The Bill Blackwood
Law Enforcement Management Institute of Texas

Policing Cybercrime:
A Need for Dedicated Investigation and Coordination within the Criminal Justice System

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Robert Rush III

Killeen Police Department
Killeen, Texas

July 2015

ABSTRACT

Cybercrime is an enormous problem, the scope of which the criminal justice system does not really know. That scope is lacking because the term has yet to be clearly defined, let alone developed to standardize legal statutes and institutional means to combat it. Archaic laws, outdated concepts of the instruments of these crimes, and a lack of training and investigative resources is causing law enforcement to fall further behind in policing this aspect of criminality. Poor communication and jurisdictional boundaries that are only kept by crime fighters and legislators compound the problem. This is relevant because of the ever-increasing digitalization of human lives. Virtually everything that humans can accomplish using a computer or network can be criminally exploited, and law enforcement has not kept pace with that exploitation. For that reason, law enforcement agencies should make an effort to dedicate resources to understanding and investigating cybercrime, as well as coordination with other criminal justice entities in order to increase the solvability of these cases.

Law enforcement needs to establish what cybercrime is, how to investigate it, how to prosecute it, and what tools are available to accomplish those goals. There is a need for communication and coordination across all jurisdictional lines to charge offenders who ignore those same boundaries, as well as a need to solicit buy-in and assistance from stakeholders and potential victims, in order to harden targets against these crimes and hopefully prevent some of them.

TABLE OF CONTENTS

Page

INTRODUCTION

Cybercrime is not a new problem, but it is an enormous one. It is not likely to diminish or disappear as the world moves toward more networked connectivity and dependence on technology for everything from bills to entertainment, from education to social interaction. As technology changes, criminal statutes have lagged behind (“Disorderly Conduct,” 2013), as has the ability of law enforcement officers to investigate and resolve offenses committed via technological means.

Cybercrime itself is difficult to define, but the prevailing idea is that it encompasses a group of offenses where computers or networks are targeted for criminal activity, such as a DDOS (distributed denial of service) attack, property crimes such as identity theft or credit card fraud where computers and/or networks are the means by which the crimes are perpetrated, or crimes against persons where computers or networks are merely used to cause some harm to others (Fair, 2005). The two most well known examples of this last form of cybercrime are cyber harassment and cyberbullying. Other more recently developed forms of cybercrime could include online impersonation, whereby a person pretends to be an existing person for the creation of online profiles, social media accounts, or even messaging, causing harm or distress without necessarily causing pecuniary loss (“Computer Crimes,” 2013).

One significant problem with cybercrime is that the scope of the problem itself is difficult to determine. This is partially due to offenses being unreported (as in the case of reluctant victims of cyberharassment/bullying), and the difficulty in separating fraud cases perpetrated by means of computers and networks from those titled identically but committed via less technical means. Identity theft is an example of this; while the FBI maintains statistics on the prevalence of this offense, the percentage of these crimes definitely committed by using computers or networks is not clear (Harrell, 2013). Sometimes these offenses can be reported to law enforcement, but the elements of a statute cannot be proven given available information, and the investigative means by which we might prove that the offense even occurred are not available, due to the evidentiary burden required to access those means. All law enforcement has is a vague and uneasy sense that the problem is huge, and it is growing, and that the means available to investigate and charge offenders seems to be lacking.

The stakes are increasing as well, both in terms of pecuniary loss and the human element to this type of crime. Aside from the prolific fraud, harassment and financial crimes commonly associated with cybercrime, human/sex trafficking (both of adults and minors), and child pornography have nearly unlimited boundaries to persist as criminal enterprises via computers and digital networks. From contemporary slave trading, to soliciting at-risk youths via social media and “Craigslist” or “Backpage.com” websites, to the exchange of horrible media depicting the victimization of children, the supply for this type of criminality seems to be ready to meet the demand with the assistance of tech-savvy bad guys exploiting inflexible laws and methods.

