community Service Unit.

Perth Amboy's cyber unit, in the investigative division, deals with a variety of cybercrimes, including possession and distribution of child pornography, cyber related fraud, cyber related identity theft. The cyber unit has a close relationship with the FBI due to being close vicinity to the headquarters in Washington, D.C.. This close relationship allows for more access to cybercrime assets, whether it be training or simply having access to FBI resources to investigate cybercrime. The most common crime that Perth Amboy's cybercrime unit investigates is child pornography. This cyber unit seems to be quite active in investigating cybercrime, as there are plenty of news

articles about the cyber unit and its successes. For example, “the Perth Amboy Police Department announced today that a Perth Amboy man has been charged with using fraudulent identities to steal expensive film equipment from companies in three different states” showing that the cyber unit is capable of working with multiple departments across many states (Middlesex County New Jersey). Another example is, “Bergen County Prosecutor Dennis Calo announced the arrest of JIMMY RIVERA (DOB: 4/4/1976; married; and employed as a print shop worker) of 502 Compton Avenue, Perth Amboy, NJ on charges of Possession and Distribution of Child Pornography” (Bergen County Prosecutor’s Office). In this example, Perth Amboy’s cyber unit assisted the arresting department and also shows that this unit investigates a variety of cybercrimes.

PAPD’s cyber unit appears to be active and on top of their target cybercrimes. It could be possible that they simply identify and investigate crimes that have occurred, but that these efforts have dissuaded others from committing cybercrimes as their cyber unit is very active in the community. On the other hand, a cybercrime unit could be potentially costing resources that could be put into investigating property crimes.

Small communities looking to implement cyber units could learn from Perth Amboy. Perth Amboy is the smallest city from the 100 cities surveyed with a cyber unit with a population of 51,000, so many cities with similar populations can try to emulate what Perth Amboy is doing. Perth Amboy shows that small cities can also use cyber units, as they are having success with their unit and it is not going to waste. Perth Amboy’s experience also shows what a city of that size would need to do to have a successful cyber unit.

A small city could look to the details of their crime problem to determine if a cyber unit could be successful or even useful. If there isn't a demand for it due to small amounts of cybercrimes, then they could do without and rely on a nearby city for help. Perth Amboy for example, analyzed their needs and determined that the amount of cybercrime occurring warranted the creation of a cybercrime unit, even when considering the city's small size. Perth Amboy's proximity to FBI headquarters allows for easy access to cybercrime materials and learning. Other small cities across the country may not be as lucky and won't be able to have such easy access to the leader in cyber investigations.

One of the best things Perth Amboy has going for them is how close they are to FBI headquarters. When a police department is deciding on whether or not to add a cyber unit, they should definitely think about how close their local FBI station is to them. Since Perth Amboy is so close to the FBI, they can send officers to receive training without expending much on travel. Other police departments will also have to think about their proximity to training areas for officers, or they'll have to hire officers who already have cyber investigation experience.

III. Involvement of Local Police in Cybercrime

Many doubt the need for local police to be involved in cybercrime. In this section, I explore the question of local cybercrime units, explaining how local cybercrime investigations are becoming more feasible and the importance of local cyber investigations for helping out the FBI.

A. Is it worth it to have local cybercrime units?

For police departments the worth of a unit is an important factor when adding a new unit or keeping a unit in the department. When it comes to cybercrime, it may be hard for chiefs of police to justify expenditures on this relatively new type of crime. Bossler and Holt (2012) suggest that it is easy for officers to write cybercrime off as something they don't need to deal with because officers don't think they have adequate training and don't think it's a priority for upper management. However, just because upper management might not take it seriously, doesn't mean it shouldn't be taken seriously by local police. Many cybercrimes can be investigated on the local level. As stated earlier around 20 to 35% of cybercrimes both the victim and the perpetrator are in the same state. On the other hand, these figures only deal with reported cybercrimes, so it may be hard to judge whether there is enough cybercrime going on to warrant local response.

One reason cybercrime should be investigated on a local level is so the justice system can begin acting proactively and get in front of cybercrime instead of letting it develop to the point where police can only react to it. Policing on the local level can add an extra set of eyes to cyber investigations and would increase the manpower put into preventing cybercrime rather than just having the FBI only in charge of the policing. Some might say it is not practical for some small 80 person police department in Montana to have a cyber unit, but "[c]ybercrime is an ever evolving threat, and an agency can't keep ahead to adequately protect themselves without somebody dedicated to the task" anyone at any time can end up being a victim of cybercrime (DOJ). Therefore, it seems practical for departments to take the initiative and prepare to

investigate cybercrimes, protecting both themselves and the community. Most often police departments take a reactive approach to crimes, but departments have an opportunity to not only take preventative measures for their own safety but also set standards for investigating cybercrimes. This could be even more advantageous as new generations are growing up in a cyber-centric environment, making easier learning curves for training new police recruits.

