THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

Investigating Cyber Security Threats:
Exploring National Security and Law Enforcement Perspectives

Frederic Lemieux, Ph.D.
Director of Security & Safety Leadership (CPS)
Associate Professor, Department of Sociology (CCAS)
The George Washington University

Report GW-CSPRI-2011-2

April 7, 2011

Abstract

This report focuses on how federal agencies define success in computer crime investigations and how they can facilitate the development and refinement of a comprehensive law enforcement strategy for addressing cyber threats. Through interviews with experienced computer crime investigators from the Federal Bureau of Investigation, the U.S. Secret Service, and the Air Force Office of Special Investigations, this project aims to identify how federal agencies conduct investigations related to cyber security and how they define operational success. Our findings show a clear emphasis on threat mitigation, instead of quantitative valuation of prosecutions, as the goal of the investigation. Strategies employ the use of intelligence gathering and sharing to fortify potential targets and identify prolific offenders. These observations are consistent with the current trends in traditional investigation which include the use of an intelligence-led policing model to combat the top national security risks to the United States.

Work supported by the Office of the Vice President for Academic Affairs and the School of Engineering and Applied Science of the George Washington University

Investigating Cyber Security Threats:
Exploring National Security and Law Enforcement Perspectives

Frederic Lemieux, Ph.D.
Director of Security & Safety Leadership (CPS)
Associate Professor, Department of Sociology (CCAS)
The George Washington University

Introduction

Computers are used to commit crime and are the target of crime every day. Besides the magnitude and scope of the threat, one of the greatest challenges in fighting computer crime resides in the fundamental nature of the computing world. Cyber space is dynamic and changes often at a rapid pace. A computer's increasing sophistication, in terms of power capacity and communication speed, increases the criminal opportunity for motivated offenders as well as the availability of suitable targets. Moreover, the worldwide computer network has transformed computer crime from a local problem to an international security issue.

Cyber threats are currently significant enough to become a national security priority in several western countries including the United States. In order to better understand the challenges that the United States' cyber infrastructures are facing, it is necessary to examine how government agencies are addressing the threats posed by those who perpetrate computer-based crimes and attacks. On one hand, we know that computer crimes are often a "hi-tech" version of more traditional crimes such as theft, espionage, sabotage, and fraud. On the other hand, the ramification of cyber crimes are so extensive and technologically complex that they require specific knowledge to better understand the evolving nature of the threats as well as the tactics and strategies to investigate them.

This report is an effort to better understand the investigative processes and strategies of three United States federal agencies as they pursue cyber criminals and attempt to neutralize cyber threats. Our study focuses on investigations conducted by the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), and the Air Force Office of Special Investigations (AFOSI). The main objectives of this research are to understand how these agencies define "success" and what investigative models they use to address computer crime.

More precisely, this research scrutinizes cyber investigation methods and practices and compares them to a traditional investigative model, namely intelligence-led policing (ILP). ILP refers to a managerial model developed in the United Kingdom in the late 1990s. This model emphasizes the targeting of prolific offenders in order to diminish both victimization and crime volume (Lemieux 2006; Ratcliffe 2008). ILP relies heavily on inter-agency cooperation and intelligence sharing in order to enhance proactive law enforcement operations. Leads, tips, and other information related to serious offenders as well as criminal organizations are all part of the intelligence gathering and sharing in this model. This report begins to explore the extent to which ILP is applied or applicable to cyber investigations for both law enforcement and national security capacities.

Characterizing the threat

Law enforcement and national security agencies are currently facing highly diversified cyber threats. For police services "cyber crime," "computer crime," "information technology crime," and "high-tech crime" usually fall within two major categories of offenses: (1) the computer is the target of the offense, and therefore attacks on network confidentiality, integrity and/or availability (i.e. unauthorized access to and illicit tampering with systems, programs or data) all fall into this category and (2) traditional offenses such as theft, fraud, and forgery that are committed with the assistance of or by means of computers, computer networks and related information and communications technology. This categorization is largely recognized by experts in the field and most government agencies.

