Future Challenges of Cybercrime

Volume 5: Proceedings of the Futures Working Group

Toby Finnie
Tom Petee
John Jarvis
Editors

Acknowledgments

The Futures Working Group and the authors that contributed to this volume wish to thank both Police Futurists International and the Federal Bureau of Investigation for supporting the efforts reflected herein. Additionally, the following individuals are recognized for their significant contributions to this volume: FBI Behavioral Science Unit Intern Angela Basso, BSU Visiting Scholar Hayley Daglis Cleary, and other staff of the FBI Training Division who provided significant assistance with the production of this volume including, but not limited to, the editing, organization, and formatting of this volume. Without their generous efforts and sincere commitment to assisting with this project, this work would not have been possible.

Suggested Citation: The Future Challenges of Cybercrime: Volume 5 Proceedings of the Futures Working Group. Toby Finnie, Tom Petee, and John Jarvis, editors. Federal Bureau of Investigation: Quantico, Virginia 2010.

Initial Release Date: September 22, 2010
Revised: November 4, 2010

Author information:

Biographical information pertaining to individual contributors and authors can be found at http://futuresworkinggroup.cos.ucf.edu.

The opinions and statements expressed throughout this volume are those of the individual authors and contributors and should not be considered an endorsement or a reflection of the official position of the Federal Bureau of Investigation, the Society of Police Futures International, or any other institution or organization for any policy, program, or service.

Table of Contents

A Word from the Chairman

The Futures Working Group, an ongoing collaboration between the Society of Police Futurists International (PFI) and the Federal Bureau of Investigation, continues to research and assemble numerous bodies of work relating to the future of policing. Many of these can be found at www.futuresworkinggroup.cos.ucf.edu. The entries in the present volume were initiated at a FWG meeting hosted by the Federal Bureau of Investigation in the Fall of 2006. I and the FWG wishes to thank all those at the Training Division of the FBI for their support during this endeavor.

During this time, a group of police managers and futurists as well as academics and military personnel gathered to consider the ongoing challenges of cybercrime. Their goal was to examine various dimensions in which the future of our dependence on computing and other electronic transactions could spell both challenges and opportunities for law enforcement.

At that time, we knew that computer crime was not only a timely topic but that it would continue to be an important issue in policing and public safety for the foreseeable future To be sure, much has recently been written about this subject; however, little has concerned itself with the future of policing and cybercrime. Clearly, there is a need for law enforcement and public safety officials to continually enhance their knowledge, skills, and abilities to keep up with the adversaries that seem to be adopting these technologies at an ever-growing pace. As the discussions progressed at this conference, it became clear that many possible futures exist with regard to this very important area. This volume is an attempt to reflect some of these deliberations and to articulate strategies to bring about what futurists refer to as "preferred futures."

As you read the entries contained herein, remember the goal of futurists--to make others think. As such, some entries are quite lengthy exploring various details of the complexities of cybercriminal behavior. In contrast, other entries are brief observations that we believe contribute to the discussion of policing and cybercrimes. All of these entries serve to introduce new, challenging, and at times disconcerting ideas. You may agree with some authors and disagree with others. You may even feel somewhat unnerved by what has been written. Often considerations of the future breed these emotions. As is constantly expressed in FWG volumes, ultimately, it is our fervent desire to devise ways to motivate individuals to create their own preferred future…--"for yourself, for your agency, and for the communities you serve."

That goal continues. We hope this latest volume and the efforts that went into it are helpful toward that end.

John P. Jarvis, Ph.D.
Senior Scientist
Behavioral Science Unit, FBI Academy
Chairman, Futures Working Group

DEFINING "CYBER-CRIME": ISSUES IN DETERMINING THE NATURE AND SCOPE OF COMPUTER-RELATED OFFENSES

Thomas A. Petee, Auburn University
Jay Corzine, University of Central Florida
Lin Huff-Corzine, University of Central Florida
Janice Clifford, Auburn University
Greg Weaver, Auburn University

In recent years, there has been considerable focus within the criminal justice system on computer-related crime. This so-called "cyber-crime" has garnered increased attention because computers have become so central to several areas of social activity connected to everyday life, including, but not limited to, personal and institutional finances, various record-keeping functions, interpersonal communications, and so on. Because of its widespread accessibility, the advent of the Internet has further served to facilitate predatory personal crimes and property offenses committed with a computer. The U.S. Bureau of Census reports that in 2000, there were 94 million people in the United States who made use of the Internet (Newburger, 2001). This greatly expands both the potential victim and offender pools for both personal and property crimes. Moreover, the nature of this forum has allowed some potential offenders to move more easily toward actual criminal behavior, because the victim(s) can be depersonalized in the initial stages of an offense. With the Internet, an offender does not have to come face-to-face with a potential target, which may make it easier for the offender to complete the victimization of the target.

But what exactly is "cyber-crime", and is it distinct from other, more traditional forms of crime? To begin answering these questions, it would be helpful to briefly look at the components of crime in general. Traditionally, crime has been defined as an intentional violation of the legal code that is punishable by the state. Central to this definition is the premise that crime occurs within the boundaries of some physical reference point, that is, a location that constitutes a specific jurisdiction. For example, when a conventional case of fraud occurs, one of the important considerations is where the actual offense took place so that questions of the appropriate jurisdiction for prosecution can be addressed. Officials need to know where the victim and offender came into contact with one another in the perpetration of the offense so that investigative and prosecutorial authority can be determined. However, this component is confounded when cyber-crime is committed because the location is no longer a static concept. With the advent of cyberspace, jurisdiction has become much more problematic, transcending local, state, and even national boundaries. One need only look at the various e-mail scams that emanate from such locales as Nigeria (i.e., the "419" scams), the United Kingdom, or China to begin to understand how crime is being redefined in the cyber-age.[1]

An equally confounding issue has to do with the scope of cyber-crime. There is a vast range of illegal behavior that could be identified as cyber-crime. Consequently, there seems to be a degree of ambiguity about what is being discussed when the subject of cyber-crime is broached. Fraud, technology theft, security breaches, identity theft, child pornography, and even stalking all potentially fall within the realm of cyber-criminality. Even within the computer community, there seems to be some disagreement about which kinds of behavior should be classified as criminal. There are some who would argue that certain forms of hacking, where a secure computer system is breached and perhaps altered, should never be thought of as a criminal act. Advocates for this position would maintain that the motivation for these actions is often not malicious and may even prove to be beneficial in terms of identifying security shortcomings. Instead, this group would rather see a focus on only those cases where sabotage or financial gain is involved (Schell, Dodge and Moutsatos, 2002). Others, including those in law enforcement communities, would strongly disagree with this position, pointing out that the so-called harmless events of hacking collectively cost billions of dollars of damage.

Some definitions of cyber-crime are relatively narrow in focus. In some cases, only hacking behavior would fall under the definition of what constituted cyber-criminality. For example, the Council of Europe’s Cybercrime Treaty makes reference to only those offenses that involve damage to data or to copyright and content infringements (see Sussman, 1999). However, most experts would agree that this definition is much too narrow and needs to take into account more traditional crimes, such as fraud and stalking, that make use of computers (Gordon and Ford, 2006; Zeviar-Geese, 1997-1998).

The legal definition of cyber-crime used in the United States takes a relatively broad view of the kinds of behavior constituting computer crime. The United States Code proscribes a range of conduct related to the use of computers in criminal behavior, including conduct relating to the obtaining and communicating of restricted information; the unauthorized accessing of information from financial institutions, the United States government, and “protected computers”; the unauthorized accessing of a government computer; fraud; the damaging of a protected computer resulting in certain types of specified harm; trafficking in passwords; and extortionate threats to cause damage to a “protected computer”

[1] “419” refers to Section 419 of the Nigerian Criminal Code. This is a variation on the classic “bait and hook” scheme, where the e-mail recipient is lured into providing personal information such as bank account numbers with the promise that they will be given a share of millions of dollars if they help the sender move funds out of the country.

(United States Code, Section 1030 of title 18). Taking into account the statutory provisions of the United States Code, the Federal Bureau of Investigation identifies a number of computer-related crimes that are part of their “cyber mission,” including serious computer intrusions and the spread of malicious code, online sexual predation of minors and child pornography, the theft of U.S. intellectual property, breaches of national security, and organized criminal activity engaging in Internet fraud (Federal Bureau of Investigation, 2006).

Despite the specific identification of offenses, the legal definition of cyber crime tends to read like a grocery list and fails to anticipate future criminal variations in cyber offending.[2] In fact, another confounding issue in defining cyber-crime has to do with the constantly changing landscape for computer-related crime. As Gordon and Ford (2006) have noted, definitions of cyber crime have evolved experientially. As technology continues to expand and as offenders become more sophisticated in their criminality, new variations in computer crime are bound to emerge. Consequently, it may be better to try to define cyber-crime in categorical terms rather than with precision. For example, Broadhurst (2006, p. 413) constructed a typology of computer-related crime, which provides a more comprehensive framework for the scope of criminal activities involved in cyber- crime. He identifies six offense categories and the current kinds of cyber crime that tend to fall in these categories:

▪ *Interference with lawful use of a computer* – which includes such crimes as cyber-vandalism, cyber-terrorism, and the spread of viruses, worms and other forms of malicious code.

▪ *Dissemination of offensive materials* – which includes child pornography, other forms of pornographic material, racist/hate-group material, online gambling, and treasonous content.

▪ *Threatening communication* – which includes extortion and cyber-stalking.

▪ *Forgery and Counterfeiting* – which includes identity theft, phishing, IP
offenses, various kinds of software and entertainment piracy, and copyright violations.[3]

▪ *Fraud* – which includes credit card fraud, e-funds transfer fraud, theft on internet or telephone services, online securities fraud, and other types of Internet fraud.

▪ *Other types of cyber-crime* – which includes interception of communications, commercial and corporate espionage, communications used in criminal

[2] This, in fact, should be expected, since the law is often reactive in nature – making provisions for new kinds of criminality only when criminal trends begin to occur.

[3] “Phishing” is generally defined as attempting to fraudulently acquire personal or other sensitive information, such as bank account numbers, passwords, or credit card information by masquerading as a trustworthy person or business in an electronic communication.

conspiracy, and electronic money laundering.

Gordon and Ford (2006) formulate an even more generic typology. Their typology includes any crime that is “facilitated or committed using a computer, network, or hardware device” (Gordon and Ford, 2006, p.14). They then categorize cyber-crime on a continuum. At one end of this continuum are offenses that tend to be discrete events, which are facilitated by crimeware programs (e.g., keystroke loggers, viruses, Trojan horses) and by the vulnerabilities of the system being exploited (identified as Type I offenses by Gordon and Ford). Examples of offenses at this end of the continuum would include hacking, phishing, and various forms of fraud. At the other end of the spectrum are offenses that involve repeated contact between the victim and offender, and which tend to use more common software (e.g., Instant Messaging, e-mail, FTP protocol) to facilitate the crime (Type II offenses). Offenses at this end of the spectrum would include cyberstalking, child predation, extortion, corporate espionage, and cyber-terrorism. The benefit of this particular typology is that it categorizes offenses according to their orientation toward either technology (the Type I offenses) or their orientation toward people (Type II offenses). Some offenses are going to be almost completely technological in nature, while others are going to be more traditional crimes that are facilitated by computers. This typology also allows for further expansion as new forms of computer-related crime emerge over time. For example, the linkage of more electronic devices through the Internet that will occur with the implementation of IP6 will increase the opportunities for the misappropriation of personal information. Similarly, the linkages of Onstar systems and cellular phones to the GPS make it possible to identify an individual’s location for criminal, as well as legal, purposes.

The question remains, however, about whether cyber-crime is distinct from other forms of crime. On one hand, every current example of cyber-crime has an analogy in more traditional crime. Several examples illustrate this point. Hacking activities are, more or less, computer-aided versions of trespassing or vandalism. When a hacker enters a restricted computer system, he/she is entering another person’s property without authorization–the definition of trespassing. Likewise, when a hacker purposely alters a website or destroys data, the action is analogous to vandalism. Various phishing schemes are essentially theft. Sexual predation, pornography, and credit card fraud are even more straight-forward, having obvious connections to their non-computer counterparts. To that end, an argument could be made that, at the present time, cyber-crime is essentially conventional criminal behavior that makes use of computers.[4] From this position, the

[4] In fact, Gordon and Ford (2006) argue that the term “cyber-crime” should be removed

impact of the computer on crime is not that it opened a Pandora's Box of criminal behaviors that previously had been impossible to perform.[5] The primary implication of computers, the Internet, and cyberspace for policing is how to adopt traditional and/or develop new enforcement strategies to existing criminal offenses that are completed or facilitated through a new channel or medium of communication. This line of argument is not intended to belittle the challenges of cyber-crime for the law enforcement community, however. The scope of changes in society that are occurring through the adoption of computers have not been seen since the invention of the automobile and airplane in the early-20th century revolutionized transportation. We believe that cyber-crime will be the primary challenge for policing in the 21st century.

On the other hand, any discussion of police futures pertaining to this topic has to consider what cyber-crime may look like in the coming years. While it is likely that the use of computers in the commission of crime will continue to expand in the near future, it is more difficult to envision a unique form of offending emerging that would fall into the categorization of cyber-crime. Nonetheless, the possibility of such an offense surfacing at some point in the future cannot be dismissed outright.