Additionally, having local police departments involved in cybercrime makes reporting these crimes more accessible to the public. If they cannot go to the local police station, citizens have to go to the FBI website to report a cybercrime. This lack of human interaction causes less people to report their cybercrime because they don't think their crime will be investigated. If local police are conducting cybercrime investigations, not only will there be more cybercrimes reported overall, but also fewer cybercrimes will be reported to the FBI. This means that the FBI will have more opportunities to deal with national security and larger scale cybercrimes.

Every police department is different, but from some research there are plenty of secondary units that could be replaced with a cybercrime unit. A main point of opposition to having cybercrime units is that they are just not an essential part of a police department, but police departments engage in other activities that could be handled by cooperation with larger agencies. When conducting my analysis of local cybercrime units, I also found that local police departments often had other interesting units as well. For example, there is a robotics unit in the West Covina Police Department, which can be used to defuse bombs or go into a seemingly unsafe environment for a human. "These units are for 'high-risk' calls, involving warrants, the

SWAT team or barricaded suspects, and are deployed only “every two to three months, depending on circumstances” (Mendelson). It may be practical to replace a unit such as this in a police department of 97 sworn officers with a unit that can be shared across several agencies, freeing up resources to use for cybercrime investigations.

B. Cyberpolicing is becoming more necessary and more feasible

As cybercrime evolves, more police departments can be involved in investigating cybercrimes. It may become less expensive to train people, as departments can look to recruit individuals with technological skills as it is becoming more common to have such skills. People born in the late 1990s are starting to graduate college and go into their careers. This means that candidates for officers are going to have more experience with the internet and electronics, because they were born and raised in an era where both were prevalent. These candidates will not only be more willing to deal with electronics and the internet, but they won’t need training on basic things because they grew up with and learned how to use them in college or high school.

A change in generation also means a change in way things can be done, with these new kinds of recruits new baselines can be set for scouting individuals with aptitude for investigating cybercrime. These baselines will gradually bleed into many different areas of a department who are looking for individuals who can investigate cybercrimes. The skills of officers that do not have cybercrime training will still be useful, as there are still plenty of crimes that don’t contain any cybercrime. Although eventually, cyber components will begin to trickle into many different types of crimes.

Furthermore, as technology and people advance, it will become more important to have local law enforcement trained in cybercrime. Taking this advancement into account, the justice system has a unique opportunity to prepare for an emerging crime problem by having potential preventative measures put in plus through policing. Cybercrime is not disappearing anytime soon. Due to this, police departments should look to evolve alongside cybercrime.

C. Local policing of cybercrimes will reduce burden on federal law enforcement

As of right now the major player in the investigation of cybercrimes is the FBI, but they are being stretched thin as stated by Dolliver:

> Countries can no longer rely solely on more reactive methods. Traditionally, threats to national borders lead to the concentration of law enforcement agents or military personnel at border crossings and points of entry. Similarly, many criminal threats are met with the deployment of extra police in a neighborhood. Now, given the access and ease of the Internet, every person who has a computer, a Smartphone, or any other device that can connect to the Internet is a potential point of entry into a country. (Dolliver).

If local police do their part to limit cybercrime then the FBI will be able to expand the services they provide and possibly use resources to find better preventative measures.

One argument against local level policing of cybercrime is the lack of reporting to law enforcement as “[a]lmost two-thirds (63.5 percent) of the officers agreed that most cybercrimes go unreported to law enforcement”, which is why the majority of cybercrimes are investigated by the FBI (Bossler and Holt 173). As police departments

think there isn't a need for them to investigate or think they don't have the ability to investigate, it leaves the FBI to investigate smaller cybercrimes. This is dangerous though, because it uses FBI resources that should be focused on national security level investigations or big business affected by cybercrime. The lack of local police investigations of cybercrime puts a large burden on the FBI.

The dark figure of crime is crime that goes unreported to law enforcement and is only known between the victim and the perpetrator (Doorewaard 1). When you factor the dark figure of crime to the equation, that creates even more possibilities. With the potential amount of unknown criminal activity, the FBI has to not only worry about small-scale cybercrime, but also cybercrimes that can affect the security of the entire United States. Cybercrime is "asymmetrical – in that one person or small group can wreak as much damage as it once took an entire army to cause. What is more, the offender does not have to be physically anywhere near the victim" with this known wouldn't it make sense to have local police handle crimes like cyberbullying, spam, phishing, and attacks on local businesses (Dolliver). When cybercrimes are referred to the FBI, many civilians may believe that either their incident isn't worth that amount of time or isn't that serious to involve the FBI. If local police departments were more willing to take cybercrime complaints, then it is possible that more people would report cybercrime.