According to the Federal Bureau of Investigation (FBI), cyber crime results in serious monetary loss and extensive fraud. In 2010, the FBI reported that a typical loss can range from $223.00 (credit card fraud) to $3,000.00 (check fraud) per complaint. The same year, the top cyber crime complaint categories were the following (FBI 2010):

- Non-delivery (paying for merchandise online, but not receiving it);
- Auction fraud;
- Debit/credit card fraud;
- Confidence fraud (also referred to as advance fee fraud);
- Computer fraud;
- Check fraud;
- Nigerian letter fraud;
- Identity theft;
- Financial institutions fraud.

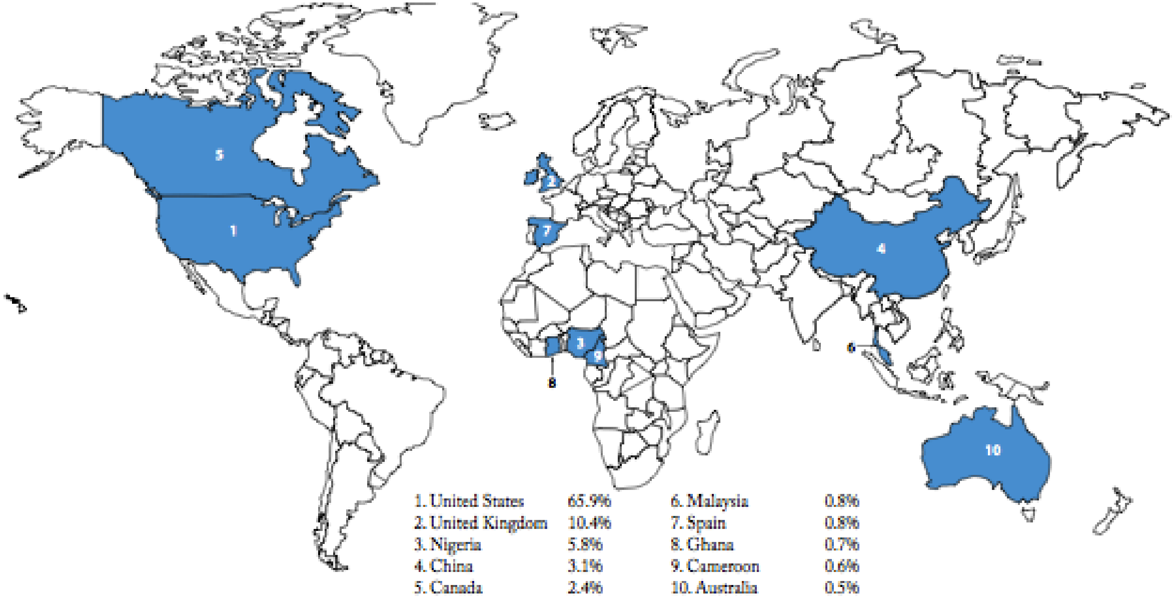
The existing literature on cyber crime investigation discusses the practical science of computer forensics at the technical level. Most of the writings in the field are intended for an audience already highly skilled in the use of computers. For example, Reyes' (2007) work addresses cyber crime from its technical beginnings, through the law enforcement role of pursuit and apprehension, to the final legal issue of prosecution. However, he does not delve into case management or the over-arching strategy of computer crime investigation. Mendell (2004) addresses computer crime investigations and forensics by examining the factors used in determining whether or not a given computer crime is "solvable." More precisely, this author explores the allocation of effort and resources in pursuing computer crime based on the probability of ultimately solving the crime. Mendell (2004) views computer crime investigation as a case by case approach as opposed to presenting a cohesive model for understanding cyber crime investigation from a more strategic perspective.

When investigating cyber crime, law enforcement agencies face several challenges, including application of tactics, cooperation with concerned parties, and regularly operating between inconsistent legal frameworks in international investigations. The work of Hinduja (2007) addresses some key concepts to be aware of when examining the process of cyber investigations, such as the tactics of traditional crime and how they apply to computer crime. The author also discusses the necessity of outsourcing investigations to the private sector, as the ability to cooperate with private companies affects both the investigation process as well as outcome (success). In the same vein, Sussmann (1999) points out another critical factor in computer crime investigations: international cooperation. Many western countries may be at the forefront of computer crime forensics and investigations, but other nations may not, and cooperation with them is a critical and on-going challenge.