A final related issue that complicates the examination of cyber-crime has to do with the determination of its frequency of occurrence. To put it simply, it is extremely difficult to measure the extent of cyber-crime occurring in the United States. This is in large part due to the fact that when cyber-crime is recorded by authorities, it is not necessarily recorded as a computer-related offense. Rather, it is most often recorded as a case of fraud, pornography, or some other conventional crime. Consequently, the scope of cyber-crime, at least as far as official statistics are concerned, is masked by reporting and recording practices. Presently, the best data available on the question of the extent of cyber-crime are found in survey data, particularly the FBI's Cyber-Crime Survey. These data, however, can only give us an estimate of the scope of cyber-crime. The lack of substantial data on computer-related crime may be another argument against classifying cyber-crime as a unique form of criminality at the present time. Yet, it may also be a reason for more clearly defining, and thus being able

from our lexicon entirely, although they concede that it likely never will.

[5] The logical and obvious exception to this line of reasoning is the theft of computer hardware or software or of digital information, specific examples of theft that were impossible before the existence of the products.

to measure, cyber-crime. Therefore, it is important that we offer what will likely prove to be a temporally bounded definition of cyber-crime that can be useful for the present day. To this end, we define cyber-crime as “any criminal offense that is committed or facilitated through the use of the communication capabilities of computers and computer systems.”

REFERENCES

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management*, *29*, 408-433.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*, *2*, 13-20.

Newburger, E. C. (2001). *Home computers and internet use in the United States: August 2000* (Current Population Reports). Washington, DC: US Bureau of Census.

Sussman, M. A. (1999). The critical challenges from international high-tech and computer-related crime at the millennium. Duke Journal of Comparative and International Law, 9, 451-489.

Zeviar-Geese, G. (1998). The state of the law on cyberjurisdiction and cybercrime on the Internet. [Electronic version]. *Gonzaga Journal of International Law, 1.*

POLICING THE DIGITAL ENVIRONMENT

Toby M. Finnie

The Wild, Wild West: Part I

The development of telegraphs and networks is significant for understanding the Internet because it demonstrates the relentless push toward more speed, more capacity, more raw volume, more "consumers."

— Anne B. Keating[i]

I sat at my desk, glumly mulling over an assignment. With a deadline looming, an analysis discussing the near and far future of Internet crime's impact on the department seemed no nearer completion than it was a month ago when Assistant Chief Murphy assigned it to me.

Strategic planning? It was difficult to grasp how cybercrime might affect us next month, let alone twenty years from now! I couldn't seem to draw a bead on it. Every week there seemed to be a new techno-toy, or news of a new computer crime scheme. If the bad guys weren't hacking they were phreaking, pharming and phishing.[5] I felt as if I was trying to grab smoke!

I glanced heavenward and silently thanked Hiram B. Thomas, my 92-year-old grandfather, for a temporary reprieve. When I'd spoken to him a week before he died, I'd griped about the cybercrime report. There was nothing, I grumbled, that could compare to the impact cybercrime was having on law enforcement.

If I was looking for sympathy (and I was) I didn't get it from Granddad.

"Your grandma used to say 'There's nothing new under the sun!'" Granddad had replied, "You're a smart boy. You'll figure it out."

The temporary reprieve arrived in the form of a small package mailed by the Executor of Granddad's estate. My grandfather had died before he could deliver it to the post office.

Curious, I opened the package. A note, written in my grandfather's shaky, not quite indecipherable hand was wrapped around an old leather-bound journal. It read:

> "This belonged to Anna Parker Thomas, my great grandmother. She was born in Chambersburg, PA in 1846. When Civil War recruitment depleted the local work force — and took away the eligible young bachelors, Anna hired on as a messenger with the Adams Express Company in 1862. She promoted to telegrapher a couple of years later.6 I think you will find her journal useful

[5] "Phreaking" involves theft of telecommunication services. "Phishing" attempts to capture personal information by prompting users to visit a fake website. "Pharming" redirects a user to a fake website without the user being aware of the redirection.

[6] Many believe that women first entered the telecommunications industry as telephone operators, to replace the unruly boys who were employed to operate switchboards. However, when the telephone was first publicly demonstrated, in 1876, women had already been part of telecommunications technology for thirty years — as telegraph operators and managers. *See* Schlereth, Thomas J. (1991) *Victorian America: Transformations in Everyday Life 1876-1915* (New York: Harpers Collins 1991) p 4

as you prepare to write your report. Remember, there is nothing new under the sun! — Granddad."

I spent the next hour skimming through Anna's journal. Covering 25 years of telegraph, railroad and personal history, her entries wove a fascinating tale of her life and times working for the Wild, Wild West's first version of the Internet: the telegraph.

The Pacific Telegraph Act of 1860[7] called for the facilitation of communication and a year later, Western Union networked with several other telegraph companies to link the east and west coasts of the United States. Six years later, a transatlantic telegraph cable connected the United States with Europe.

In May 1869, Union Pacific and Central Pacific conjoined tracks to become the first transcontinental railroad, opening the western territories to expansion. Following along railroad rights of way, telegraph wires crisscrossed the country, awed the public, and forever changed the conduct of business.

That the public was enthralled by the rapid transmission of dash-dot encoded messages was an understatement, in light of the fact that mail sent from St. Louis, Missouri to Sacramento, California via Pony Express took 11 days.[ii]

The "email" of its day, a telegraph message could be encoded and transmitted from San Francisco to New York in under fifteen minutes. Even more noteworthy, the same message could be transmitted to thousands of recipients, paving the way for snake oil salesmen to mass-market worthless products.[iii]

Two days after the intercontinental telegraph was completed the Pony Express became obsolete and hung up its saddles forever. Other businesses flourished.

Richard Sears, a telegraph operator and railroad station manager, started a mail order service to sell watches via the telegraph. His business developed into what would later be known as the Sears-Roebuck Company. All manner of goods could be ordered by telegraph and shipped by express companies: even mail-order brides![8] Thomas Edison introduced the stock ticker and printing telegraph. In Europe, the Associated Press formed an alliance of Morse telegraph services and transmitted news dispatches worldwide.

Relationships and romances heated up the telegraph wires.[iv] Alexander Graham Bell was even said to have complained about "unseemly" messages exchanged between telegraph operators. Telegraphers developed their

[7] The Pacific Railway Act, July 1, 1862. *An Act to aid in the Construction of a Railroad and Telegraph Line from the Missouri River to the Pacific Ocean.* (U. S. Statutes at Large, Vol. XII, p. 489 ff.)

[8] In addition to a regular money order service, the telegraph companies maintained a telegraphic shopping service, permitting the purchase by telegraph of any standardized article that could be picked up or delivered by parcel post or express. SEE *Ross, Nelson E. How To Write Telegrams Properly.* 1928 *http://www.telegraph-office.com//pages/telegram.html#How%20to%20Save*

own jargon in Morse code and when business was slow, they played games with other telegraph operators.

> For amusement at such lonely stations, two telegraph operators, maybe 75 miles apart, would both plug into the same “spare telegraph wire circuit” and play games by wire such as chess or checkers or certain playing-card games, or maybe just to “chew the rag” or listen in on Western Union and get the latest news even before it came out in the city newspapers.[v]

The telegraph further extended its reach in May 1897 when Guglielmo Marconi transmitted the first wireless telegraph communication over water.

Expanding railroads, telegraph and express delivery companies set up agencies in the territorial West so their businesses could be managed remotely. Entrepreneurs, cattlemen and homesteaders settled near the agencies. As a consequence, communities rapidly developed where buffalo formerly roamed.

The U.S. Post Office took advantage of the rail systems, shipping huge volumes of mail across the country, even sorting mail while in transit. Express companies delivered commodities and transported gold, securities and cash via rail car. Commerce was on the move and following the money, so were the criminals:

> By the very nature of their physical construction, railroads became the prime prey of many well-organized bands of outlaws. Theft was rampant and the losses in dollars of freight, parcels and luggage were overwhelming to the railroad companies. Bridges, tunnels, stations, tracks and railroad cars were dynamited in daring holdups. Following the Civil War, thousands of unemployed soldiers/hobos took to the rail yards and to the rails to loot and rob.[vi]

Just as flim flam artists promoted bogus lotteries and other get rich quick schemes via the telegraph, opportunistic outlaws also took advantage of new technologies. They rode fast horses, used high-powered rifles and smokeless powder (so they could fire at pursuers from a distance without giving themselves away). They hired safecrackers to help them break into safes and employed explosives experts to blow up railroad tracks and trestles.

Family members and gullible young men looking for excitement were recruited to join outlaw gangs. In Highwaymen of the Railroad,” William Pinkerton wrote:

> “The majority of these robbers are recruited from among the grown boys or young men of small country towns. They start in as amateurs under an experienced leader. They become infatuated with the work and never give it up until arrested or killed.”[vii]

Outlaw gang members wore disguises and used aliases — “Kid Curry” (aka Harry Logan), “Tall Texan” (aka Ben Kilpatrick) and the “Sundance Kid” (aka Harry Longbaugh) were but a few — to mask their identities.

They were enticed by large sums of money and showed little fear of arrest for their meticulously planned and well-executed robberies. They hacked into telegraph systems to monitor law enforcement activities and cut telegraph wires to impede police operations.

Unlike romanticized, movie-inspired portrayals of outlaws leaping from horseback onto moving railcars, robbers gained access by laying in wait and attacking when trains stopped at refueling stations. Sometimes railroad tracks were dynamited or trestles were burned, with resulting injuries and death to passengers and crewmen when train cars derailed. Gawking passengers, curious to see why their train was "held up," were sometimes shot for their inquisitiveness.

To avoid arrest, some gangs split up and escaped across state lines or territorial and international borders. Others retreated to remote hideouts. Some gangs (the James Brothers, for example) made no effort to hide; so confident were they of community protection.

Federal response was lethargic. The U.S. Army had jurisdiction over the territories but the army was no good at policing and already had its hands full dealing with Indian Wars. U.S. Marshals also had jurisdiction but were very thinly spread, out-manned and out-gunned. They were often forced to deputize posses or seek assistance from citizen vigilance committees. Some frontier towns were lawless and dangerous. The outlaws "became terrors to the community in which they lived. It was impossible to get the necessary evidence to convict them, as, to a certain extent, they controlled, through terrorizing, some of the local judges; and the local authorities, either through sympathy or fear, were afraid to do their duty."[viii]

Local law enforcement (where there was local law enforcement) was overwhelmed. Police had expanding responsibilities, limited operating funds, and poorly trained personnel. Only the larger police agencies could afford to keep up with technology. The smaller agencies were forced to make do with what they had—and what they had wasn't much. Federal criminal statutes were all but nonexistent; state statutes were inadequate.

Even so, police worked with the tools they had. They printed and distributed wanted posters and shared information with neighboring law enforcement agencies via telegraph. To help maintain law and order, they deputized citizen posses and sought the assistance of private sector investigators. (Unknown in local communities, private investigators could more easily conduct covert investigations, especially in situations where the outlaws controlled the citizenry.)

The railroad and express companies, needing to protect assets, fought back. They pressured politicians to enact statutes such as the Pennsylvania Railroad Police Act (1865)[9] and the

[9] On February 27, 1865, the Pennsylvania legislature enacted the Railroad Police Act — the first act officially establishing railroad police. The act authorized the governor of the state to appoint railroad police officers, and gave statewide authority to these officers. This act provided the model legislation for the other states to follow. Norfolk Southern Police Department. *History of Railway Police.*

federal Mail Fraud Act of 1872 — the country's oldest consumer protection statute.[10] They lobbied Congress to make train robbing a capital offense.

Railroad companies started up their own police departments and lured experienced police investigators away from public service with offers of higher salaries.

To protect shipments and property, express companies hired guards and armed them with high-powered weapons. They reinforced strongboxes with iron stropping and bolted them to coach and railcar floorboards. They purchased heavy-duty safes and limited employee access to the combination lock codes. They contracted private detectives to relentlessly hunt down perpetrators.

A standout agency of its time was the Pinkerton National Detective Agency.[11] After enjoying a brief stint as a detective with Chicago Police Department, Allan Pinkerton started up the agency in 1851. The "Pinks" were highly successful in solving train and express company robberies, in no small part due to guiding principles and innovative investigative techniques developed by Pinkerton himself.

Pinkerton demanded the utmost integrity from his operatives and instilled in them a strict code of ethics. He hand-picked agents for their intelligence, perceptiveness and courage and in 1856 hired the first female detective in the U.S. — forty years would pass before police departments began to hire women — and Kate Warne would become one of his most successful operatives.

Working with technologists, telegraphers, and firearms experts, Pinkerton strove to ensure that his agents had up-to-date training, the newest equipment and the finest investigative tools. His agents participated in crime dramatizations and role-playing exercises, learned to wear disguises and assume various personas.

The Pinkertons incorporated science and technology in ways that presaged and shaped the future of public sector crime fighting, including crime analysis and crime mapping:

> So frequent and routine were the Gentleman Bandit's stagecoach holdups over the years that the Pinkertons had been able to plot his movements on a map of the American West.[ix]

By the 1870s Allan Pinkerton, together with his sons William and Robert, had compiled the largest collection of mug shots and criminal profile data in the world. [x] Pinkerton agents in the field gathered information about criminals from police, informants, and especially from newspaper articles.