The ability to define, understand, and resolve all these criminal cases, from the basic computer competence required to understand the problem to clearly identified and current lines of communication with all the state and federal agencies combatting this issue, just do not seem to be present in many agencies (Fair, 2005). In spite of the prolific nature of cybercrime, agencies do not seem to place a high priority on dedicating resources to it (Fair, 2005). For that reason, law enforcement agencies should make an effort to dedicate resources to understanding and investigating cybercrime, as well as coordination with other criminal justice entities in order to increase the solvability of these cases.

POSITION

In spite of the fact that it has existed for as long as there have been computers and networks to exploit, a clear understanding of what constitutes “cybercrime” remains elusive. This is a unique phenomenon in the criminal justice system, where legal statutes and the elements required to violate those statutes are carefully written. Homicide, for example, involves a person causing the death of another person with a range of sub-categories and offense levels that are dependent on culpable mental states and other factors (“Criminal Homicide,” 2013). Even though titles, certain mitigating information and punishment ranges vary from state to state, there is still a pretty clear understanding of what that offense is.

This is not the case with cybercrime. The definition itself of cybercrime has never been as clearly established as say, burglary or murder. Obviously this makes investigating and prosecuting these kinds of incidents highly problematic (Brenner, 2007a). Cybercrime can be defined as simplistically as offenses committed using networked information systems, but that vagueness potentially includes almost the entire range of criminal behavior (Brenner, 2007a). Cyber terrorism, cyber warfare, cyber stalking, cyber bullying, all involve the use of networked information systems, and not only the elements of these offenses but critical jurisdictional issues that define responsibility for prevention and prosecution of these offenses remains unclear (Brenner, 2007a).

Even when the offenses and jursdiction are established, the ability for the agency with jurisdiction to pursue offenders is limited (Brenner, 2007a). This is probably one of the most fundamental problems in dealing with cybercrime. Three categories that cybercrime can fall under, however, are not offense titles in themselves, but they encompass a series of criminal offenses that may or may not always constitute a cyber-offense. These categories are: offenses where the information network or system itself is the target of the attack, as in a distributed denial of service (DDoS) attack; offenses where a computer or network is used to perpetrate crime, as in identity theft or credit/debit card abuse offenses; and offenses where the computer or network is used incidentally, as in cyber bullying/harassment or stalking (Nhan, 2008). An interesting evolution of these categories is that technology has increased the versatility with which these crimes are committed and led to the development of entirely new computer crimes like online impersonation (“Computer Crimes,” 2013). Given that the criminality of these offenses depends on clearly articulated statutory language, investigating and prosecuting these cases will continue to be a losing proposition without more concrete legal definitions.

Even where offenses are clearly written, in too many cases the statute itself has not kept pace with the technology used to commit the offense. In Texas, for example, the current offense of harassment still mentions the use of outdated and nearly obsolete technologies such as pagers and facsimile machines, but it fails entirely to specify the more probable manners in which this offense could be electronically perpetrated, with computer accounts and social media networks (“Disorderly Conduct,” 2013). The statute also makes it criminal to intentionally call a person and fail to hang up or disconnect.

While this is still technically possible with some old phone systems, it is largely a remnant of analog telephony and this open line problem has been resolved with the almost near universal adoption of digital telephony and ubiquity of cellular smart phones, where even the person receiving the call can terminate the call and disconnect. This is just one example of the language of a criminal statute being tweaked over time to include some mention of technological advances, but which has utterly failed to keep pace with technology (Fukuchi, 2011).

It is a commonly held belief in law enforcement that the best opportunity to describe an initial crime scene and preserve evidence rests with the first responder. In practical terms, this means the patrol officer who either responds to a call, proactively discovers a crime in progress or evidence of one, or who is working at a departmental information or intake desk where citizens walk in and file reports. These officers need training in and awareness of a multitude of potential crimes, both to determine if an actual offense was committed and to know how to process what if any crime scene exists.