Kerr (2008) provides a valuable overview of recent cases in computer crime from a strictly legal standpoint. He outlines how the legal framework present in the United States allows for the prosecution of cyber crime, though this is not always the case in other countries. Figure 1 shows a worldwide distribution of origins of perpetrators and reflects the geographic challenges related to investigating computer crime.

Finally, funding presents a critical challenge for most law enforcement agencies. The size of a law enforcement agency's budget determines the number of agents it may employ and the amount of resources at its disposal. Investigation resources are always limited, in both the cyber and 'real' worlds, inevitably provoking a certain level of attrition in pursuits of particular cases. There is simply insufficient manpower and resources to adequately develop the skills of the workforce in charge of cyber crime investigation. Budget constraints and resource limitations are pervasive factors that heavily impact cyber crime investigation processes and tactics.

Figure 1: Origin of computer crime perpetrators at the international level
(Source: Internet Crime Complaints Center, 2011)



Due to their importance with the realm of national security, crimes which target a computer system are of special interest to governments and private industries. The large quantity of classified information and data stored in government computers, as well as computer-dependent infrastructures within western countries represents critical political, economic, and security assets which require protection from attackers (state and non-state actors) both within and outside of a country. In retrospect, public awareness of the critical infrastructure and vulnerabilities of a computer network never fully developed until 1999 when Y2K became a front-page issue that highlighted society's dependence on computer systems for everything from ensuring prompt arrival of trains to protection of nuclear reactors.

Today, national security preoccupations are directed in part toward large scale cyber attacks which could target public and private computer infrastructures. However, according to Table 1, most cyber attacks are largely limited to denial of service attacks or incidents lacking long term impact (e.g. e-mail bombing or defacing of public domain websites). Most attacks perpetrated by state and non-state actors lack the capability to cause harm to a person, to damage property, or to incite fear in the general population. In most cases, damage has been limited to computer stations, websites, software, and email communications.

Table 1: Widely publicized breaches of national security and critical infrastructures

Year	Attacker	Target	Consequence
1982	United States - CIA	Logic bomb targeting USSR Siberian gas pipeline	Destruction
1999 & 2000	Russia	Pentagon, NASA, National Labs	Steeling information espionage
2004	China	Sandia National Laboratory, Lockheed Martin and NASA	Espionage
2007	China	U.S. computer networks (750,000 computers)	Denial of service
2007	Russia	Estonia's government web sites	Denial of service
2008	Unspecified	U.S. military network	Malicious code and zombie machines
2008	China and/or Russia	U.S. Presidential elections	Intrusion into email systems
2008	Russia	Georgia government and banking computer systems	Denial of service
2010	Unspecified	Iran uranium enrichment centrifuges	Sabotage
2010	Anonymous "Operation Avenge Assange"	Multiple western targets (public and private)	Denial of service

Despite warning signals from public and private sectors, doomsday and digital terrorist attacks have not yet caused the total collapse of western institutions. Nevertheless, threats of cyber warfare, virtual espionage, and "hacktivism" have materialized in the past two decades. Among the various challenges for national security practices, preventing and neutralizing attacks against U.S.'s critical infrastructure at the hands of state and non-state actors is certainly a priority (NSCS, 2003). In that regard, Cavelty (2008) draws attention to the concern of adequately securing government and military systems as well as addressing vulnerabilities in critical infrastructures in the United States by scrutinizing the context of policy planning and international relations. Carr's (2010) examination of the concept of cyber warfare delves deeply into the vulnerabilities and political considerations of this new form of conflict (2010). Specifically, the author underscores the dangers related to cyber warfare and outlines future threats and cyber warfare strategies (prevention or defense). This work builds on previous assessments conducted by U.S. law enforcement agencies for internal purposes.