<http://nspolice.com/history4.htm. Assessed June 1, 2007.

[10] Enacted June 8, 1872, ch. 335, § 301, 17 Stat. 283 (codified at 18 U.S.C. 63 § 1341), the mail fraud statute was one section in a recodification of the Postal Act.

[11] So profitable was Allan Pinkerton's business model that the Pinkerton National Detective Agency has been in continuous operation for one hundred and fifty-six years. Securitas AB, a Swedish company, acquired *Pinkerton* & Burns Security Services (formerly Pinkerton National Detective Agency) in July 2003. Securitas is one of the largest security companies in the world.

The information was then telegraphed to the main office in Chicago. When warranted, mug shots[12] and criminal profile data was relayed to Pinkerton and police investigators. [13]

The crime data was also used in reward posters and information bulletins such as Pinkerton's Criminal Mug Shot & Information Book that was provided to members of the American Bankers Association. That book listed photos, descriptions and general information, including handwriting samples, about 300 known criminals and described criminal "methods of forgers, sneak thieves, robbers and swindlers." It also provided tips to banks on entrapping criminals before calling the police.[14]

Pinkerton was a founding member of an organization that became known as the International Association of Chiefs of Police (IACP). As a director on the IACP board Pinkerton's vision for a centralized bureau to collect, store and maintain criminal data became a reality in 1897 with the creation of the National Bureau of Criminal Identification. In 1924, the records were permanently transferred to the Federal Bureau of Investigation.

The Pinkertons also developed a secure method for sharing sensitive information via telegraph through the use of cipher text. Copies of the cipher code were distributed to the American Bankers Association and other clients.[15]

Pinkerton agents' pursuit of suspects was relentless, even across international borders. Agents hounded outlaws Butch Cassidy and the Sundance Kid in Argentina. Dogged pursuit of the Reno Brothers after they fled to Toronto, Canada led to extradition agreement revisions between the two governments.

Pinkerton and his sons educated the business community, offering "advice and preventative measures to banks,

[12] Invented and in use by 1851, the Pantelegraph, an electrochemical telegraph, was able to transmit graphic images so that "together with the proclamation for somebody's arrest it can also provide a portrait of the criminal." Castella, Bjarne (n.d.) *The Predecessor of the Facsimile from the Last Century* (Post & Tele Museum, Denmark) <http://www.teponia.dk/museumsposten/index.php?artikelid=157> Accessed March 23, 2007

[13] Of the 195 criminal investigations binders, two-thirds cover the period of Pinkerton's greatest activity in criminal work, from 1880 to 1910. The binders contain photographs and sketches of criminals, suspects and gang members, as well as Pinkerton operatives; photographs and illustrations of burglar tools, safe-cracking equipment, and crimes in progress; "Reward" and "Wanted" posters and handbills; many press clippings from 1870 to 1938; penciled daily draft reports from detectives; criminal histories (Pinkerton "rap sheets"), gang histories, and crime chronologies. Also included are "office narratives," written by clerks, covering all or parts of an investigation; interoffice communications concerning investigations; correspondence with local law enforcement officials; correspondence with Pinkerton informants; letters to Pinkerton from criminals; and correspondence between criminals. SEE Urschel, Donna (2000) *The First Private Eye: Library Receives Pinkerton Archives*. The Library of Congress: Information Bulletin 2000) http://www.loc.gov/loc/lcib/0006/pink.html> Accessed May, 2007

[14] Samples of Pinkerton's Mug shot books can be viewed at this link: <http://www.pimall.com/nais/pivintage/pcriminalphotobook.html>

[15] Samples of wanted posters and information flyers can be viewed at this link: <http://www.pimall.com/nais/pivintage/telegraphcipher.html>

shipping offices, mail services and other enterprises that dealt with the handling and movement of money."[xi]

Nearly sixty years transpired between the first train robbery in 1866 and the last recorded hold-up in 1924. A concerted partnership effort by police, business owners, private investigators, legislators and ordinary citizens finally put a halt to the "hold ups."

I had been born into the generation of grade school students who enjoyed the smell of freshly mimeographed papers. I learned to type on manual typewriters. I didn't know much about the history and development of digital technologies that emerged in the '90s, but Granddad's axiom that "there is nothing new under the sun" resonated deeply.

As Granddad had implied I would, I was beginning to see the analogous relationship between the technological challenges faced by 19th Century detectives and 21st Century cybercrime investigators.

The Wild, Wild West: Part II

“If we aren't vigilant, cyber crime will turn the Internet into the Wild West of the 21st century,”
Janet Reno, U.S. Attorney General (1998)

One hundred years after telegraph wires snaked across the U.S. continent, new technologies converged once again to revolutionize the conduct of business around the world: the microchip, the desktop computer, and the nascent Internet.

In 1969, The U.S. Department of Defense funded a network research project to facilitate information sharing between geographically distant nuclear physics researchers. Two years later, the “ARPANET” project was deemed a success when four universities briefly communicated through networked computer terminals.

As new network tools and applications were developed, tested and refined in the next decade, more universities in the U.S., Canada and Europe connected to the ARPANET, making it the first international network.

Computer scientists and engineers who used the network were delighted. They no longer had to wait days for the postal service to deliver an important research paper from a distant colleague. An electronic copy of the paper could be retrieved through ARPANET in a few minutes time — even if the computer they retrieved it from was thousands of miles away!

If struggling to solve a knotty physics problem, a researcher only had to type out a single query, send it to an appropriate newsgroup such as

Internet Milestones

1970: Electronic Mail (EMAIL). Text messages could be transmitted to recipients across the ARPANET. Researchers appreciated ease-of-use, informality and rapid transmission of messages.

1980: The User’s Network (UUNET). Distributed Bulletin Board Systems (BBSs) provided decentralized communication between geographically distant users. Using a modem and telephone, a participant could log into UUNET to leave a message and to read other users’ responses. Messages were typically grouped by topic into “newsgroups.” By 1999 there were tens of thousands of newsgroups participating.

1983: The Transmission Control Protocol/Internet Protocol (TCP/IP) networking procedure was formally adopted by ARPANET and all supplementary networks connected to it. Collectively those systems become “the Internet.”

1988: Internet Relay Chat (IRC). Users anywhere in the world could “converse” in real time with other users through exchanges of typed messages.

1988: Search engines were developed to categorize, index and sort through the massive amounts of knowledge that was accumulating: text files, images, and databases.

1989: Mailing Lists (Listservs). An automated process that enabled an email message to be transmitted to multiple users who had interest in the same topic.

1989: First Public Internet Service Provider (ISP): The World.com offered dial-up Internet connection services available to the general public.

1990: Management turnover. US Department of Defense moved classified data to its own network, MILNET, turning over management of the Internet to the National Science Foundation (NSF) through its network, NSFNET. At its peak, NSFNET connected more than 4,000 institutions and 50,000 networks across the Unites States, Canada, and Europe. Commercialization restriction is lifted.

1991: World Wide Web (WWW). The development of hypertext computer language and launch of “The Web” provided easy access to information.

1992: Multimedia: First audio and video multicasts were successfully demonstrated online.

1993: Web Navigation Software (Browsers). The earliest web browser, Mosaic, and later its commercial version, Netscape, incorporated text, sound and video into an easy-to-use graphical application that neatly integrated three Internet technologies: web, email, and newsgroups.

1995: NSFNET transferred management of the Internet to independent organizations.

"alt.physics" and request feedback from other researchers. Replies from colleagues were often immediate.

By 1983, networks, computers and network software applications switched to a standardized communication protocol called Transmission Control Protocol/Internet Protocol ("TCP/IP"). With that changeover, ARPANET began to be called the "Internet." In 1984, the numbers of terminal hosts ("users") reached 1,000 and still even more universities signed on. By 1989 there were over 100,000 users.

The Internet was no longer the exclusive domain of scientists and engineers using arcane computer languages on mainframe computing systems. Their orderly world was becoming more chaotic: Students, unsupervised and relatively undisciplined, were now flocking to the Internet, logging on from desktop and laptop computers.

In November 1988, a 23-year-old student named Robert Tappan Morris introduced code into the Internet network, as part of a research project he claimed he was conducting. Morris intended for his self-replicating "worm" code to measure the size of the Internet. Unfortunately, the code was flawed and caused thousands of computers logged onto the Internet to become inoperable.[16] The "Morris Worm" story was extensively reported in the news.

Other, more sinister characters began to probe deeply into the Internet. In his novel, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, author Clifford Stoll described a network intrusion incident that occurred in 1986. Stoll recounted his tedious but patient tracking of an intruder through a university network and into various military computers on MILNET. Stoll traced the illegal activity to Markus Hess, a 25-year-old German citizen who was recruited by the Russian KBG to hack into and steal sensitive information from US military computing systems. Stoll experienced a great deal of frustration in attempting to gain the interest and investigative support of law enforcement:

> Stoll contacted various agents at the FBI, CIA, NSA, and Air Force OSI. Since this was almost the first documented case of cracking (Stoll seems to have been the first to keep a daily log book of the cracker's activity) there was some confusion as to jurisdiction and a general reluctance to share information (Stoll quotes an NSA agent as saying, "We listen, we don't talk").[xii]

The fledgling Internet was not built to guard against such attacks and penetrations. Internet engineers were given pause to consider what the long-term impacts might be. Network security became a hot topic of discussion.

World.com, the first commercial Internet Service Provider (ISP) in the United States, began offering dial-up connectivity to the public in 1989. Any World.com customer with a computer

[16] Robert Morris was tried and convicted of violating the 1986 Computer Fraud and Abuse Act. After appeals he was sentenced to three years' probation, 400 hours of community service, and a fine of $10,050. He is now a professor at Massachusetts Institute of Technology.

and a modem could dial-up, log on, and cruise the Information Highway.

Navigating the complex architecture of the Internet network challenged the skills of individuals unfamiliar with complex computer command line syntax. The introduction of the "World Wide Web" and web browser applications, such as "Mosaic" and "Netscape," helped to propel delighted users from email, to newsgroups, to World Wide Web exploration, all from one user-friendly interface.

In 1990, Department of Defense migrated all classified information to a proprietary network and assigned Internet management responsibilities to the National Science Foundation (NSF). At the end of the year, about 300,000 users were accessing the Information Highway.

The Internet community of users was excited about NSF's plans to open and fully promote the Internet to commercial enterprises.

> From the time the National Science Foundation (NSF) assumed responsibility for the U. S. Internet backbone, they anticipated a transition to commercial use. There were a few commercial ventures in the 1980s, like the Clarinet News Service, CARL UnCover for scholarly documents, and the Computists' Communique electronic newsletter, but the NSF acceptable use policy and Internet culture were largely non-commercial. NSF is phasing out their support, and commercialization is taking off — you can even order pizza![xiii]

The Federal Networking Council (FNC), responsible for coordinating networking needs among U.S. Federal agencies, determined that the Internet was "a critical resource for the national research and education communities" and concluded that the Internet "…should be made available to the widest possible customer/user base with the highest possible level of service."[xiv]

As Internet Service Providers (ISPs) opened for business across the country, growth rates escalated. In 1994, there were three million users perusing 10,000 newsgroups and 10,000 websites. A year later there were 6.5 million users and the number of websites had increased to 100,000.

The NSF quietly transferred its network management responsibilities to independent organizations on April 30, 1995. The Internet's doors were thrown wide-open for commercial business. The times, they were a-changing.

One Internet user ("netizen") bemoaned the changes but also expressed hope for the future:

> The Internet …was formed in an atmosphere of craftsmanship and information exchange, which persists today. … Perhaps more important, the Internet culture supports open communication. People answer questions, make suggestions, and freely discuss a myriad of topics for the satisfaction of participation and perhaps some enhancement for their reputation — the payoffs are not explicit. This barter/gift-exchange arrangement makes for a more comfortable society than one in which every information transaction is explicitly compensated, and no

> accounting is needed. This open culture is subject to abuse, but it has persisted for years on the Internet. Will increased commercialization end openness? Must it? Can we find policies that balance openness and marketplace efficiency? Social predictions are difficult at best, and the global nature of the Internet makes them even more difficult.[xv]

At the end of 1996, the Internet community consisted of 12.8 million users and a half million websites. The Internet was primed to become Wild Wild West (version 2.0).

The Wild, Wild West: Part III

The dynamics of global growth are changing at least as profoundly as they did with the advent of railroads or electricity. The evolution of the Internet as a pervasive phenomenon means that the traditional factors of production — capital and skilled labor — are no longer the main determinants of the power of an economy.[xvi]

Business Week Online (1999)

In 1994 Forrester Research predicted Internet sales would grow to $4.8 billion by 1998.[xvii] Only a few years later an even rosier economic forecast was reported:

> People are becoming more comfortable with the technology, and businesses are pushing web transactions as a way of reducing costs and increasing efficiency. Efficiency and competitive pricing in the Internet's "frictionless" marketplace are expected to dramatically increase business-to-business sales over the Internet. Richard Prem of Deloitte & Touche expects business-to-business transactions alone to exceed $300 billion by the year 2002. Forrester Research has predicted total web sales of $1.45 trillion by the year 2003.[xviii]

The business community had finally awakened to the huge market potential in Internet sales and the rush was on. It was "Internet or bust!" Everyone wanted a piece of the action and to flaunt the newest status symbol: a web address.