Once it becomes clear that local law enforcement has a role to play in investigating cybercrimes, the next step is to talk about what types of cybercrime should be investigated on the local level. It is obvious that a local police department can't stop a DDOS attack on the White House or any other terrorist related cyber-activity or terrorist related activity in general, but they can do the little things. For example, local

law enforcement could investigate cyberstalking, phishing, spam, internet related identity theft, and attacks on local businesses. These crimes have the highest rate (excluding identity theft) of having the victim and the perpetrator be in the same state.

Nobody expects police departments to be able to eradicate cybercrime entirely, but as stated before this is a rare opportunity for the justice system to explore whether proactive policing of cybercrime is effective. The theory of proactive policing can truly be put in place with a series of crimes that are still growing.

IV. Barriers to Local Investigation of Cybercrime

With all things, there are obstacles to implementing local involvement in cybercrime investigations. In this section, I outline 7 barriers to having local police involved with cybercrime. The 7 barriers are difficulties with training, lack of exposure, no clear goal/definition, cybercrime is on a global scale, victims and perpetrators are faceless, cost, and pressure to produce results.

A. Training

The first barrier is training: either the training given isn't adequate or police officers do not have the capacity to take on another responsibility. It isn't easy to train people to deal with cybercrime. Officers may not want to deal with cyber-related events if they have no training. "[T]he level of skills and training within units is often not sufficient to address the nature and growing complexities of investigating cyber-crime" (Harkin). Cybercrime investigation skills are not easy concepts to teach or learn, and it takes certain skills and knowledge such as "technical aptitude, digital comprehension,

and analytical talents" to be able to recognize these crimes (Ec-Council). This leads to opposition in having it be added to the already full lists of activities undertaken by officers and departments.

Opposition to cybercrime being implemented into local police departments is real. "When asked if local cybercrime should be primarily investigated by local law enforcement, only 18.3 percent of the officers agreed" (Bossler and Holt 171). This opposition may be because officers don't believe they have the capacity or the training to be able to police cybercrime. As said before, training isn't easy and takes special qualifications to be able to police cybercrimes. Additionally, this training can be difficult and costly to obtain. Currently employed officers would have to take time out of their schedules to go to seminars. Depending on the police department they might not have enough officers to spare so they could send some to a training out-of-state or at the closest FBI office. Not only is training hard, but training also requires departments to lose their employees for a certain amount of time.

B. Lack of exposure

The next barrier is a lack of exposure to cybercrime for police officers, who may not be aware what policing cybercrime entails. So police officers not trained to deal with cybercrime may be less able to help victims. "The respondents estimated that 11 percent of the officers in their department had previously worked on a cybercrime case" (Bossler and Holt 171). As Bossler and Holt conducted their study in a police department with one of the biggest cybercrime units in the U.S., so we can expect the amount of officers in other departments without experience with cybercrime to be

substantial. If one of the more cyber capable departments has such a low rate of exposure for the officers, then the majority of police departments may either have a similar rate or possibly an even lower rate.

Lack of knowledge about cybercrime may reduce public confidence in police. “Cyber-crime is one of the few areas where civilians are unquestionably more likely to have much greater expertise than traditional police and this was widely recognized by our research participants.” (Harkin 530) This leads to lack of trust in police, and when this happens crimes may go unreported because people either think local police will be unable to investigate their crime or the FBI will not have the capacity to investigate their crime. If the public doesn’t trust in the police to investigate cybercrime, it may cause cyber-vigilantism where victims may look to find their own solution to their problem and this could lead to further problems. Once we have civilians on the internet trying to solve their own problems they might end up making the situation worse for themselves and compromise more of their information doing so.

With how common cybercrime is becoming it simply may not be possible for departments to turn a blind eye to the current situation. “With the advent of cyberspace, the fight against cybercrime, such as fraud via the Internet, is now also part of the basic units' workload. There also seems to be a worldwide lack of resources regarding cybercrime” (Leukfeldt 12). Although cybercrime is becoming more common, the investigative response is not increasing fast enough. The low involvement of local police in investigating cybercrimes is not because there is a lack of crimes, it is because departments do not have the resources or expertise to deal with the crimes they are presented with. Many police departments don’t think they have enough capacity or

resources to actually deal with cybercrime, which leads them to redirect those in need to the FBI. They perceive state or federal agencies as the appropriate investigative agencies to respond to such cases (Bossler and Holt 167). Local police departments often act as a stopgap and soon send persons in need to a less tangible resource in the FBI, such as sending a victim to a complaint website that gives tips on how to keep their information safe and gives no guarantees if an investigation will actually be held.