In 2005, the FBI published the results of its own computer crime survey. This exercise demonstrates the FBI's keen interest in preserving the security of the "nation's businesses." It provides a broad overview of the computer security problems facing U.S. businesses, how much financial damage these security breaches are causing, and the measures U.S. businesses are taking to protect themselves (FBI 2005). In addition to the 2005 survey conducted by the FBI, the Computer Security Institute (CSI) conducts a very thorough annual survey of the use of computer security software and the effects of computer crime in U.S. businesses (Peters 2009). More recently, 29 percent of respondents to a survey conducted by McAfee (2010) on worldwide prevalence of cyber attacks in critical infrastructures reported experiencing multiple large-scale denials of service attacks on a monthly basis with two thirds of those attacks impacting operations.

While there is an abundance of literature available on the subject of computer crime, very little is focused on maximizing efficiency in public agencies through analyzing current investigation models and strategies. Most of the research does not address the current state of computer crime investigation processes or how law enforcement and national security agencies work to effectively address cyber threats. Given that public authorities currently face a wide range of cyber threats, it’s important to know: (a) the ways in which law enforcement and national security agencies set investigation priorities; (b) the ways in which law enforcement and national security agencies achieve their organization objectives and goals throughout the investigation process; and (c) the operational definition of “success” as conceived by law enforcement and national security agencies.

Methods

This study employs primarily qualitative methods in research design and analysis. Document review served as the initial data collection tool. News stories taken from western media sources, reports produced by official agencies (including press releases), and public records of criminal cases reported by both law enforcement and national security agencies were reviewed for cyber investigation content. The information found in public reports and news media sources helped to identify specific cyber investigations and the corresponding federal agencies in charge of them. This data collection was useful in identifying the study participants (investigators) and preparing for interviews with them.

A second set of data was collected through semi-structured interviews with individuals employed by the Federal Bureau of Investigation (FBI), U.S. Secret Service (USSS), and Air Force Office of Special Investigations (AFOSI) who have extensive experience in cyber crime investigations. These organizations were purposely chosen for inclusion based on their responsibility for investigating cyber threats. Interviews were conducted with lead investigators (participants) and questions focused on the participants’ professional backgrounds, points of view on how they measure success in their cyber-related investigative work, and their understanding of the differences/similarities between traditional crime investigations and cyber crime investigations.

In the United States, the FBI has investigative jurisdiction over all facets of computer crime. The Secret Service is also an important agency to include in the study due to their heavy involvement in financial crimes, a major subset of cyber crime. AFOSI was chosen as it was able to provide a distinctly different perspective, specifically that of internal counter-intelligence gathering from within the federal government. Though AFOSI is a federal law enforcement agency, its jurisdiction in law enforcement is limited to the Air Force and federal government agencies only. However, by playing a role of an insider in the US military apparatus, AFOSI facilitates computer counter-intelligence related to cyber threats. Consequently, this agency has a key role at the national security level.

Investigating cyber threats: preliminary findings

This section presents preliminary findings resulting from interviews conducted with cyber investigator participants working at the FBI, USSS, and AFOSI. More precisely, the analysis focuses on three key aspects explored during the interviews. Responses were examined as to the professional backgrounds of the participants and how those backgrounds do or do not shape investigation processes and tactics. The interviewees’ responses were also culled for their perspectives on the investigation process, with particular emphasis placed on the starting point of the investigation, investigative discretionary power, and case attrition. Finally, this section reports the participants’ responses regarding investigation outcomes.

Professional background, skills, and tactics

One of the interesting characteristics noted from our interviews is the fact that none of the individuals interviewed began their career as cyber investigators. In general, the participants have between seven and eleven years of experience in the field of cyber crime investigations, though all of them started as police officers. According to their responses, the skills acquired as a law enforcement officer are critical to their current work due to the feeling that the nature of the threats in the cyber space still requires traditional law enforcement tactics. According to the interviews, it seems that a background in traditional law enforcement, combined with current work within the arena of national security, provides a valuable composite lens through which to recognize and negotiate the differences in the handling of traditional crime investigations and cyber crime investigations.