Amazon.com opened a virtual bookstore in 1994, promising customers an enormous selection of new and used books. In 1995, "eBay" started an online auction service where users could sell items by way of the Internet, and later introduced "PayPal" payment processing for online vendors. PayPal customers could send, receive, and hold funds in 17 currencies.

All manner of goods could be ordered from the Internet and delivered by regular mail or express companies. A few Russian websites even offered mail-order brides! Stock brokerages went online, as did financial institutions. The Associated Press, CNN and other news media began to distribute information across the Internet.

Online chatrooms spawned friendships, romances and sometimes even marriages. On the seamier side of the Internet, pirated software, hacker's tools, and child pornography images were freely distributed. Concerns were raised about the exploitation of children by pedophiles. Several well-publicized arrests and convictions of huge pedophile rings got the public's attention, but failed to deter the pedophiles. In seemingly endless numbers they continued to slither through the Internet's underground.

Internet users developed their own jargon: IM (Instant Message), LOL (Laughing Out Loud), IIRC (If I Recall Correctly). Special interest groups formed social networking communities, interactive gaming and gambling sites, and discussion forums. Students emailed bomb threats to their teachers and mercilessly harassed other students online. Grifters traded swindling techniques.

Handheld wireless devices such as “Smartphones” and “Personal Data Assistants” allowed users to “go online” without the need for a telephone dial-up connection. Voice Over Internet Protocol (“VOIP”) telephone services enabled clandestine phone conversations to be held over the Internet — and under law enforcement’s radar.

Huge volumes of email, including junk email (“spam”) and invitations to provide personal information to fraudsters were transmitted across the country and around the world. Express companies delivered commodities that had been purchased online. Commerce was on the move and following the money, so were the criminals:

> The United States economy, including the growing e-commerce aspect of it, is increasingly threatened by cyber economic crime. Multiple studies still show that fraud, security, and privacy continue to be the primary detriment to the growth of e-commerce. Most economic crimes have a cyber version today. These cyber crimes offer more opportunities to the criminals, with larger payoffs and fewer risks. Websites can be spoofed and hijacked. Payment systems can be compromised and electronic fund transfers to steal funds or launder money occur at lightning speeds. Serious electronic crimes and victimization of the public have caused consumer confidence to waiver. These issues have also lead to growing privacy concerns and demands. In turn, the reluctance of the American public to embrace e-Commerce fully is preventing this new form of business from reaching its potential. We are quickly eroding the trust in our society that has been built up over the centuries.[xix]

Anxious to mitigate liability and stop loss due to credit card fraud and theft of company intellectual property and customer information (“data leakage”), businesses began to take security more seriously in the twenty-first century. More robust security protocols and access controls were put into practice. Employee background checks became a more common practice. In-service employee training on security and data protection was initiated and acceptable use policies were drafted and put into effect. Corporations lobbied Congress for more protection.[xx]

Some businesses and government agencies initiated customer awareness “Internet fraud” prevention programs, sending information in mailings and posting notices on websites — to little avail. Increasingly Machiavellian “phishing” and “pharming” attacks continued to elicit personal information from unsuspecting customers.

Opportunistic Internet outlaws used the Information Highway as their personal road to riches. They used high-end computers and stealth technology such as proxy servers, encryption, steganography and phony (“spoofed”) email addresses. They probed for weaknesses in networks and hijacked accounts to harvest information they could further exploit for profit.

> “Around one in four criminals use false identities, with identity theft

> being both a means of masking the criminal's own identity and therefore evading detection — as well as a vehicle for committing further fraud at a later date."[xxi]

Teenagers who were bored and looking for excitement were recruited by organized crime into "hacker" (network intrusion), "carder" (credit card theft) and "phreaker" (telecommunication services theft) gangs. Teens had a significant advantage over investigators: time — time to learn and hone their skills. Many were enticed by the promise of large sums of money and scoffed at the idea of being apprehended by law enforcement.

In 2001, Assistant U.S. Attorney Sean B. Hoar referred to identity theft as "the fastest-growing financial crime in America and perhaps the fastest-growing crime of any kind in our society, because offenders are seldom held accountable."[xxii]

Perpetrators victimized multiple victims in multiple jurisdictions, making investigations especially challenging. Others operated remotely from safe harbors such as Nigeria and Sierra Leone and made no effort to hide. They knew U.S. law enforcement couldn't touch them.

In spite of the ongoing criminal activities and threats to national security, there was no Internet Highway Patrol to maintain law and order. Police were about twenty years behind the technology curve.

The proliferation of desktop computers and boomtown atmosphere of the Internet took police managers by surprise. It didn't help that commanders were averse to using computers. (Parents were experiencing the same problem at home: kids knew more about computers than the adults.)

The larger police agencies could better afford to keep up with technology but for the most part, it was old technology: dumb terminals networked to mainframe computers. It would be well into the first decade of the new century before most police regularly sent and received email and used the Internet as a resource and investigative tool.

The smaller agencies were forced to make do with what they had—and what they had wasn't much. Some of them didn't have computers, let alone email or Internet connections. The smaller agencies felt "high tech" if they used facsimile machines. It was sadly ironic that grade school students had better, faster computers than most police.

A few investigators had an interest in computers and taught themselves the skills they needed to investigate "cybercrime" and they shared their knowledge with other investigators.

> In those days, we were working without resources, real knowledge, or awareness and exposure to computer violations. We were not experts. We worked hard to overcome the critical gap between the knowledge of those investigated and the knowledge of the investigators.[xxiii]

Some of those early law enforcement pioneers would later become founding members of computer crime-fighting associations such as High Tech Crime Investigators Association and International Association of Computer Investigator Specialists.

Software developer companies responded to law enforcement's request for forensic tools to assist investigators to preserve and analyze digital evidence. Some of the early pioneer-developers were Access Data, ASR Data, Mares & Company, New Technologies, Inc., and Norton Utilities/Symantec.

In September 2000, the National Institute of Justice published results of a survey identifying issues and obstacles that interfered with successful investigation of cybercrime. State and local law enforcement agencies reported they lacked adequate training, equipment and staff to meet present and future needs to combat electronic crime. Among the findings, there was a demand for:

- Uniform training and certification courses
- Development of electronic crime units
- Investigative and forensic tools

Additionally, NIJ reported that "acquiring appropriate investigative hardware and software poses one of the biggest problems, as such tools are often beyond the budgets of most law enforcement agencies. Findings indicated a large gap between the expertise and resources of many cybercriminals and the agencies that investigate them."[xxiv]

Five years later another survey sponsored by NIJ demonstrated that law enforcement agencies were still struggling to get up to speed on the Information Highway: [xxv]

- Most agencies had no digital evidence unit or resource
- Most agencies did not find or collect digital evidence in most of their investigations
- Only half of state and local law enforcement had attended digital evidence awareness and handling training
- A majority had no policies concerning digital evidence

Investigators who had computer forensic analysis training complained that most of their commanders didn't grasp the scope of the problem. Said one investigator, "I finally got enough training that I felt somewhat confident about my forensic skills and they rotated me back to patrol. All that training — wasted!"

Other officers claimed that they were appointed the "computer forensic guy" because they knew how to boot up a computer.

Another investigator complained about the procurement process. "I'd ordered a new computer workstation to use in the forensic lab. It took nearly a year for the purchase order to be approved. The day I got approval was the same day new computer models went out on the sales floors. I was stuck: forced to buy out-dated technology!"

Federal criminal statutes were inadequate and needed updating. For example, federal statute, 18 U.S.C. 1028, addressed the fraudulent creation, use or transfer of identification documents. There was no provision for theft or criminal use of personal information. Enacted on October 30, 1998, the “Identity Theft Act,” contained an amendment that criminalized fraud in connection with the unlawful theft and misuse of personal identification.[17]

As late as 2007, some states still were without criminal statutes to address computer intrusion or identity theft.

Many of the cases involved transnational investigations but police had limited means to seize foreign perpetrators’ digital evidence. The formal Mutual Legal Assistance Treaty or Agreement (MLAT or MLAA) processes through U.S. Department of Justice Office of Foreign Affairs was far too time consuming. It took so long to process the paperwork that by the time the legal documents were in order, the volatile digital evidence was no longer recoverable.

Local prosecutors refused to extradite out-of-state suspects for “small dollar loss” cases, even when the combined loss from multiple victims in other jurisdictions was substantial — but not substantial enough to interest federal prosecutors. Federal prosecutors weren’t interested in small dollar loss cases, either.

Victims grew upset, feeling that their complaints were ignored, which for the most part they were: 25% couldn’t even get the police to take a report.[xxvi] Some agencies played “pass the victim” — local police referred victims to a federal agency, that agency referred the victim to another agency and so on, until finally the victim gave up in frustration.

In another example of “victim abuse,” the Las Vegas Sun reported that 300 victims requested assistance through a telephone hotline associated with the Nevada Attorney General's Identity Theft Passport program that was set up to “help identity theft victims clear their name.” Not one of the callers received any assistance whatsoever. According to the article, state officials said the lack of assistance was due to a lack of funding.[xxvii]

Meanwhile, the media constantly broadcast news stories about millions of identities being stolen, traded, or lost. Internet sales were dipping. Some customers expressed reluctance to make online purchases and expose themselves to identity and credit card theft, but it didn’t really matter. Whether they shopped online or not, their personal information was vulnerable to misuse from myriad sources: mail theft, purse snatching, workplace data leakage — the list was endless.

The problems weren’t exclusive to U.S. police; law enforcement officers in other countries were under similar pressures. The London Metropolitan Police Force (the largest police agency in England), called for a national unit to address the problem, warning that the “U.K.’s local police forces can ‘no longer cope’ with e-crime.”[xxviii]

It wasn’t all gloom and doom; there were some positive developments.

In 1985, The California District Attorney’s Technology Theft Association (DATTA) applied for a grant to “… train San Francisco Bay area investigators

[17] Identity Theft and Assumption Deterrence Act (“Identity Theft Act”), 18 U.S.C. § 1028 (a)(7).

and prosecutors in high-technology theft investigation." One program goal was "To establish an organization base that will provide the nucleus for the development of a regional high-technology theft prevention effort."[xxix] The goal was met in 1986 with the formation of the High-Technology Crime Investigator's Association (HTCIA) with over 30 Southern California law enforcement jurisdictions participating.

One of the first digital evidence analysis courses taught in the United States was Computer Investigative Specialist (CIS) training, hosted at the Federal Law Enforcement Training Center in Brunswick, GA in October 1989. Trainees included criminal investigators from the Internal Revenue Service and the Canadian Tax and Revenue Service. That same month, instructors for the CIS course met and founded the International Association of Computer Investigative Specialists (IACIS).[xxx]

In 1995, the U.S. Secret Service started up a private-public partnership known as the Electronic Crimes Task Force in New York City. It was unique in that it comprised not only local, state and federal law enforcement investigators but also private industry and academia. By 2007, there were "ECTFs" in 25 cities across the U.S.[18] (It was ironic that the Secret Service, established in 1865 under the capable guidance of Allan Pinkerton, should be also the first federal agency — one hundred years later — to gather public and private sector cybercrime fighters together under a single collaborative roof.)

Some local police agencies also sought private sector assistance. In 1998, the State of New York initiated "Operation Sabbatical," an investigation of a group suspected of distributing images of child pornography. Low on resources and skills, the police contacted and vetted a computer user group named "Ethical Hackers" who agreed to provide technical expertise.

> Law enforcement officials obtained 21 search warrants in 14 states and 4 countries, while the members of Ethical Hackers played central roles from their home computers. While warrant-bearing police knocked on doors of suspected members of the ring, the members of Ethical Hackers effectively barred access to a discussion area in cyberspace where child pornographers were known to congregate, flooding it with meaningless data to render it unusable. The idea was that if the members could not communicate, they would not be able to warn one another about the raids.[xxxi]

It was also noted that Internet "netizens" were happy to assist law enforcement with cybercrime investigations, more so than with garden-variety street crime. Perhaps this was so because amateur "cybersleuths" felt more comfortable rendering assistance while safely ensconced in front of computer monitors. (Or perhaps police had so insulated themselves from their

[18] Atlanta, Baltimore, Birmingham, Boston, Buffalo, Charlotte, Chicago, Cleveland, Columbia SC, Dallas, Houston, Las Vegas, Louisville, Los Angeles, Miami, Minneapolis, Newark NJ, New York, Oklahoma City/Tulsa, Orlando, Philadelphia, Pittsburgh, San Francisco, Seattle, and Washington D.C.

constituencies they lost sight of the fact that most citizens were willing to help maintain law and order in their communities — both real and virtual.)

In Florida, the Flagler Beach police department conducted, in partnership with a private sector vigilante group, an Internet sexual predator sting. Twenty-one men, including a police officer, were arrested for attempting to have sex with a minor.[xxxii] Chief Roger Free remarked, “Teaming with private entities is the wave of the future.”[xxxiii]

It was the wave of the future? Clearly, Chief Free hadn’t heard about Allan Pinkerton.