C. Definitions of Cybercrime

Another barrier to police departments policing cybercrime is the differing cybercrime definitions and definitions that are too broad, making it hard to tell what resources should be allocated to cybercrime. The FBI definition of cybercrime, which includes “any crime conducted via the Internet, network or digital device.” This definition here often leads to non-cybercrimes to be mistaken as cybercrime. This definition would include, for example, somebody using a cell phone to call a drug dealer to set up a meeting. It may be inappropriate to consider this crime a cybercrime, although a drug deal where the buyer browses a website and has the drugs shipped to their house might be more appropriate to consider a cybercrime. This would lead to any crime involving a cellphone to be regarded as a cybercrime when not all crimes using a cellphone can be called a cybercrime. This would cause a barrier as cyber units could be given anything regarding cell phones leading to potentially wasting resources when the crime could have been in fact investigated by a different unit.

This is an issue with other definitions as well. Another definition comes from the South African portal for resources and information on Cybercrime, which states that

"'cybercrime' means illegal acts, the commission of which involves the use of information and communication technologies" this definition was later revised several months later to "'[c]yber crime' means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them" (Internet Safety Campaign Africa). South Africa's first definition would encompass a large amount of crimes that wouldn't be actually considered cybercrimes, like the example of the drug deal earlier. The revised definition provides a reduced scope, but may still be overly broad. The definition of cybercrime seems to range from country to country with focuses changing depending on country. "[T]here is no consensus in the Netherlands on how cybercrime should be defined and which crimes it encompasses exactly. In their literature study, Van der Hulst and Neve (2008, p. 19) concluded that: 'A common definition and consistent conceptual framework is lacking for this field of crime" (Leukfeldt 2).

The lack of consensus of a definition leads to placing resources and training in the wrong areas. It also simplifies a complex crime into a basic crime or makes a basic crime seem more complex. Due to lack of clear definition officers struggle to find importance in policing (usually cyberbullying) or make their own definition, which can lead to misallocation of resources. The U.S. definition compared to South Africa's, is similar as both definitions have some crimes blended in with each other most specifically white collar crimes and cybercrimes. The problem is that cybercrime can be a white collar crime and vice-versa, but not every cybercrime is a white collar crime neither is every white collar crime a cybercrime. So it is important that we can make a

distinction so that departments can get the proper units to investigate what they specialize in or so those units can collaborate with each other.

D. Cybercrime is Inter-Jurisdictional

The fourth barrier deals with how cybercrime is a crime that can affect people all around the world. Someone from Idaho could get their identity stolen by somebody from Europe. This is not a crime that can be solved by local police because of the internet's interconnectivity and anonymity. It can be difficult for first responders in the US to deal with crimes committed from across the world. Furthermore, The fact that cybercrimes like that are highly publicized may convince local police that cybercrime is outside of their domain. For example, " [p]ublicly known examples of alleged hostile state action include Russian interference in the US election and North Korea's WannaCry attack that so affected the NHS" (BCS). As a result, people think of cybercrime as big national attacks on governments or some complicated hack to steal somebody's identity. Of course in these cases the FBI may be the first response, but there are also plenty of cybercrimes that are on a smaller level that could be solved by the local police.

E. Cybercrime is intangible and can be done from a distance

The lack of tangibility of cybercrimes is the next barrier, as perpetrators of cybercrimes can be difficult to observe. Finding a criminal can be easier with a face, body type, or just a general description. With cybercrime, none of these characteristics may be necessary or helpful. However, without some sort of profile, investigations are similar to looking for a needle in a haystack. Instead of looking for a physical footprint,

police need to look for a digital footprint. The concept of looking for physical footprint is often easier to grasp for most officers than trying to find a digital one.

Police may also have trouble locating the perpetrator of a cybercrime, especially considering the lack of evidence left behind in a cybercrime. The likelihood that the perpetrator is in the same state, while on the rise, is still low compared to non-cybercrimes. This makes it harder for officers to investigate and make arrests, causing officers to be less interested in policing the crime. “Prosecuting a distant perpetrator will be less of a priority as a matter of deterrence” (Swire 113). It is simply easier to wrap their head around keeping a criminal on the run than catching a criminal sitting at home behind a screen. The chance that a criminal doesn’t fall in their jurisdiction is higher than a physical crime, possibly causing even a simple cybercrime to be complex.

F. Cybercrime investigations are costly

The sixth barrier is how costly it can be for police departments to develop cyber investigation capabilities. This can be expensive not only in terms of training costs, but also in terms of how much labor they will lose by sending someone to get training. Simply putting cybercrime on a police officer's daily tasks isn’t efficient because there is a certain expertise needed to handle cybercrimes and expecting an officer not specially trained to investigate a cybercrime could lead to mishandled investigations. Consequently, in many places special cyber units have been created. “For cybercrime and cyberpolicing more specifically, contingency theory suggests that as cybercrime becomes more prevalent and costly, local police departments are likely to devote greater resources to policing those types of crime, which may include the creation of

specialized units." (Nowacki and Willits 109) The demand for cyberpolicing is becoming more prevalent, but with how already understaffed most police departments are they are not equipped to lose four or five officers to training. However, cybercrime is developing so quickly that if departments don't send people to learn cyberpolicing they will eventually have to scramble to either find people already trained or lose officers to training in the future.