A finding reported by all interviewees was the necessity for traditional crime investigation techniques to remain an integral part of cyber crime investigations. Despite the technical nature of the crimes they are fighting, there is always a human element which is a major consideration in traditional crime solving. No matter how complicated and technological a computer crime may be, the perpetrator, the victim, and the investigator are still human.

Another reportedly critical aspect taken from traditional law enforcement techniques and featured in the response set is the ability to present investigative findings to a judge and/or jury. When a cyber-arrest is made and a prosecution begins, the preparation for court requires traditional tactics. The evidence and case against the accused needs to be presented in a form that anyone can understand and in a manner appropriate for a court of law. The members of the jury or the judge may not be as skilled in the realm of computers and information technology as the investigators are, making simplicity and clarity in presentation of evidence and investigative processes essential.

Investigation process

In a traditional investigation setting, it is widely understood that the solvability of a crime will be a critical element in the decision to conduct an in-depth investigation. Usually, the factors which determine the solvability of a case consist primarily of technical and physical evidence and other aspects such as the severity of potential damage or damage done. Though these investigative considerations are important in the case of cyber crime, they are not central. In fact, the two main considerations indicated by interview responses had to do primarily with threat elimination and the possibility of prosecution. Threat elimination relates to the level and scale of the crime itself, as well as the possibility of the investigation leading up the “chain of command” of a larger organization.

The possibility of prosecution refers to the decision of the Assistant to the U.S. Attorney in the relevant district “to be on board” with the cyber investigation case. U.S. Code, Title 18, Chapter 47, Section 1030 outlines the federal law regarding the amount of damage which must be done in order for federal prosecution to occur. This legal prerequisite represents a significant limitation to the investigative process and accounts for considerable case attrition in cyber investigations. If the loss is simply not great enough, a prosecution is not possible at the federal level. Even when the loss is sufficient for it to be considered a violation of federal law, the Assistant to the U.S. Attorney must be in agreement with the investigators to prosecute the case. According to the interview responses, if the cooperation between the investigators and U.S. Attorneys’ offices is not established in the early stage of the investigation, much effort may be wasted.

In regards to the smaller cases of cyber crime, it appears that many cases which involve less damage are often left to local police to investigate and prosecute. However, not all smaller cases are left to the locals. For example the FBI may open a lower-order case if it is believed that the case will serve as the basis of an investigation into a larger organization. This notion ties in with the concept of threat elimination and its importance to federal investigators. The elimination of larger threats may begin at the lower levels, and the trail of investigations may lead the FBI or Secret Service up the ladder or hierarchy to a larger threat. The tactic of building an investigative ladder from the lower threats to the greater threats parallels the intelligence-led policing model. Interview responses point out that the cyber criminals that pose the greatest threat are often at the top of organizations which operate on an international scale. These top-level individuals present the opportunity for the largest amount of threat elimination through a single investigation.

In general, cyber investigations are handled on a case-by-case basis. According to the study participants, no two cases are approached exactly the same way. For example, AFOSI does not actively monitor systems in the Department of Defense (DoD), over which it has investigative jurisdiction. The investigation process begins when AFOSI receives specific requests from a federal agency, such as DoD. Once a request is received, AFOSI will begin to investigate the affected system and monitor it for continued breach attempts, if the system remains online. The FBI and Secret Service begin many investigations in a similar manner, through complaints or notification from private companies or government agencies. For all three agencies, the starting point of a cyber investigation is mainly reactive or in reaction to a complaint. This observation shows a critical departure from the ILP model which places an emphasis on proactive (rather than reactive) investigation initiatives.

Beyond the initial detection, cases evolve depending on the magnitude and nature of the threat detected. This is one of the core principles of combating high levels of cyber crime as reported in participant responses. A consistent reaction to the large number of cyber cases involving a lesser severity of damage was to not pursue the criminal at all. Rather, participants' responses representing all three agencies indicated that for crimes of a lesser degree, the reaction would be to simply strengthen the target, much like the problem-oriented policing in traditional crime. For AFOSI, this translates into making or advising changes in security measures or systems. For FBI and Secret Service, they each have established extensive partnerships with private businesses, especially large businesses and financial firms[1] allowing them to exchange information on threat patterns and crime prevention. Moreover, the Secret Service also benefits from partnerships with research institutions such Carnegie Mellon University and University of Tulsa[2].