The Wild, Wild West: Part IV

This is the first time in American history that we in the federal government, alone, cannot protect our infrastructure. We can't hire an army or a police force that's large enough to protect all of America's cell phones or pagers or computer networks — not when 95 percent of these infrastructures are owned & operated by the private sector.

Baley, U.S. Secretary of Commerce (2000)

As we enter into the fourth decade of the technology age, law enforcement must prepare to respond to progressively complex cybercrimes, including information warfare.

> Many states are developing highly sophisticated information and cultural warfare capabilities and exploiting the pervasiveness and pliability of digital information to gain commercial or political advantage.[xxxiv]

Cybercriminals, including terrorists, do a much better job of communicating among themselves than do the police. There is a cultural reason for the difference. Police have traditionally kept information closely held. They are unwilling to share information with "outsiders" — including other police jurisdictions. Neither do most police officers spend appreciable amounts of time engaging in online chat, developing an understanding of online users behaviors, or familiarizing themselves with the Internet underground.

Conversely, cybercriminals spend hundreds of hours online, working to perfect their tradecraft. After testing and validating exploits, hacking into telecommunication systems, or selling stolen credit cards, they freely chat with peers about "best practices."

No longer are young hackers boasting about defacing websites. Now they're involved in much more sinister (and profitable) endeavors. As an example, an as yet unidentified group of "hactivists" deployed virtual armies of computers infected with malicious software "bots"[19] to attack Estonia's government, business and banking systems. Alarmed at the damage to national security, ecommerce and consumer confidence, Estonia's President Toomas Hendrik Ilves announced,

> "It is a serious issue if your most important computer systems go down in a country like mine, where 97 percent of bank transactions are done on the Internet," Ilves said. "When you are a highly Interneted [sic] country like we are, then these kinds of attacks can do very serious damage."[xxxv]

These rogue groups are also responsible for using bot-controlled networks to mass-email Internet users with

"Pump and dump" stock offers and other scams

"Phishing" invitations designed to lure consumers to phony websites and

[19] A "bot" is an automated software program that executes certain commands when it receives a specific input (like a ro-"bot"). "Botnets" are compromised networks of computers that criminals control of to distribute spam (to perpetrate more frauds) or malicious computer code to attack other computers.

trick them into entering identification, banking, and other critical information.[20]

Organized crime groups are actively recruiting talented computer programmers to steal millions of dollars and thousands of identities.

> “Web Mobs” have developed into an international clearinghouse of stolen plastic card and identity documents ranging from passports, driver’s licenses to student ID cards. … A very successful international framework has been created for criminals to buy and sell data and share their expertise with each other. Criminals no longer have to be specialists in all areas of fraud. They can simply learn how to steal data and then sell it to someone who manufactures cards and actually commits the fraud, or vice versa.[xxxvi]

At the local level, police have identified a correlation between individual methamphetamine users, identity theft, and organized crime. According to a press release issued in April 2007 by Senator Maria Cantwell, “…the Spokane County [WA] Sheriff found a meth connection in each of the area's identity theft crimes. That same year, Pierce County [WA] officials reported that between 80 to 90 percent of the county's identity theft defendants had either a pending or prior meth charge.”[xxxvii]

Further, identity theft and credit card fraud are funding terrorism.

Significant links between Islamic terrorist groups and cybercrime were discovered after “Irhabi007” (aka Younes Tsouli) and two accomplices were arrested and later convicted of inciting murder using the Internet.

This image was found on ikbis.com, an Arabic website. The caption reads: “Evolution of Thieves.” (Note: Arabic is read from right-to-left. The photo should be viewed right-to-left)

On one computer belonging to the suspect, forensic investigators found 37,000 stolen credit card numbers along with personal information on the identity theft victims (account holder’s address, date of birth, credit balances and limits).

The three terrorists made more than $3.5 million in fraudulent charges using credit cards stolen in phishing scams. In addition, they:

> Compiled shopping lists for items that fellow jihadists might need for their battle against the American and allied forces in Iraq, including global positioning satellite (GPS) devices, night-vision goggles, sleeping bags, telephones, survival knives and tents. Records show the men had purchased other operational resources, including hundreds of prepaid cell phones, and more than

[20] Virtually all spam is now sent from hijacked computers.

> 250 airline tickets using 110 different credit cards at 46 airlines and travel agencies.
>
> Al-Daour also allegedly laundered money through online gambling sites -- using accounts set up with stolen credit card numbers and victims' identities -- running up thousand-dollar tabs at sites like AbsolutePoker.com, BetFair.com, BetonBet.com, Canbet.com, Eurobet.com, NoblePoker.com and ParadisePoker.com, among others. All told, al-Daour and other members of the group conducted 350 transactions at 43 different online wagering sites, using more than 130 compromised credit card accounts. It didn't matter if they lost money on their wagering. Winnings were withdrawn and transferred to online bank accounts the men controlled.[xxxviii]

Investigators in the United States and abroad spent hundreds of hours tracking the trio's financial activities across thousands of merchants in more than a dozen countries.

Police aren’t the only ones who are scrambling to catch up with technology; the judiciary is struggling, too. At the “Irhabi007” trial,

> The magistrate overseeing the trial, Justice Peter Openshaw, interrupted the proceedings with a statement that observers said stunned prosecutors for the Crown. “The trouble is I don't understand the language. I don't really understand what a Web site is.”[xxxix] (Emphasis added.)

One of the case investigators was reported to say, “There is no law enforcement agency in the world that, if this wasn't a terrorism financing case, would follow up on this. They just don't have the resources.”

Another credit card fraud exploiting Voice Over Internet Telephone (VOIP) surfaced in 2006. “Vishing" uses automated dialing and transmission of a recorded message that advises victims their credit card has been used illegally. Users are instructed to call a telephone number to provide account verification by entering a 16-digit credit card number on the keypad.[xl] Other more sophisticated exploits will be developed; VOIP technology is relatively new.

Malware will become more widespread in web pages, videos and on opinion-discussion websites called “blogs.”[xli]

Other wide open markets ripe for targeting with malicious bots and phishing messages are mobile devices and smart phones. These threats may especially impact first responders who use mobile technology.

Radio Frequency Identification (RFID) is emerging technology used to uniquely identify objects, animals and persons. RFID chips are being embedded in US and UK passports, credit cards and identification. There is one reported instance of an RFID security probe that successfully scanned and read data on a passport that was sealed in an envelope.[xlii] Vulnerabilities are still being assessed, but it is certain that there will be future attempts to exploit RFID technology.

In 2000, William C. Boni predicted that "techno-crimes… will continue to increase in intensity and sophistication on a massive global scale… the attacks may become so prevalent and vicious that there will be an outcry for governments to take action to stop outrageous violations of international and national laws. These demands for government action will come primarily from businesses, especially those involved in e-commerce whose businesses will be suffering major losses."[xliii]

The emerging field of digital evidence forensic analysis already threatens to overload police resources, with no sign of easing up. There will be a steady demand for qualified experts who can identify, investigate, collect and analyze digital evidence, both in the public and private sectors. Demand is likely to exceed supply, especially if law enforcement is unwilling to hire non-commissioned personnel.

Pay differential between public and private sectors will negatively impact police recruit applicant pools. Police will struggle to retain experienced investigators and digital evidence examiners because private sector employers will attempt to lure them away with offers of higher wages, better benefits and more attractive workplace environments.

Mass production coupled with dropping prices will enable more consumers to purchase digital devices, increasing the numbers of potential perpetrators and victims.

Devices will continue to shrink in size, but data storage capacities will expand. Easier to conceal, miniaturized devices may not be recognized as evidence repositories or they may be recognized, but overlooked.

Digital evidence acquisition, processing and analysis times will exponentially increase.

Greater amounts of evidentiary data will place demands on police evidence storage facilities. Long-term storage of digital evidence on unreliable or defective storage media may expose agencies to liability if data is lost or corrupted.

Digital forensic training and equipment costs will challenge even the largest law enforcement agencies. Examiners must keep current with forensic software tools and techniques. Further, as new digital devices are marketed and used or abused by criminals, additional new forensic training, hardware, software and human capital will be required to process and analyze the evidence. Procurement cycles must be shortened in order to keep pace with technology.

Because each digital device has its own proprietary operating system, forensic software developers will be unable to stay abreast of production and proliferation of new devices.

As the emerging field of digital evidence forensics matures, there will be mandates necessitating certification and recertification of examiners, adding more costs to be factored into police budgets.

A digital forensic examiner recently commented, "It'll get worse before it gets better. This is the Wild, Wild West version two-point-oh. We're on a runaway train and the outlaws mean to derail us.”

The Wild, Wild West: Part V

Cybercrime, with its global reach, presents daunting challenges to law enforcement, but challenges faced by 19th century law enforcement are essentially no different than challenges confronting 21st century crime-fighters. We can overcome the obstacles and reduce the impact of Internet crime by bearing in mind that there is nothing new under the sun.

By the time I'd finished my research I had only one thought. "We're doomed!"

Fortunately Granddad's adage, that "there's nothing new under the sun," reminded me to look to the past for solutions to future problems.

Twenty-first century investigators can emulate the tactics that Pinkerton and law enforcement investigators successfully used to fight nineteenth century "high tech" crime.

Our agency operates with a less than optimal budget, is under equipped and often understaffed. We may need to look at out-of-the-box solutions to acquire the technology skills, hardware and software we need to stay abreast of cybercrime. Pinkerton's innovative business practices might be worth considering. Some ideas for consideration are:

1. Use innovative hiring practices; screen candidates for performance suitability.

Build a reserve or volunteer cadre of knowledgeable experts from the community who will work under the supervision of experienced investigators to assist in seizure and acquisition of digital evidence. Their strength would be their technical skills; their weakness would be a lack of knowledge of evidence preservation. It may be more cost effective to teach evidence preservation to non-police than to teach digital evidence seizure and analysis to police. Possible sources for technicians are:

- Information and network system administrators
- Computer science teachers or students
- Computer programmers

Qualified candidates could also assist with digital evidence analysis. Some candidates (or their employers) might even pay for their own forensic software training and or certification.

2. Ensure investigators have up-to-date training, equipment and materials.

Procurement Cycles: Meet with civic administrators to discuss ways policies might be revised so that police can keep up with technology.

Needs Statement: Prepare and personalize arguments about how failure to keep up with technology can come back to haunt police and community administrators.[21]

[21] *Sheriff's Office Comments on Kylie Taylor Case* (Clark County Sheriff: Press Release, September 22, 2004) <http://www.clark.wa.gov/news/news-release.asp?pkNewsSeq=420>; (Perverted Justice.com Archives, September 18, 2004) < http://www.perverted-justice.com/?missing=46>; (Corrupted Justice.com) <http://www.corrupted-

Sponsorships: To augment strapped budgets, community or business donations could be solicited. A nonprofit consortium of technology-based businesses could be formed to provide assistance, guidance and support. "Brand marketing" (discrete paid advertising on police equipment, for example) could be a source of funds.

Public Relations: Police can apprise constituents about lack of and need for skills training, hardware and software and request the community's financial support. An open solicitation fund-raising drive may be more successful than traditional tax-based requests. Explain how community will benefit in the long term. Consider using a theme such as "We can't help you if you can't help us fight cybercrime."

3. Make continuous learning a high priority.

Mentoring: Request all personnel to learn about technology trends, new products, threats, and forensic techniques and share knowledge with others.

Newsletter: Create an in-house newsletter that summarizes news articles, surveys, war stories, product reviews, etc. Use email distribution to save printing costs. Judiciary and prosecutors could contribute articles, as well.

Roll Call Training: Technology experts and product representatives could be brought in to give brief talks about their area of expertise (e.g., Internet Service Providers, cell phone company representatives, or bank fraud investigators).

4. Information management should be in a constant state of updating and renewal.

Chiefs Meeting: Discuss regional approach to information sharing. Draw up MOUs once agreements are reached.

Local: Evaluate extent of communication with other jurisdictions. Are we sharing information about possible cross-jurisdiction cases (elderly abuse scams, mail box thefts, etc.)? How can we improve?

Statewide: Are we receiving timely, relevant information from the data fusion center? What needs to be changed to make better use of the data?

Community: What about setting up a text messaging alert system to go out over cellular phones? Amber alerts and BOLOs could be broadcast, with appropriate cautionary warnings. Participants could sign up via the department website.

5. Vision Statement: "We never sleep" (in relentless pursuit of criminals).

justice.com/forums/viewtopic.php?t=1437&postdays=0&postorder=asc&start=45>; (North American Missing Persons Network: Kylie Taylor) <http://www.nampn.org/cases/taylor_kylie.html>; (Genderberg.com) <http://www.genderberg.com/phpNuke/modules.php?name=News&file=article&sid=98> Also see Grigoriadis, Vanessa (2007) *'To Catch a Predator': The New American Witch Hunt for Dangerous Pedophiles* (Rollingstone.com Issue 1032 July 30, 2007) <http://www.rollingstone.com/news/story/15723886/to_catch_a_predator_is_nbcs_primetime_dragnet_the_new_american_witch_hunt> Accessed July 31, 2007

Decide upon a vision statement with respect to cybercrime, and then live the vision department-wide. Encourage businesses and citizens to live the same vision.