Another problem is that it is hard to measure the success of the training. "[H]igh quality training alone would not improve the quality and success of investigations. Successful investigations, they suggested, also depended upon appropriately skilled and motivated personnel being available" (Cockcroft). The fear for some departments is that they send officers to get training, and they won't be able to use this training effectively to police cybercrime because of how quickly cybercrime develops. This would make the cost of the training even higher as not only did it cost money to send officers to the training, but it also cost manpower and now they have a possibly flawed skill that can't be properly employed in their work.

G. It may take time to see the results of new cybercrime capabilities

The last barrier is the pressure for the newly implemented units to perform. If a department spends the money to have certain officers trained in cybercrime or create a cybercrime unit, they are going to be looking for clear and immediate results. Quick results may not be found due to the complexity of some cybercrimes and results may vary on what a department expects from their unit. "First, staff report there has been an escalation and acceleration of the quantity of the work cyber-crime units are expected to

undertake. Second, the resourcing of cyber-crime units has not developed commensurate with increasing demands. Third, the level of skills and training within units is often not sufficient to address the nature and growing complexities of investigating cyber-crime, which can lead to disproportionate pressure on the small number of tech-savvy staff present within specialist units" (Harkin 520). This could be why so many departments in the U.S. don't have cyber units. There is a lot of pressure to perform, so if there is a jurisdiction with a large number of cyber investigations, a small unit could be overtasked. Depending on the size of the department, these "specialists" may end up being tasked with non-cybercrimes because of necessity or simply because departments don't think they have enough work. These extra duties can put more stress than there needs to be on these individuals, which could also cause officers to not want to learn how to cyberpolice.

V. Overcoming Barriers

In the previous section, I identified the barriers to the implementation of a cyber unit in local police departments. In this section, I will explore how these barriers can be overcome.

A. A new generation of tech-savvy police officers will reduce training costs

Training and the cost of training were primary barriers found to be impeding the addition of cyber units. This is mainly due to training for cybercrime being both costly and difficult, as it is something that many officers may have never dealt with. These two factors bring into question the necessity of having a local law enforcement unit deal with

cybercrime. Many ask why should local law enforcement be involved when training is so expensive in comparison to how much cybercrimes occur or with how difficult it is to train officers to solve cybercrime.

The solution to the issues with training is the next generation. The upcoming generation of future officers have grown up using the internet and having smartphones. This will give them an advantage when being trained in cybercrime as they bring in different skill sets and learning capacities that will make training easier for them. This could lead to a reduction in the cost for training as well, since they already bring a solid base with technology.

Not only will future officers change, but also the way crime is committed will also change as technology evolves. There will be more opportunities to commit crimes with technology due to innate freedom given by the internet. “The internet is a suitable environment where a crime can be designed, because it is a valuable source of information. Information is the essence of the internet itself, which can be defined as an enormous database embracing almost all fields of knowledge. Information is free, updated and is also easily attainable by those persons who are not very accustomed to PCs” (Savona 11). With how rapid the internet is growing, it is critical training for policing cybercrime is implemented because soon cybercrimes are going to become the norm. Once that happens, it will be very important for police departments to become proactive in their efforts to prevent cybercrime.

B. Clearly defined roles will reduce jurisdictional barriers

To overcome the barrier of the scattered goals, multiple definitions, and lack of exposure, there needs to be clearly a defined role for local cyber units that satisfies both what police departments want from their cyber unit and how the FBI would want police departments to lighten their caseload. In order to do this, local police and communities will have to become more knowledgeable about what cybercrime, in order to recognize cybercrime as a problem they tend to steer closer to cyber equivalents of commonly-policed crimes. This leads to neglect of smaller issues and can cause confusion into what local law enforcement agencies consider cybercrime. In return, some will question whether it would be worth it for local law enforcement to deal with small local cybercrimes. Not keeping smaller cybercrimes in check can lead to larger crimes being committed and local law enforcement have a better chance to deal with smaller cybercrime than the FBI.

Along with that those who don't have units often believe that there aren't enough cybercrimes in their area due the misconception of cybercrime being completely anonymous. So the issue with having local law enforcement police cybercrime is that because of how expansive the internet is the perpetrator can be from anywhere. Though as stated before cybercrimes between individuals in the same state are on the rise in recent years, so the majority of what local law enforcement would be asked or expected to handle would be small cybercrimes that wouldn't reach an international level since the FBI handles those kinds of cases. Nobody is asking a local police force to investigate a terrorist bomb threat and in similar fashion with cybercrime nobody would ask them to investigate somebody hacking into federal government mainframes. Though in terms of cybercrime we expect the opposite from our federal entities as local

law enforcement often default to the FBI on small crimes such as ID-theft or malware cases. Local law enforcement don't rely on the FBI to handle a thief stealing a handbag from a store, which can be considered equivalent to ID-theft.