The investigation of cybercrime is no different. What has been discovered, however, is that patrol officers often lack not only the awareness of cybercrime but the skills to conduct an initial investigation on such offenses (Bossler, 2012). This skill includes specific things to look for in an investigation as how to power down information systems and digital devices of evidentiary value, documenting these items in place prior to seizure, and the packaging, transport and storage of these items after seizure. Other cybercrimes, like cyber harassment, online impersonation, and stalking might require training on obtaining account information for both the victim and suspect (if known), billing statements or call histories, and even knowing how to search for metadata on digital photographs. Even basic computer literacy is a critical component for first responders in terms of investigation but happens to be acknowledged by officers as a need for improvement (Bossler, 2012).

Another potential improvement that could be made in terms of investigation of cybercrime could be in the assignment of these cases for follow up. This might require a multi-pronged approach. Many law enforcement agencies with specialized criminal investigation units are still organized along traditionally grouped offense types. A medium sized agency might have a crimes against persons section, crimes against property, vice/narcotics, major case unit (dealing with aggravated and sexually assaultive offenses, robbery and homicide) and youth offenses where the victim/offenders are underage. These categories involve many different offenses that could be reported and investigated but are routed for follow up investigation according to similar characteristics.

Youth offenses as a specific unit, however, could present a viable model for cybercrime routing/assignment. Not counting status offenses like underage possession of alcohol/tobacco, being a runaway, truancy, et cetera, the offenses investigated by a typical youth offenses unit are based on the same statutes as those investigated by any other. The difference is the age of the offender or victim. In the case of a juvenile victim, there are protections and procedures in place that make resolution of some of these cases unique, as well enhanced punishments for the offenders. In the cases of juvenile offenders the prosecution goes through an entirely different court system.

Grouping cybercrimes and routing them for investigative follow-up according to defined similarities could help agencies track patterns as well as statistics more accurately. This could be accomplished by modifying whatever records management or reporting system is in place for an agency. The broad range of such systems used requires those changes to be made at vendor or end-user levels, but separating cybercrimes from other similar crimes committed by traditional means would not only help law enforcement get a better sense of the scope of cybercrime, it would help officers focus on this category of crime and could even create a niche for investigators at a local level who demonstrate aptitude. This is clearly a desired goal and not a current state of affairs, as existing research indicates that not only are officers unaware of the scope of cybercrime in their jurisdictions (Bossler, 2012), but many agencies have no dedicated cybercrime units (Fair, 2005). Nevertheless, training line officers to react appropriately to alleged crimes and process evidence is a good idea. Similarly, dedicating resources to a significant crime problem and modifying organizational structure to support that effort reflects an agency committed to reducing that crime problem.

As indicated above, one major obstacle with the investigation and prosecution of cybercrime is the extent to which the commission of the offenses blur jurisdictional boundaries. Local law enforcement agencies are especially constrained by these boundaries, and pursuing an offender across county, state, or even international borders to resolve criminal cases of varying severity may just not always be possible. Some significant challenges are also present in terms of the evidentiary burdens required to charge, prosecute, and convict an offender, and to obtain evidence. For both of these reasons, it is important that agencies improve coordination with each other both locally and at federal/international levels. Establishing these paths of communication and making sure they stay viable can make easier the passing of a case to an agency with a greater chance of prosecuting it successfully, even if the jurisdictional issues cannot be resolved.

Coordination need not be limited to the law enforcement arm of the criminal justice system. Police agencies and prosecutors should interact with legislators and work to create or modify laws in ways that shift some of the evidentiary burden to the accused (Fukuchi, 2011), forcing them to affirmatively defend the charges against them. Currently, the “overwhelming evidentiary burdens” required to prove cybercrime cases frequently make them not worth the expense and effort in a triage-based prosecutorial system or simply impossible (Fukuchi, 2011, p. 291). Unless improvements are made in this area, the problem will continue.