Investigation outcomes

According to all the interviewees, the perception of success within their agencies was not solely oriented toward the arrest and prosecution of offenders. Statements made by individuals from all three agencies indicated an emphasis on the maximization of threat elimination with regards to cyber crime and counter-intelligence in the realm of national security. Threat elimination is very broad and encompasses a range of outcomes from efforts to single out ring-leaders or more valuable targets to strengthening potential targets in the private and government sectors. The definition of success in cyber crime investigations, as detailed in interview responses, revealed a policy and technique which mirrors the lessons learned from studying other strategic threats like organized crime and terrorism. In other words, when the success of an investigation is defined by the number of arrests and prosecutions, the likelihood

[1] Interviewees specifically mentioned a critical collaborative effort established to protect these businesses: Infragard.

[2] At Carnegie Mellon, Secret Service agents are embedded at the institution working with civilians conducting software engineering projects to further the development of the U.S.'s protective capabilities. At the University of Tulsa, a recognized 'center of excellence' by the Secret Service, agents collaborate with students and educators in efforts to further research on cell phone encryption systems.

of an investigator going after lesser offenders is greater, which results in a safer operating environment for the more dangerous and larger players in the cyber criminal world.

The participants' responses that emanated from a national security standpoint offer some different ideas of what success means. These responses reported the possibility of gaining counter-intelligence from a cyber threat as a measure of success in an investigation. When a system is infiltrated by a cyber criminal and it is determined to be a national security issue versus a criminal issue, then the possibility of a prosecution decreases significantly. In a national security matter, the priority become attribution, discovering the country or group the individual is from. If that can be done, then the presence and activity of the individual can be used as a valuable source of intelligence. As long as the value of the information gained outweighs the risks the intruder is causing, they may be allowed to continue their activities.

Conclusion: Cyber investigation and intelligence-led policing

The federal government is currently planning to invest a vast amount of money and resources to protect public and private cyber infrastructures. Therefore, it becomes imperative to better understand the current and emerging investigation strategies and tactics that have proven effective in addressing this sort of crime. The potential for computer threats to do financial, and possibly even physical, damage has already materialized. In the face of such danger to the U.S.'s economy, public safety, and national security, it is crucial that the federal agencies protecting the country from cyber crime conduct their missions in the most efficient ways possible. This report presented preliminary findings to this end by identifying the basic measures of success and policing models currently in use by U.S. agencies. The identification of an element of intelligence-led policing in these models opens the door to further study into its effectiveness in investigating cyber crime.

During the interviews, participants described the top-down organization of computer crime on a world-wide scale. They made particular note of the relatively small number of hackers which are capable of the more damaging hacks and malicious programming, which involve only ten to twenty individuals at any given time. These high-level programmers maintain networks underneath them, keeping a strategic level of separation between the lower levels of the network and the top, thereby keeping the coders protected. Interviewees also mentioned that around ninety percent of major computer crime organizations take refuge overseas in order to avoid discovery and investigation. Cyber criminals seek out locations where they can operate with as little threat from the law as possible. One interviewee called individuals from Eastern Europe the current "masters of the universe" of computer crime. This global threat, similar to any other global threat, requires intelligence sharing and cooperation with foreign services to safeguard national critical infrastructures.

Despite the existing traces of intelligence collection and sharing combined with inter-jurisdictional collaboration, there is no evidence of a systematic application of an intelligence-led policing model to cyber investigation. This report has shown how the threat is characterized, highlighting the significance of its scope (national and international) and magnitude (volume and consequences). Despite the importance and the nature of the problem, which is comparable to the traditional threats of organized crime and terrorism to some extent, agencies addressing cyber threats seem to use a complaint-led model rather than an intelligence-led model. In addressing traditional serious crime, agencies having adopted ILP rely on both strategic and tactical assessments in order to prioritize threats and set investigation directions and requirements (Strang 2007). This differs from our participants' responses which indicate a reliance on national directives in order to prioritize threats.