A counter to this thought would be how would local law enforcement handle a situation where the perpetrator is in one state and the victim is in another. This would obviously be the biggest hindrance in having local law enforcement deal with cybercrime instead of the FBI. But once again it is not as if local law enforcements don't deal with people committing crimes in one state then leaving to another or a perpetrator is a resident of one state and committed a crime in another. Similar procedures could be followed, in the case of cybercrime, as the normal crime. Communication between local law enforcements is key and due to the likelihood that one perpetrator probably has multiple victims the FBI instead of completely taking over the case can act as an intermediary and connect the agencies with the perpetrators home law enforcement agency. The FBI doesn't have to serve in an investigatory capacity as once the perpetrator is found all that is needed is for the home agency to trace back all of the perpetrators activities. So in retrospect dealing with perpetrators and victims in different states can be handled similar to how law enforcement handle them in normal crimes.

C. Managing Police Productivity Culture

With how much pressure is put on cybercrime units to produce results, the goal of many police departments is clear. They want results to justify adding such a unit, which is seen as non-essential. To overcome this barrier police culture would have to change as a whole, but with how quick cybercrime is developing a different approach

can be taken. “Certainly law enforcement is behind the curve when dealing with digital crime... that technology changes at an astounding rate while law enforcement techniques, which traditionally are reactionary, do not” (Gogolin 116). With how young cybercrime is law enforcement has the ability to finally get the upper hand on potential criminal activity. The small crimes may not seem like much, but being proactive in policing can help acclimate officers to the new norm of cybercrime. Setting small goals is always a way to create responsibility and will eventually lead to bigger things meaning local law enforcement, once they catch up with the developing cybercrimes can be given more responsibility in the realm of cybercrime.

VI. Conclusion

Cybercrime has many definitions, but the one followed in this paper and followed by the FBI is “Cybercrime has an expansive definition that includes any crime conducted via the Internet, network or digital device. Capturing digital evidence, such as that found on cellular phones, GPS devices, computers, tablets and network servers, is crucial to investigating and solving cybercrimes.” Following this definition has led to many well-thought out plans in regards to what to do about the cybercrime situation. However, there are still barriers to implementing cyberpolicing at a local level. These barriers are difficulties with training, lack of exposure, no clear goal/definition, cybercrime is on a global scale, victims and perpetrators are faceless, cost, and pressure to produce results.

To overcome these barriers requires patience as reducing difficulty in training will come with a new generation of police cadets who have a large amount of experience

with the internet and technology. Along with difficulty being reduced cost will go down as cadets will need less basic instruction. Police departments need to change their goal in terms of how they should be dealing with crime, especially a crime that is still in development. The opportunity that presents itself to implement proactive and preventative measures to combat cybercrime is an enticing possibility to see if it is possible to actually prevent crime from happening. As for actually policing cybercrime the FBI doesn't have to be involved, but it would be beneficial if they acted as an intermediary between other police departments since a good amount of cyber investigations will likely cross state lines. Having the FBI connecting different police departments together will allow for smoother investigations, while also not having to rely on them to investigate every cybercrime like they are currently doing.

Cybercrime is on a rapid climb, which is why the opportunity presented to local police departments is so vital. As this is the first time that lawmakers and law enforcement can witness the birth and growth of a crime. Especially a crime that requires a lot of planning to enact and generally doesn't have the element of crime of passion, which makes other crimes harder to prevent. If law enforcement are ever going to be proactive in their policing this is the time for it since once cybercrime reaches a level where cybercrime is common it will have become too late and law enforcement will have to continue their reactionary ways of policing.

Appendix

The following are websites of the 100 police departments that were randomly selected and were used in the data collection for this paper.

https://www.cityofevanston.org/government/departments/police

https://www.tfid.org/186/Police

https://www.sanmarcostx.gov/151/Police

http://wrga.gov/index.aspx?NID=607

https://www.leesburgva.gov/government/departments/police-department

http://bibbsheriff.us/

http://www.ci.bristol.ct.us/200/Police-Department

http://www.newbedfordpd.com/

https://www.wcpd.org/

http://www.hendersonville-pd.org/

https://www.mcallen.net/departments/pd/criminal-investigations

https://www.cityofsouthgate.org/233/Police

https://www.sheriff.org/LE/Pages/Districts/Deerfield-Beach.aspx

https://www.yourmpd.com/

https://www.spanishfork.org/departments/public_safety/police.php

https://www.brokenarrowok.gov/90/Police-Department

https://www.denvergov.org/content/denvergov/en/police-department.html

https://www.maricopa-az.gov/departments/police-department

https://www.littlerock.gov/for-residents/police-department/

https://www.miamibeachfl.gov/city-hall/police/

http://www.jeffersoncitymo.gov/government/police.php

https://www.cityofchino.org/cms/One.aspx?portalId=10382662&pageId=11471198

http://www.longbeach.gov/police/about-the-lbpd/bureaus/investigations-bureau/detective-division/#computer