Cybercrime, by its nature, involves offenders using networks, software, websites, and other services that they do not own. Their activities are often tracked or logged as a matter of course or even as a function of the fundamental principles of networking, albeit in a more raw and less easily interpreted form at that level. With that in mind, it seems counterintuitive that such a difficulty in investigating suspects and offenders would persist. Reasons why include privacy issues, liability attached to those entities for voluntarily releasing subscriber or other information, and even procedures used by law enforcement to compel the involuntary release of that information, are all somewhat unclear.

Procedures for obtaining search warrants once probable cause has been obtained are in place, but timelines for obtaining and the execution of a search warrant for digital information compared to the retention periods for that information are inconsistent at best. Routing such requests for information to the correct person at a third party company can be very tedious and some companies might even make locating the contact information for that person intentionally difficult. If probable cause has not been established for the sake of an evidentiary search warrant, the problem is even greater.

A Grand Jury subpoena for records or information is an alternative to a search warrant, but given that they are issued by Grand Juries the availability of this alternative for the investigation of misdemeanor cybercrimes is not guaranteed. Especially with the proliferation of cyber harassment, and online impersonation crimes (which are misdemeanors unless specific penalty enhancement criteria are met), it is currently difficult or even impossible to prove up these crimes and identify or charge an offender (“Computer Crimes,” 2013; “Disorderly Conduct,” 2013).

The best possible way to fix this problem is for all stakeholders in cybercrime reduction to lobby for the legislative change that will give these cases a chance to be investigated. One example might be some kind of “implied consent” law requiring all internet companies to include in their Terms of Service an agreement for account holders to authorize the company to release limited information to law enforcement agencies conducting a criminal investigation.

COUNTER POSITION

Traditional workflow of law enforcement agencies and investigative units is motivated by solvability (Nhan, 2008). Solvability involves a subjective determination based on several factors that an offender can be identified, charged, and prosecuted. Some law enforcement entities have attempted to reduce solvability into objective scores, but the inclusion of factors into the solvability process (such as witnesses, evidence collected, known suspect, vehicle information, NCIC/TCIC entries or hits, etc…) and the weight each of those factors has on a case remains subjective.

At the local law enforcement level, investigative units are overburdened and can rarely assign 100% of the cases they review and so must prioritize the ones they do assign according to a determination of that solvability. Problems with jurisdictional authority/responsibility in cybercrime cases dramatically lowers the probability of these cases being finally solved (disposed of), which in turn lowers their priority in assignment and follow up (Brenner, 2007b). That said, nontraditional methods of addressing frequent and focused crimes has been successful, even those methods that are more intent on prevention and intervention than reaction and prosecution (Scott, 2007). Methods include partnering with community leaders and directly interacting with those who are at risk to offend (Scott, 2007), and increasing the stake the community holds in preventing/solving the problem (Nhan, 2008). This might be more problematic in international cybercrime prevention, at least from the perspective of a typically policed community; but education, resource sharing, and coordinated defensive measures at any community level could have a positive impact.

As previously stated, leaving case management and investigation at the status quo for the sake of pure solvability may not be the best option. An argument against devoting time, personnel, and training resources to investigating cybercrime and even impacting legislation is budgetary. It simply costs money to train officers, and training them on information systems or specialized investigative techniques can be extremely expensive. Technology is ever changing, so an investment in training entire departments on competence with computer systems and networks and how to look at them investigatively could be cost prohibitive. When balanced against the still-low probability of solving these crimes, on the surface, it could be considered a bad financial decision to implement such sweeping changes.

That said, the financial cost and the human impact of cybercrime indicate that it may be too expensive *not* to implement change. Media outlets regularly report suicides that are directly attributed to cyber harassment or bullying. Homicides where victims are targeted via social media or online personal ads have been reported (Philip Markoff, n.d.; Caufield, 2014).