Based on interview responses, it's unclear as to how much is done regarding the integration of local and regional agencies in the process of cyber investigations. For example, the "ladder" between federal and local agencies is not part of a systematic and procedural approach in cyber investigations, as it is in traditional investigations. The same observation can be made at the international level. Currently, it seems difficult for U.S. federal agencies to initiate international joint cyber investigations mainly due to the lack of harmonization in justice systems as well as varied levels of technological sophistication and investigative know-how (Lemieux 2008). Further study of the applicability of an ILP model to this type of investigative work may suggest ways for domestic and international police organizations to work around these barriers to cooperation in their mutual pursuit of cyber criminals.

Acknowledgments

I would like to acknowledge the research contributions of Brian Bales and Wilson Lee, two graduate students in the Master of Professional Studies in Security and Safety Leadership in the College of Professional Studies.

References

Carr, Jeffrey. Cyber Warfare. Sebastopol: O'Reilly, 2010.

Cavelty, Myriam. Cyber-Security and Threat Politics. New York: Routledge, 2008.

Federal Bureau of Investigation. “2005 FBI Computer Crime Survey. ” (2006). Retrieved April 9, 2010 from http://www.digitalriver.com/v2.0img/operations/naievigi/site/media/pdf/FBIccs 2005.pdf.

Hinduja, Sameer. “Computer Crime Investigations in the United States: Leveraging knowledge from the Past to Address the Future.” International Journal of Cyber Criminology. 1.1 (2007)

Internet Crime Complaint Center. 2010 Internet Crime Report. National White Collar Crime Center, 2011.

Kerr, Orin. Computer Crime Law. Eagan: Thomson-West, 2008.

Lemieux, Frederic. Information Technology in Criminal Intelligence Services: An International Comparative Perspective. In Leman-Langlois, S. (ed.) Technocrime. Columpton, UK: Willan Publishing, pp. 139-168, 2008.

Lemieux, Frederic. Normes et pratiques en matière de renseignements criminels : une comparaison internationale. Ste-Foy: Presses Universite Laval, 2006.

McAfee Labs. McAfee Threats Report: Third Quarter 2010. Santa Clara: McAfee Inc, 2010.

Mendell, Ronald. Investigating Computer Crime in the 21st Century. Springfield: Charles C. Thomas, 2004.

Peters, Sara. CSI Computer Crime and Security Survey. New York: Computer Security Institute, 2009.

Reyes, Anthony. Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors. Rockland: Syngress, 2007.

Strang, Steve. Project SLEIPNIR: An Analytical Technique for Operational Priority Setting. Ottawa: Royal Canadian Mounted Police, 2007.

Sussmann, Michael. “The Critical Challenges From International High-tech and Computer-related Crime at the Millennium.” Duke Journal of Comparative & International Law. 9:451-490, 1999.

United States. Department of Homeland Security. “The National Strategy to Secure Cyberspace”, February 2003, p.23 http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf, 10 Oct 2010.

United States. Department of Justice. Federal Bureau of Investigation.“Cyber Division”. http://www.fbijobs.gov/311132.asp, 23 March, 2010.

United States. Department of Justice. Federal Bureau of Investigation. “Cyber Crime”. http://www.fbi.gov/about-us/investigate/cyber, 30 Oct 2010.

Frederic Lemieux, Ph.D.
Director of Security & Safety Leadership (CPS)
Associate Professor, Department of Sociology (CCAS)
The George Washington University

flemieux@gwu.edu

Frederic Lemieux, Associate Professor of Sociology and Director of Police Science Program, received his PhD in criminology from the University of Montreal in 2002. Dr. Lemieux' research has focused upon social control and policing. Dr. Lemieux has also published various journal articles examining crime control during major disasters, criminal intelligence agencies, and police cooperation. He has published four books, Militarization of the Police Apparatus (2005), Norms and Practices in Criminal Intelligence: An International Comparison (2006), Homeland Security Handbook (2007), and International Police Cooperation: Emerging Issues, Theory and Practice (2010).