https://www.cityofboise.org/departments/police/

https://ci.lubbock.tx.us/departments/police-department

https://www.allentownpa.gov/Police

https://meridiancity.org/police/

http://euclidpd.org/

https://police.southbendin.gov/

https://www.tulsapolice.org/content/cyber-crimes-unit.aspx

https://columbiapd.net/

http://www.ci.dearborn-heights.mi.us/departments/public_safety/police_department/index.php

https://www.norfolk.gov/305/Police

https://www.cedarparktexas.gov/departments/police-department

https://www.cityofkeller.com/services/police

http://www.sjc.utah.gov/police/

https://www.huntsvilletx.gov/185/Police-Department

https://www.coralgables.com/departments/Police

https://www.bullheadcity.com/departments/police

https://www.valdostacity.com/police-department

https://www.venturasheriff.org/

https://www.fmpolice.com

http://www.ci.pittsburg.ca.us/index.aspx?page=272

http://www.siouxcitypolice.com/

https://charlottenc.gov/CMPD/Organization/Pages/InvestSvcs/Cyber-Crimes.aspx

http://www.barnstablepolice.com/

https://www.highpointnc.gov/police

https://www.wgpd.com/174/Police

https://www.vbgov.com/government/departments/police/Pages/default.aspx

https://www.miami-police.org/

https://www.torranceca.gov/our-city/police

https://www.cityofmesquite.com/442/Police

https://www.cityofconcord.org/183/Police

https://ci.billings.mt.us/101/Police

https://www.perthamboynj.org/government/departments/police_department

https://www.cityofmartinez.org/depts/police/default.asp

http://www.riversidesheriff.org/bureaus/computer-hitech.asp

https://www.cdaid.org/police

https://www.johnsoncitytn.org/services/public_safety/police_department.php

https://www.newhavenct.gov/gov/depts/nhpd/

https://www.cville.org/253/Police-Department

http://www.nbpd.org/

http://www.coppelltx.gov/government/departments/police-department

http://www.flaglersheriff.com/

http://www.elkgrovepd.org/

http://www.pbso.org/inside-pbso/law-enforcement/strategic-operations/special-investigations-division/

https://dauphin.crimewatchpa.com/hbgpd

https://www.pueblo.us/102/Police-Department

http://www.lawpd.com/294/Police

https://www.woburnma.gov/government/police/

https://www.houstontx.gov/police/divisions/cyber_&_financial_crimes/index.htm

https://www.lancaster-tx.com/198/Police

https://www.santa-ana.org/pd

http://www.dalycity.org/City_Hall/Departments/police_department.htm

http://www.cityofparmapolice.com/index.htm

https://www.jacksonms.gov/departments/jackson-police-department/

https://www.cityofwestminster.us/police

https://www.cityoffederalway.com/police

https://www.bradentonpd.com/

https://cityofshawnee.org/departments/police

https://www.tompsc.com/166/Police

https://www.topeka.org/tpd/

http://www.binghamton-ny.gov/departments/police-department/police

http://salempd.org/

https://www.yumaaz.gov/police/

http://www.fwpd.org/

https://www.cityofdelano.org/105/Police-Department

https://www.fishers.in.us/241/Police

https://rentonwa.gov/city_hall/police

https://www.mckinneytexas.org/166/Police

https://www.roswellgov.com/government/departments/police

https://www.fremontpolice.gov/

https://www.cityofpensacola.com/733/Pensacola-Police-Department

https://www.cityofcapegirardeau.org/departments/police

https://www.westerville.org/services/police

https://www.stamfordct.gov/police

https://www.flpd.org/

http://www.mansfieldpolicedepartment.com/

https://dunwoodyga.gov/index.php?section=dunwoodypd

https://www.capecops.com/

Bibliography

Bergen County Prosecutor's Office. "JIMMY RIVERA OF PERTH AMBOY, NJ CHARGED WITH CHILD PORNOGRAPHY." *BCPO16*, www.bcpo.net/press-releases/496-jimmy-rivera-of-perth-amboy-nj-charged-with-child-pornography.

Bossler, Adam M, and Thomas J Holt. *Policing: An International Journal of Police Strategies & Management*, vol. 35, no. 1, 2012, pp. 165–181.