While the full extent of financial cybercrime is not known, what financial impact is known is of great concern. Perpetrators of identity theft, which is only one of the many financial crimes that can be grouped under cybercrime, victimized over sixteen million US citizens in 2012, for a financial impact of $24.7 billion (Harrell, 2013). Many of these people were victimized more than once, and in about 91% of the cases no suspect or offender information was obtained (Harrell, 2013). That is a very small snapshot of the entire problem, and when cybercrimes resulting in debit and credit card abuse and the host of other means by which computers can be used to commit financial scams are taken into account, the amount of loss in the US each year dwarfs the entire gross domestic product of some countries (“List of Countries,” n.d.).

There is also no requirement that law enforcement agencies implement costly changes all at once with 100% of their personnel. Tiered training programs over several years would doubtless still have positive impacts, as would ongoing coordination with other criminal justice entities. The cost of these programs could be spread out over time, making it that much more affordable.

RECOMMENDATION

It is absolutely critical that the criminal justice system gets better at investigating and prosecuting cybercrime. The only way to do this is to dedicate more resources and personnel to understanding it, defining it, clearly criminalizing it, and making the cases solvable. Updating statutes to reflect the manner in which the crimes are actually committed is a step in that direction. It would be anachronistic for the current definition of aggravated assault to include the use of a flintlock pistol; yet harassment and other statutes still retain language of obsolete (or “merely” antiquated) technology.

Ensuring that first responders and follow-up investigators have the necessary tools to work these cases is another step. Coordinating with prosecutors and legislators to shift evidentiary burdens to the accused and making it possible for law enforcement to obtain information related to the crimes from third parties could be of great help. Lastly, coordinating with agencies locally, at the federal and international level to establish clear cross-jurisdictional means of assistance and responsibility, and then keeping those lines open, could only help those in criminal justice fight this type of crime. It is strongly recommended that municipal and state police agencies make the training of their officers on computer literacy, cybercrime-scene processing, and digital forensics a very high priority. It is also recommended that agencies organize these types of crimes and route them to dedicated personnel, so those with more experience and better training will have a greater chance to solve the cases, and in order to better identify the full scope of the problem.

REFERENCES

Bossler, A. M. (2012, March). Patrol officers’ perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies and Management*, *35*(1), 165-181.

Brenner, S. W. (2007a, February). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law & Criminology*, *97*(2), 379-475.

Brenner, S. W. (2007b, March). Cybercrime jurisdiction. *Crime Law Social Change*, *46*, 189-206.

Caufield, P. (2014, February 17). Pennsylvania 'Craigslist killer' says she slayed dozens more across U.S. as part of satanic cult. *NY Daily News*. Retrieved from http://www.nydailynews.com/news/national/craigslist-killer-claims-slayed-dozens-part-satanic-cult-report-article-1.1616297

Computer Crimes, Tex. Penal Code, 33, (2013).

Criminal Homicide, Tex Penal Code, 19 (2013).

Disorderly conduct and related offenses, Tex Penal Code, 42, (2013).

Fair, R. C. (2005, November). *Feasibility of a cybercrime investigation unit in a police department.* Huntsville, TX: The Bill Blackwood Law Enforcement Management Insititutue of Texas.

Fukuchi, A. (2011). A balance of convenience: The use of burden-shifting devices in criminal cyberharassment law. *Boston College Law Review*, *52*, 289-338.

Harrell, E. L. (2013). *Victims of identity theft, 2012.* Washington, DC: U.S. Department of Justice.

List of Countries by GDP (nominal). (n.d.). In *Wikipedia*. Retrieved January 24, 2015, from http://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal)

Nhan, J. (2008). *Policing cyberspace: The compatibility of the internet with traditional forms of law enforcement, law, and policy.* Ann Arbor, MI: UMI Dissertation Publishing.

Philip Markoff. (n.d.). In *Wikipedia*. Retrieved January 24, 2015, from http://en.wikipedia.org/wiki/Philip_Markoff

Scott, E. (2007). *Revisiting gang violence in Boston.* Boston, MA: Harvard College.