6. Relationship building.

Cultivate relationships with technology savvy constituents, both in the community and on the Internet. Investigators should learn to use the same tools that the Internet underground uses.

Use community "eyes and ears" (and keyboards) to stay abreast of threats, techniques and crimes in progress. Mentor "netizen" activist groups.

Give community presentations on computer security, fraud, Internet safety, and best practices. (Use experts if officers do not have the knowledge so that they, too, will learn.)

7. Know thy enemy.

Develop online informants. Learn about technology uses and abuses from the people who use the technology. A good place to start is with students; they're likely to have the latest technology products and to be learning about exploitations and abuses. User groups might be another resource.

8. Prevention.

Police to Business: Can we build a network with businesses via email or Internet web page? This could be an avenue to distribute crime bulletins and "in progress" alerts and request for assistance notifications. Notices about Internet crimes such as phishing, credit card thefts, etc., that impact our community could be broadcast.

Police to Citizens: A similar website could be built to jump off the police-to-business website. Information about Internet scams, and fraud prevention tips as well as neighborhood crime watch notifications could be distributed either via the website or email.

Insist that citizens and students become the first line of defense. Show them how. Lead by example.

9. Public Relations.

Be honest with the community. Share successes, but also failures.

Send a message to the criminals that cybercrime will be treated no differently from street crime and aggressively prosecuted.

.

[i] Keating, Anne B. and Hargitai, Joseph R. *A Guide to Incorporating the World Wide Web in College Instruction.* (New York University Press 1999) p 13

[ii] (n.d.) *Wiring the Continent: The Transcontinental Telegraph Line.* IEEE The Virtual Museum. <http://www.ieee-virtual-museum.org/collection/event.php?id=3456807&lid=1> Accessed May 2, 2007

[iii] Ross, N.E. (1928) *How to Write Telegrams Properly.* <http://www.telegraph-office.com//pages/telegram.html#How%20to%20Save> Accessed May 2, 2007

[iv] Wynn, William R. (n.d.) *The Telegraph Romance and Bushwhacking Mystery* (Unusual Family Stories (of White & Cleburne Co.)) <http://www.rootsweb.com/~arwhite/unusual.html> Accessed March 5, 2007

[v] Clay, Wallace (1969) A. *The Life Of A Telegraph Operator On The "Old C. P." In The Golden Spike Era.* (Oral History 1969). <http://www.nps.gov/archive/gosp/research/pappy_clay10.html> Accessed March 12, 2007

[vi] Norfolk Southern Police Department. *History of Railway Police.* <http://nspolice.com/history2.htm> Accessed March 15, 2007

[vii] Pinkerton, William (1893) *Highwaymen of the Railroad.* The North American Review (November 1893) Legends of America: A Travel Site for the Nostalgic & Historic Minded. <http://www.legendsofamerica.com/WE-RailroadHighwaymen.html> Accessed March 31, 2007

[viii] Pinkerton, William (1893) *Highwaymen of the Railroad.* Ibid.

[ix] Waite, Donald E. (1977) *The Langley Story Illustrated: An Early History of the Municipality of Langley.* (D.W. Friesen & Sons Limited, Altona, Manitoba: November 1977) p 173

[x] Geringer, Joseph (n.d.) *Allan Pinkerton and His Detective Agency: We Never Sleep: The Wild West.* Court TV Crime Library: Criminal Minds and Methods. <http://www.crimelibrary.com/gangsters_outlaws/cops_others/pinkerton/5.html> Accessed April 9, 2007

[xi] Geringer, Joseph (n.d.) *Allan Pinkerton and His Detective Agency: We Never Sleep: The Wild West.* Ibid.

[xii] *The Cuckoo's Egg (book)* (n.d.) Wikipedia, the free encyclopedia <http://en.wikipedia.org/wiki/The_Cuckoo's_Egg_(book)> Accessed July 8, 2007

[xiii] *Commercialization of the Internet* (1994) (Communications of the ACM, Vol 37, No 11, November, 1994) <http://som.csudh.edu/fac/lpress/comm.htm> Accessed July 7, 2007

[xiv] *FNCAC Resolutions* <http://www.nitrd.gov/archive/fnc-material.html> Accessed June 22, 2007

[xv] *Commercialization of the Internet (1994)* Ibid.

[xvi] *The Internet Economy: the World's Next Growth Engine.* (Business Week Online. October 4, 1999) <http://www.businessweek.com/1999/99_40/b3649004.htm. Accessed July 9, 2007

[xvii] *Commercialization of the Internet* (1994) Ibid.

[xviii] *The Growth of Internet Sales, Continued* (n.d.) <http://www.taxpayfedil.org/igrowth.htm. Accessed July 7, 2007

[xix] Gordon, Dr. Gary R. and Curtis, Dr. George E. (2000) *The Growing Global Threat of Economic and Cyber Crime* (National Fraud Center. December 2000) pp 9-10. Available at <http://www.lexisnexis.com/risksolutions/conference/docs/cyber.pdf> Accessed May 3, 2007

[xx] Sarkar, Dibya (2007) *Big Names Team up to Lobby against Cyber Fraud* (MSNBC.com July 26, 2007). <http://www.msnbc.msn.com/id/19980384/> Accessed July 31, 2007

[xxi] (2007) *Cybercrime Goes Back 50 Years, Says BCS Expert.* (Public Technology Net: E-Government and Public Sector IT News) <http://www.publictechnology.net/modules.php?op=modlead&name=News&file=article&sid=7960> Accessed February 28, 2007

[xxii] Hoar, Sean B. (2001) *Identity Theft: The Crime of the New Millennium.* (U.S. Department of Justice: United States Attorneys' USA Bulletin. March 2001 Vol. 49, No. 2) p 3

[xxiii] Levin, Yanir (n.d.) *Analyzer in Israel – Investigator vs. Hacker* (MYPI Services.) <http://www.mypi.co.il/articles/analyzer-in-israel-investigator-vs-hacker/> Accessed July 9, 2007

[xxiv] Stambaugh, H; Beaupre, D, Icove, D., Baker, R Cassaday, Wayne and Williams, W.P. (2000) *State and Local Law Enforcement Needs to Combat Electronic Crime (National Institute of Justice: Research in Brief*. U.S. Department of Justice: Research in Brief, NCJ 183451 August 2000.) p 2

[xxv] Appel, Edward J., Pollitt, Mark W., (2005) *Report on the Digital Evidence Needs Survey Of State, Local and Tribal Law Enforcement* (Joint Counsel on Information Age Crime, Inc. and Northeastern University College of Criminal Justice for National Institute of Justice. March 2005) p 3

[xxvi] (2006) *President's Identity Theft Task Force Interim Recommendations* (September 19, 2006) p 6 Available at <http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf> Accessed May 23, 2007

[xxvii] Pratt, Timothy (2008) *ID theft victims feel burned by state's 'hotline'* (Las Vegas Sun/Sun News, June 28, 2007) <http://www.lasvegassun.com/sunbin/stories/text/2007/jun/28/566622574.html> Accessed June 29, 2007

[xxviii] Espiner, Tom (2007) *U.K. Police: We're Overwhelmed by E-crime."* (CNet News: January 26, 2007) <http://news.com.com/2100-7348_3-6153743.html> Accessed January 26, 2007

[xxix] Smith, John C. (2001) *History of HTCIA.* (History of the High Tech Crime Investigation Association) <http://www.jcsmithinv.com/HTCIAhistory.htm> Accessed July 14, 2007

[xxx] King, Pamela (2007) *History of IACIS*. (IACIS Newsletter, Issue No. 1. 2007) p 2

[xxxi] Richtel, Matt (2000) *In the Pursuit of Cybercriminals, Real Detectives Rely on Amateurs* (New York Times: May 17, 2000) <http://query.nytimes.com/gst/fullpage.html?res=9802E1D81F3BF934A25756C0A9669C8B63> Accessed July 10, 2007

[xxxii] (2006) *21 Arrested in Central Florida Predator Sting* (Local6.com News: December 12, 2006) <http://www.local6.com/news/10519503/detail.html> Accessed July 15, 2007

[xxxiii] Garrett, Ronnie (2007) Internet Watchdogs (Officer.com: Law Enforcement Technology, March 2007) <http://www.officer.com/publication/article.jsp?pubId=1&id=35694> Accessed May 22, 2007

[xxxiv] (2007) *The DCDC Strategic Trends Programme 2007–2036* (UK Ministry of Defence, Development, Concepts and Doctrine Centre (DCDC), January 2007) Available at <http://www.mod.uk/NR/rdonlyres/5CB29DC4-9B4A-4DFD-B363-3282BE255CE7/0/strat_trends_23jan07.pdf> p 61 Accessed April 2, 2007

[xxxv] McKinnon, John D. (2007) *Estonia Presses Bush for Cyber-Attack Research Center* (The Wall Street Journal Online: Washington Wire June 25, 2007) <http://blogs.wsj.com/washwire/2007/06/25/estonia-presses-bush-for-cyber-attack-research-center/> Accessed June 27, 2007

[xxxvi] (2006) *Organized Crime Driving Card Fraud to New Heights of Profitability* (CUNA Mutual Group: Press Release, June 22, 2006) <http://www.cunamutual.com/cmg/newsReleaseDetail/0,1252,15837,00.html> Accessed July 15, 2007. And Leland, John (2006) *Meth Users, Attuned to Detail, Add Another Habit: ID Theft* (New York Times, July 11, 2006) <http://www.nytimes.com/2006/07/11/us/11meth.html?ex=1153540800&en=7b6c7773afa880be&ei=5070>

[xxxvii] (2007) *Committee Clears Cantwell Measure to Investigate Link Between ID Theft and Meth: Cantwell Study Included in Comprehensive Anti-Identity Theft Package* (Press Release of Senator Cantwell, April 26, 2007) <http://cantwell.senate.gov/news/record.cfm?id=273186> Accessed July 15, 2007

[xxxviii] Krebs, Brian (2007) *Terrorism's Hook Into Your Inbox: U.K. Case Shows Link Between Online Fraud and Jihadist Networks* (WashingtonPost.com) <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153_pf.html> Accessed July 5, 2007

[xxxix] Krebs, Brian (2007) *Terrorism's Hook Into Your Inbox: U.K. Case Shows Link Between Online Fraud and Jihadist Network* Ibid.

[xl] Jaques, Robert (2007) *Cyber-criminals switch to VoIP 'vishing'* (Vunet.com, July 10, 2006)

[xli] Thomas, Vinoo (2006) *Hackers Use Wikipedia as Bait* (McAffe Avert Labs Blog November 7, 2006)<http://www.avertlabs.com/research/blog?p=128> Accessed Mar 22, 2007

[xlii] Kirk, Jeremy (2007) Crack! Security expert hacks RFID in UK passport (Computer World: Security March 6, 2007) <http://www.computerworld.com/action/articl

e.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&articleId=9012406&taxonomyId=82&intsrc=kc_top> Accessed March 8, 2007

[xliii] William C. Boni and Kovacich, Gerald L. (2000) *Netspionage: The Global Threat to Information* (Butterworth-Heinemann: Massachusetts) p 238

In the lawless "Old West," outlaws robbed banks & held up trains:

Toby M. Finnie & Earl Moulton

1800s	TRANSPOR-TATION	ORGANIZATION	TECHNOLOGY	COMMUNICA-TION	COMMUNITY	INVESTIGATION	FORENSICS	LAW	PREVENTION
U.S. Law Enforcement	• Rode horses & used horse-drawn conveyances	• US Army had jurisdiction over territories • US Marshals were few & far between • Formed specialized groups such as railroad police • Deputized private investigators • Deputized citizen posses	• Had limited access to new technology • Printed & distributed illustrated wanted posters	• Shared information via telegraph (1851) & telephone (1877)	• Were sole enforcers, sometimes with little, inconsistent, or no community support • Citizens formed vigilance groups (some turned vigilante, meting out frontier justice)	• Collected evidence, interviewed witnesses & victims • Analyzed telegram headers for leads	• Fingerprint identification	• Pacific Railway Act • Used extradition processes to bring outlaws to justice • Enacted state & federal legislation	• Incarceration • Public hangings
Canadian Law Enforcement (RCMP)	• Rode horses and used early US railways	• Established in 1873 as formal policing agency modeled on Royal Ulster Constabulary acting as sole LEA in advance of settlement	• Complete lack of technology, reliance on US telegraph services – reliance on Metis and Indian translators	• Reliance on US facilities until 1885 then reliance on public telegraph • Used by Gov't to scout telegraph routes	• Formal authority preceded settlement and had full community and First Nations support	• Acted as investigative, judicial and custodial authority	• Reliance on eyewitness *viva voce* evidence	• Imported British law and authority	• Used existing Metis and First Nations leaders and lots of discretion to introduce new legal system
U.S. Private Sector	• Transported large sums of money & commodities via railroad, overland & coaches & express wagons	• Employed armed guards as agents & express men • Hired private sector investigators who were not constrained by jurisdiction	• Used telegraph & railroads to increase business revenue • Purchased & supplied high powered hand guns & rifles to enforcement & security personnel	• Used telegraph to coordinate arrival & departure of trains & shipments • Used "wireless" telegraph overseas • Advertised & marketed via telegraph	• Investigators gathered & analyzed information about outlaws from community	• More manpower, flexibility to act quickly • Used women as investigators • Investigators used crime analysis, geo-mapping, & criminal profiling • Used undercover operatives; covert operations	• Fingerprint identification	• Lobbied for federal jurisdiction over train robberies • Pursued outlaws across borders & into foreign countries • Extradition laws revised	• Designed stronger safes • Used physical access controls to protect shipments • Investigators educated business owners; provided mug shots & criminal profiles • Warned of certain capture & prosecution of suspects
Canadian Private Sector	• Banking system moved west with after legal authorities well established	• Jurisdiction extended over 1/3 of continent only constrained by US border	• Made do without	• Utilized only in rarest of circumstances	• Officials only engaged in investigations	• Not Used	• Not used	• RR PD est. 1885 – confined to RR property only	• Not used
U.S. Outlaws	• Rode horses & used horse-drawn conveyances	• Formed outlaw gangs such as the James Brothers, Dalton Brothers, & the "Wild Bunch" • Recruited family & friends. • Used aliases & disguises	• Hired expert safe crackers • Used explosives & smokeless powder	• Cut telegraph wires • Conspired via telegraph • Carefully planned robberies	• Often received encouragement , support & shelter from community • Recruited & mentored young men • Threatened witnesses • Wounded or killed innocents	• Gangs split up to elude investigators • Hid out in remote areas	• Wore gloves & masks to evade detection	• Escaped across state lines or borders to evade capture • Bargained release by promises to "go straight"	Fear of loss of freedom or life
Canadian Outlaws	• Used expanding US rail network to access goods and alcohol for trade into Canada	• Outlaws occasionally rode into Canada but returned on encountering formal authority and lack of community support	• Limited or no use	• No organized groups requiring communication	• No community support as coummunity was comprised of settlers & ranchers	• Not an issue	• Very little face to face crime requiring disguise	• Had certainty of outcome with formal system	• Certainty of process and outcome