Charlotte Mecklenburg Police Department. "Our Organization." *City of Charlotte Government*, charlottenc.gov/CMPD/Organization/Pages/Office-of-the-Chief.aspx.

Cockcroft, Tom, et al. "Police Cybercrime Training: Perceptions, Pedagogy, and Policy." *Policing: A Journal of Policy and Practice*, 2018, doi:10.1093/police/pay078.

"Crimes Against Property." *Sioux City Police Department*, www.siouxcitypolice.com/crimes-against-property.

Cybercrime.org.za, cybercrime.org.za/definition.

"Cyber Crime." FBI, FBI, 3 May 2016, www.fbi.gov/investigate/cyber.

"Cybercrime Investigations." Law Enforcement Cyber Center, www.iacpcybercenter.org/officers/cyber-crime-investigations/.

"Cybercrime: The Police Response." *BCS*, www.bcs.org/content-hub/cybercrime-the-police-response/.

Davis, J. *" Policing: An International Journal Examining perceptions of local law enforcement in the fight against crimes with a cyber component",* Vol. 35 No. 2, 2012, pp. 272-284.

Department of Justice (DOJ). *Police Are Victims Too: How to Protect Your Department*

from Cybercrime, cops.usdoj.gov/html/dispatch/09-2019/cyber_crime.html.

Dolliver, Diana S. “How Cybercrimes Challenge Law Enforcement.” *Scholars Strategy Network*, scholars.org/contribution/how-cybercrimes-challenge-law-enforcement.

Doorewaard, Cecili. “The Dark Figure Of Crime and Its Impact On The Criminal Justice System”.

EC-Council. “6 Skills Required for a Career in Digital Forensics: EC-Council Official Blog.” *EC*, 30 Apr. 2019, blog.eccouncil.org/6-skills-required-for-a-career-in-digital-forensics/.

Gogolin, Greg, and James Jones. “Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business.” *Information Security Journal: A Global Perspective*, vol. 19, no. 3, 2010, pp. 109–117., doi:10.1080/19393555.2010.483931.

Fort Wayne Police Department, www.fwpd.org/.

Harkin, Diarmaid, et al. “The Challenges Facing Specialist Police Cyber-Crime Units: an Empirical Analysis.” *Police Practice and Research*, vol. 19, no. 6, 2018, pp. 519–536.

Huey, Laura, et al. “‘Uppity Civilians’ and ‘Cyber-Vigilantes’: The Role of the General Public in Policing Cyber-Crime.” *Criminology & Criminal Justice*, vol. 13, no. 1, 2012, pp. 81–97., doi:10.1177/1748895812448086.

Hunton, Paul. “The Stages of Cybercrime Investigations: Bridging the Gap between

Technology Examination and Law Enforcement Investigation.” Computer Law and Security Review: The International Journal of Technology and Practice, vol. 27, no. 1, 2011, pp. 61–67.

Leukfeldt, Rutger, Sander Veenstra, and Wouter Stol. "High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands." International Journal of Cyber Criminology, vol. 7, no. 1, 2013, pp. 1-17.

“McAllen Police Department.” *Criminal Investigations*, www.mcallen.net/departments/pd/criminal-investigations.

Mendelson, Aaron. “Police Robots: Departments Lack Rules on Whether They Can Kill.” *Southern California Public Radio*, 29 Sept. 2016, www.scpr.org/news/2016/07/26/62776/robots-common-at-police-across-southern-california/.

Middlesex County. News.” *Middlesex County*, www.middlesexcountynj.gov/Government/Departments/PSH/Prosecutor/News/Pages/02-05-18.aspx.

Nykodym, Nick, and Sonny Ariss. “Fighting Cybercrime.” *Journal of General Management*, vol. 31, no. 4, 2006, pp. 63–70.

Pinguelo, Fernando M., and Muller, Bradford W. “Virtual Crimes, Real Damages: a Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminal.” *Virginia Journal of Law and Technology*, vol. 16, no. 1, 2011, pp. 116–188.

Santa Ana Police Department. “Special Investigations.” *The City of Santa Ana*, www.santa-ana.org/pd/investigations-bureau/special-investigations.

Savona, Ernesto Ugo. *Crime and Technology : New Frontiers for Regulation, Law Enforcement and Research*. 2004.

Swire, Peter P. “No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime.” *SSRN Electronic Journal*, 2008, doi:10.2139/ssrn.1135704.

Virginia Beach Police Department. *Police :: VBgov.com - City of Virginia Beach*, www.vbgov.com/government/departments/police/.

Willits, Dale, and Jeffrey Nowacki. “The Use of Specialized Cybercrime Policing Units: an Organizational Analysis.” *Criminal Justice Studies*, vol. 29, no. 2, 2016, pp. 105–124., doi:10.1080/1478601x.2016.1170282.