In the Lawless “Old West” of the Internet, online outlaws rob banks and customers:

1900s	TRANSPOR-TATION	ORGANIZATION	TECHNOLOGY	COMMUNICA-TION	COMMUNITY	INVESTIGATION	FORENSICS	LAW	PREVENTION
U.S. Law Enforcement	• Few agencies proactively patrol the “Information Highway	• Form special investigative groups such as USSS Electronic Crimes Task Forces (US) & Serious Fraud Office (UK)	• Some agencies use Internet as investigative tool • Some agencies cite equipment, personnel training costs as insurmountable barrier • Make no attempt to be proactive	• Most communicate via telephone, email & cellular phones • Some use PDAs, text messaging • A few use encrypted email, & secure web portals or VPNs	• Too few officers spread too thinly to adequately patrol the Information Highway • Citizens begin to form vigilance & vigilante groups	• Investigators overwhelmed by sheer numbers of fraud cases • Take complaints, rarely follow up with investigation • May suggest victims contact federal LE • Federal LE take complaints but rarely follow up • Huge demands on LE resources • Offender data not collected	• Computer & network forensics exams conducted by a few agencies • A few forensic software applications are in use • Digital video forensics is introduced	• DAs refuse to bring action due to jurisdictional issues • Multiple small-dollar loss victims reside in multiple jurisdictions • MLATS process too slow • National ID Theft Task Force established	• Ad hoc development of programs by interested officers
Canadian Law Enforcement (RCMP)	• Lack of resources , knowledge, skills and priorization of persons crime reduces focus on Cybercrime	• Specialized units slowly developed	• Skills, abilities developed to be successful but with little capacity to handle volume • Proactive overwhelmed by reactive needs	• Communica-tion and information access controlled by IT personnel without full regard to operational needs	• Community lack of knowledge keeps demands for service relatively low	• Only very limited capacity to pursue cases • Evidence gathering impeded by existing evidence and jurisdictional law	• Forensics capabilities lag behind the need •Lag time is increasing	• Limited availability of knowledgeable prosecutors and judges • Legislative process unable to keep pace with technology	• Ad hoc development of programs by interested officers
Private Sector	• Transport large sums of money via computer networks & the Internet •Financial institutions close accounts that are breached by fraud • Institute broad strategies for handling data leakage	• Hire in-house investigators (often former LE) • Employ IT security professionals & consultants	• Lax operational security practices with respect to online banking operations	• Telephone & cellular phones, plain text &/or encrypted email, PDAs, text messaging, web boards, VPNs, portals • Some use VOIP	• Costs of fraud passed onto merchants • Consumers charged higher interest rates • Targets of burglary are wallets & credit cards; not electronic goods	• Intrusion cases investigated • Fraud loss is cost of doing business • Traditionally thought to be uncooperative with police	• Employ investigators with CFE training • Rely on network administrators to conduct investigation	• Lobby against tougher regulatory statutes • Privacy rights advocates protest data analysis & monitoring	• Some attempt to educate consumers about best practices
U.S. Cybercrime Outlaws	• Use the Internet Highway as a road to riches • Continue to “follow the money” (via new tech such as smart phones, Voice over Internet Protocol, GPS) • Bot-infected computers controlled by “bot herders” act on behest of organized criminals to attack on broad scale	• Organized crime, terrorists involved • Form distributed networking groups to share exploits, exchange credit card & ID theft information • Pay for development of spyware & keyloggers • Opportunistic use of social networking sites such as MySpace.com	• Exploit emerging technology to assist in criminal activities • Devote hundreds of hours to perfect skills; take advantage of mentors	• Telephone & cellular phones, VOIP with encryption, email (with encryption), steganography, PDAs, text messaging, web boards, blogs, IRC • Use technology to contact & coordinate group activities	• Receive encouragement , support & validation from online peers • Recruit & mentor others to participate • Share best practices information, data, exploits • Develop new tools to perpetrate crimes • Develop new ploys to defraud consumers	• Act with impunity • Use encryption, steganography, proxy servers, obfuscated email addresses & operate from safe haven countries to elude detection & arrest	• Use anti-forensics (encryption, data shredders & obfuscators) • Hide information via steganography	• Aware that jurisdictional problems work in their favor • Fear of prosecution not a deterrence • Privacy protection laws favor criminal • Light sentencing not a deterrent	
Canadian Cybercrime Outlaws	• “MafiaBoy” a “script kiddie” hacker, has far-reaching impact	• Process and procurement capabilities far outstrip those of LEA	• Criminals are the epitome of early adopters	• Quick identification of emerging communication technologies	• Creating own communities of interest • Limited external impact means further extremist positions	• Exploit jurisdictional and time constrants	• Use IT to distribute both knowledge and tools to thwart LEA	• Exploitation of existing laws	

In 2000, things began to change…

2000s	TRANSPORTATION	ORGANIZATION	TECHNOLOGY	COMMUNICATION	COMMUNITY	INVESTIGATION	FORENSICS	LAW	PREVENTION
Law Enforcement	• "On scene" investigations often consist of remote acquisition of evidence • Digitally "patrols" the Information highway via spiders & bots, noting deviancies & abuse patterns in communication traffic • Becomes proactive as well as reactive; concentrating on prevention rather than just prosecution	• All LE officer-recruits are trained to recognize digital evidence devices; applicable criminal statutes; & can protect digital crime scenes • Organize citizen Internet Patrols "CIPs" to act as eyes & ears, reporting suspicious activity to Data Fusion Centers (DFCs) • Police proactively use social media and the eyes & ears of consumers to "patrol" the Internet & identify antisocial behaviors, fraud trends, perpetrators & victims	• Data Fusion Centers (DFCs) promote real time decision making by multiple jurisdictions • Procurement processes changed • Increased demand for reliable data retention & storage capabilities • Powerful catalogue, index, search & retrieval software developed • Digital fingerprints are required authentication	• Victim's complaints are self-reported onto a Universal Police Report that is verified by any PD prior to submitting it into it's system • Decentralization: Cases are assigned to investigator(s) according to codified indicators, which may involve multiple investigators working in different geographic areas • Information shared via secure wireless telecommunication systems	• Citizen vigilante groups are organized, & trained to work directly with law enforcement • Law enforcement relies on citizen groups & business owners to identify trends, target perpetrators & prevent escalation of fraudulent activities. • Voluntarism accepted in the analog world will become acceptable in the digital world	• Computer forensics now includes remote acquisition & analysis of data • With court authorization, critical cases are forensically analyzed in real time • Solid state devices enable terabytes of data to be stored as evidence • Statutory changes address both volume and timely nature of digit evidence	• Through data fusion centers, forensics capabilities & assistance flow down to even the smallest police agency • Digital evidence retention & reliable storage capacities & lengthening times for forensic analyses present unique challenges • Standards for both tools and practitioners will emerge	• Council of Europe's Convention on Cybercrime Protocols ratified by 100 nations • Countries agree to enable swifter collection of digital evidence, render mutual assistance, & share information • Best form of "law" will set out the basis for continual change of the law	• Citizens receive government sponsored best practices training upon purchase of digital devices • State/Federal governments enact "shall issue" user licenses that put onus for safe operation & use of digital devices upon citizen-users; compel manufacturers & software developers to make low cost training programs available to purchasers • Call-home mechanisms enable LE to track & recover stolen digital devices. • Changes made to the underlying protocols – SMTP etc. – to better enable processes of authentication, non-repudiation and data integrity
Private Sector	• Routinely store & transport financial & other sensitive data on networked computers • Businesses must certify that employees use best security practices through training & testing	• Citizens participate in CIPs & report suspicious activities • Financial Institutions work directly with LE	• Newly developed AI-driven technologies track usage patterns & deviancies • Mechanisms embedded into systems & software enable tracking • Will continue to drive the development and rollout and applications of new technology	• Businesses may routinely track & anonymously report abuse patterns, virus attacks, etc to DFCs	• Citizens attend digital device workshops, earn certifications in security • Schools compel students to use best practices to secure user license	• Businesses regularly work with LE to prevent & prosecute digital criminals • Prevention is prioritized over prosecution	• Enables product encoding & RFID tracking to prevent piracy & copyright violation • Retains data files, images & surveillance videos		• Threat of banishment from digital devices becomes effective deterrent • Development of new detection & analysis technologies
Cybercrime Outlaws	• Rely less on Internet & more on mobile technology such as smart phones, PDAs • Commission of offences for the purposes of technology , e.g."happy slapping," etc)	• Use Internet to share information, communicate & plan • Exploit vulnerabilities	• Continue to stay a few paces ahead of LE • Increased social stigma against cybercriminals	• Facilitate mass mobilization ("flashmobs") via real-time sharing of information	• Form temporary alliances • Contract-hire rogue programmers • Use encrypted devices	• Adopt more sophisticated encryption & activity-cloaking techniques to counteract detection	•Employ anti-forensics • Use full disk encryption to impede forensic examination	• Surveillance of society challenges privacy, civil liberties	• Threat of loss of access to digital devices deters criminal activity

Cybercrime in the Year 2025

Gene Stephens

In 1981, this author wrote: “Data from all areas of the [criminal justice] system will be computerized and cross-referenced. Computers will store the *modus operandi* of convicted felons, and when a crime occurs, police may call on the computer to name the most likely suspects, or, in some cases, the exact offender” (Crime in the Year 2000, *The Futurist*, April 1981, p.52). It seemed quite logical at the time, but turned out to be overly optimistic, underestimating the antipathy to change and the turf protection within the system.

The first paragraph of a subsequent article was more on target: “Billions of dollars in losses have already been discovered. Billions more have gone undetected. Trillions will be stolen, most without detection, by the emerging master criminal of the twenty-first century—the cyberspace offender” (Crime in Cyberspace, *The Futurist*, Sept-Oct 1995, p. 24). Admittedly vague, it still seems to be a fairly accurate evaluation of the evolution of cybercrime.

In the same article, this author went on to correctly predict an explosion of cellular time theft and phone fraud; increased cyber attacks and fraud against the government and business; massive credit card theft and fraud; internal theft of identification of clients by financially-struggling and/or greedy employees of credit bureaus, banks, etc.; more cyber stalking and cyber porn, as well as cyber harassment and cyber vengeance; and use of biometrics and encryption as methods of protecting data in cyberspace.

In some other areas, forecasts weren’t as accurate. A fascination with the embryonic field of nanotechnology lead to a prediction of organic nanocomputers implanted in citizens’ brains by the early 21st century and thus forecasts of terrorists sending subliminal messages directly to the brain implants of potential recruits, cyber extortion by hacking into brain implants and scrambling or threatening to scramble information in it, and the problem of persons with brain implants being unable to separate virtual reality—perpetrated by cyber offenders—from flesh-and-blood reality. In defense, it’s still early 21st century—plenty of time for this technology and these disturbing crimes to begin to appear.

In the 1995 article, this author was rather pessimistic about the short-term capacity of police to cope with emerging cybercrime:

> The outlook for curtailing cyberspace crime by technology
> or conventional law-enforcement methods is bleak. Most
> agencies do not have the personnel or the skills to cope with
> such offenses…. Cybercrime cannot be controlled by conventional methods. Technology is on the side of the
> cyberspace offender and motivation is high—it’s fun, exciting, and profitable (p. 28).

As far as a suggested solution:

> The only real help is one that has not proven very successful in recent decades: conscience and personal values, the belief that theft, deception, and invasion of privacy are simply unacceptable (p. 28).

This approach could work, but unfortunately seems even more "pollyanna" today. So what can we expect in the next few years?

Technology Explosion

According to Ray Kurzweil's "Law of Accelerating Returns," technological change is exponential rather than linear; thus, "we won't experience 100 years of progress in the 21st century—it will be more like 20,000 years of progress (at today's rate)" (www.kurzewilai.net, published March 7, 2001). Predicting the advances and their impact on crime and crimefighting by 2025 then is analgous to reviewing the next 5,000 years of technological progress in society.

Kurzweil himself made several predictions that could have major impact in the field of cybercrime, such as that by 2010 PCs will be capable of answering questions by accessing information wirelessly via the Internet (one prediction that arrived a little early). By 2019, he held a $1,000 personal computer will have as much raw power as the human brain but possibly more important, computer chips will be everywhere, embedded in furniture, jewelry, walls, clothing, etc. Also by 2019, he predicted computers and humans would communicate via two-way speech and gestures rather than keyboards. Virtual sex, via computer, will become a reality, as education, business, and entertainment also will be increasingly computer based. Roadways, Kurzweil forecasts, will be automated and computer controlled, while human-robot relationships will be commonplace.[1]

Possibly the most renowned of Kurzweil's predictions is the coming of "the singularity"—the melding of humans and machines. Kurzweil sees this process well underway by 2025, as nanobots begin to surf the human bloodstream on search and destroy missions to combat pathogens, and data nanobots augment human intelligence and access to information. Transhumans will be on their way to having within their bodies the capacity to communicate and interact with others—humans, machines, and transhumans.

As for this author's forecasts, here goes: Computer/internet use will become increasingly seamless, as hands-free, voice-activated communications and data entry and retrieval will be commonplace by the early teen years of this new millennium. That will mean the world community has moved a long way in a few short years, as even in late 2007, when it was reported 1.25 billion people had access to the internet, only about 2% of the world population regularly accessed it (www.internetworldstats.com). Science fiction writer William Gibson, who coined the term "cyberspace" in his 1982 short story, "Burning Chrome," forecasts a ubiquitous fully-wired world—a single unbroken interface without need for computers—will complete the evolution to full access of all citizens of earth. (www.williamgibsonbooks.com). [2]

Whereas the Defense Advanced Research Projects Agency (DARPA) set up the internet and set it in motion (www.arpa.mil), DARPA will likely overhaul its invention in the teen years, and not only will the outcome be faster and larger capacity usage, but by virtually "starting over" with the security aspects, the new internet will be safer and more difficult to attack and disable. [3]

Nanotechnology will increasingly impact cyberspace by the late teen years, and in trying to gain the most advantage possible from its use, new security gaps (which could turn into nightmares if not handled carefully) will emerge. For example, as data nanobots are implanted in the brain of users (later organic bots will become an integral part of the individual), special attention will have to be paid to providing advanced firewalls to keep intruders from cracking into the bots and terrorizing the recipient. Could there be a more frightening crime than having your brain-stored knowledge erased or scrambled, or hearing voices threatening to destroy your memory unless you pay extravagant blackmail—mindstalking? [4]

Designer nanobots may also be released on the worldwide web to engender types of mischief and destruction not yet contemplated. All advanced technology has the capacity to be used for good or evil, dependent on the developer/user, and nanotech would appear to be the ultimate example, as it literally can be used to develop nanosize weapons that could destroy the world while providing nanosize defense systems that could protect the planet.

The geometrically-enhanced capabilities of the emerging web technology spotlights the long-ignored issues of ***who owns the worldwide web*****,** ***who manages the worldwide*** **web**, and ***who has jurisdiction over the worldwide web***? The answer now is: nobody! Can the world's most powerful socio-politico-economic network continue to operate almost at random, open to all, and thus excessively vulnerable to cyber criminals and terrorists alike? Yet any attempt to restrict or police the web can be expected to be met by extreme resistance from a plethora of users for a variety of reasons, many contradictory.

Another sound prediction would be that the internet will become not only the number one means of communicating, conducting business, socializing, entertaining, and just "living," in the future but indeed will handle a huge majority of such interactions; thus failure to establish and enforce some basic ground rules will lead to socioeconomic disaster, at the very least.

If exchange of resources is to be accomplished almost exclusively over the internet, anonymous surfing will be a potential threat and moving funds without identification could perpetrate not only individual fraud but could bankrupt the system itself. Biometrics and more advanced systems of ID will need to be perfected to protect users and the network. In addition, multinational cybercrime units will be required to catch those preying on users worldwide, as web surfers in Arlington,Virginia, USA, and Victoria, British Columbia, Canada, may be victims of cyber scams perpetrated in

Cairo, Egypt, or Budapest, Hungary. Coordination and cooperation will be keys to making the internet a safer place to travel and conduct business.

As we near the year 2020—with its accumulation of 4,000 years equivalence of tech advancement from the beginning of the 21st century—it becomes more difficult to forecast, as even the concepts, theories, and formulae for the changes have not yet emerged from the plethora of ongoing research and development.

But again, here goes: Every square meter of atmosphere hugging the earth will be filled with unseen nano devices designed to provide seamless communication and surveillance among all persons in all places. Humans will already have nanoimplants to accommodate both the instant communications and identification capacity of the omnipresent network, with everyone on earth having a unique Internet Protocol (IP) address. Nano storage capacity being almost limitless, all activity and utterances will be recorded and recoverable. Transparency will become increasingly ubiquitous as word and deed—whether spoken or acted out in anger, frustration, or as a joke—can be almost instantly compared to "the record." Can human or even transhuman behavior evolve rapidly enough to withstand such scrutiny? If current laws were enforced with this level of supporting evidence, who could pay for the prison space required to carry out the mandated punishment?

Another possibility would be the perfection of The Matrix—envisioned by Gibson and subject of a series of popular books and movies—where a powerful central force controls all activity in a seemingly free society. The reaction in individualistic societies, such as the U.S., would likely be similar to that in these fictional portrayals—rebellion with a goal of destruction of the web of control. A counter force that could create a different type of harm for the individual would be continuance of the policy of no control of the internet, allowing often destructive activity—e.g., harassment, terrorism and fraud—without jurisdiction and authority to curtail it. Which would be worse would depend on which value dominates—security (i.e., safety and order) or civil liberties (freedom and chaos). As always, the role of public safety in all this is finding the balancing point, where the degree of safety is enough to allow the pursuit of individual happiness.

Cybercrime Progression

As technology advances at a dizzying pace, so will the ways and means of those wishing to use the rapidly changing cyberspace as a tool/milieu for fun and profit or worse. In the immediate future, the increasingly creative scams to bilk internet users of their resources will continue, with literally scores of new schemes appearing daily on the worldwide web. Sheiks, abandoned Russian women, and unclaimed lottery winnings will be joined by relatives seeking heirs and other electronic "pigeon drops" yet unimagined.

For those who burn with faith or passion for a cause, the internet will continue to provide a means both to fleece infidels for funds to pursue their goals, while at the same time providing an avenue for recruiting others to their flock, as well as presenting opportunities to target their enemies for economic and even physical destruction via cyber terrorism.

Already the number one crime in the U.S. and rapidly expanding throughout the internet world, identity theft can be expected to increase at a faster pace and wreak havoc on the financial and social worlds of millions around the globe. It well may be that the only way to gain control over this profitable criminal enterprise will be the suggested DARPA reconfiguration of the web and its security apparatus.

These, however, are short-term crises, which thanks to the rapid pace of change will be outmoded by the ubiquitous wireless communications network that should be fully evolved by the middle to late years of the second decade of this new millennium.
What type of cybercrime will come with the absence of computers and only signals in the air to handle all social and economic activity is yet to be invented. Yet, unless a values revolution (whether spiritual, religious, or humanistic in origin) occurs and humans/transhumans choose to refrain from stealing, killing, and defiling one another, you can bet creative malcontents will develop new methods to manipulate the system for their own ends.

In its quest for speed and efficiency on the web, networks will grow in size and scope. For example, a network including all branches of a large bank becomes a larger net when several banks merge and larger still when all banks in a region join to reduce costs and speed service delivery. Then a national banking net emerges and is soon replaced by a multinational and finally a worldwide net. While the net becomes more powerful as it grows, it also becomes more vulnerable to attack. A shutdown of a regional net would create havoc, but the slack could be picked up by other nets. However, if the worldwide net is closed, true chaos ensues, leaving banks/customers at the mercy of blackmailers/extortionists/terrorists. Thus, the larger the networks (e.g., energy, medical, education; regional, international, worldwide), the more critical security becomes.

On the other hand, many may see a greater threat evolving from the powerful technology available to thwart cybercrime and, indeed, all criminal activity. Authorities have long said, “If you have nothing to hide, you have nothing to fear” when talking about police state surveillance capabilities. It would appear that theory will be well tested by the evolving technology of the next few years, as all activity will be seen and recorded and ready for retrieval and prosecution and then development of preventive strategies. Do we really want to live in a society where law is supreme, without recourse, and mistakes are not allowed, where “the record” is proof positive and there is no place for plea bargaining or mediation/arbitration. Have we evolved to this level of “perfection?”

Conclusion

The future path through cyberspace is filled with threats and opportunities, most of which cannot even be imagined at this time. With 5,000 years of technological progress expected between 2100 and 2125, it's difficult to forecast the dilemmas that lie ahead, but thanks to the creativity and genius of William Gibson, Ray Kurzweil, and others like them, some predictions have been made and can be used as a base for an examination of future cybercrime and crimefighting.

The internet as we know it—computers, websites, email, blogs, commerce, etc.—may be outdated as soon as the early years of the next decade when a seamless, wireless network of airborne signals received directly by transmitters in the possession of individuals and nanobots implanted in the bodies of individuals handle all communication. At this point, cyber offenses will become very personal, as an attack on the web is a direct attack on the user—possibly even invading his brain and memory stored in neural networks.

As nanoscience advances to the point that bots in the atmosphere capture and record all spoken and physical activity, the choice will evolve: tightly control all human interaction by holding individuals responsible for every deed and action (each of which is supported by permanently stored evidence) in a efficiently networked worldwide web or allow creativity and individualism to emerge by refusing to set boundaries and jurisdictions on the internet, leaving it much as it is today—without management or enforcement. The former would curtail cybercrime and make the web a safe vehicle for communication, socializing, commerce, etc., but at a substantial cost to privacy, freedom of speech, and other civil liberties. The latter would allow a free flow of information and exchange of goods and services without government interference, but with a substantial threat to the economic and social lives of individuals and society itself posed by cyber offenders.

By 2025, it is likely the whole concept of the internet and cybercrime may be passé—part of the dustbin of history. The greatest threat then might be the extreme difficulty of separating virtual (cyber) reality from physical reality. Already psychologists warn that perception is more important than truth; thus, if cyber reality is more convincing than physical reality, does the virtual world become the "real" world? Welcome to The Matrix.

Notes

[1] Much more about Kurzweil and his work can be found at: www.kurzweilai.net and www.kurzweiltech.com.

[2] In addition to a brief review of his life and works, partially in his own words, at Gibson's "official website," www.williamgibsonbooks.com, a more complete listing of his full body of work can be found at www.skierpage.com/gibson/biblio.htm.

[3] For details on DARPA's role in developing the internet, go to the Internet Society website at www.isoc.org/internet/history/brief.shtml.

[4] For details on nanotechnology go to:
www.crnano.org/whatis.htm and
www.nanotech-now.com.

Street Crime in a Cashless Economy

Michael Buerger

At some point, in the not-too-distant future, we will stop using money. Indeed, the old “Life Takes Visa” TV commercials, in which the easy flow of commerce in various settings comes to a grinding halt when a patron tries to pay with cash or check rather than swipe a card, is a harbinger of such a transformation. Criminal enterprises depend upon the relative anonymity of cash because it severs the link between the crime and its profits, and the disappearance of a cash economy will have implications for crime.

The nature of economic transactions has changed through the years. The “hard currency” of coins and bars became abstracted into paper representations: dollar bills, bearer bonds, and personal checks. Further abstraction into credit and debit cards has permitted the wedding of commerce with electronic communications: a series of numbers (whether on checks or on plastic cards) represents actual wealth held elsewhere, or potential wealth.

Money transformed into numbers conveyed across the electronic network changes the nature of security as well. At the present time, two models of security exist—a third is emerging. The dominant security models are token-based (“what you have”) and knowledge-based (“what you know”) (Woodward, Orlans, and Higgins, 2003). Tokens include the form of identification requested for paying by check (and in some cases by credit card), electronic passkeys, and the like. Personal Identification Numbers (PINs) and passwords comprise knowledge-based security.

When the abstract money of a debit or credit card is presented as payment, an additional abstraction (a PIN and/or a code printed on the reverse side of the embossed card) is required to validate the numbers visible on the card. A thief who obtains the primary numbers needs a second set of numbers or letters (presumably known only to the rightful owner) to use the primary string. When doubt arises, numbers integral to complementary systems – the last four digits of a Social Security Number (SSN), for instance – serve to backstop the system-created safeguards (see note 1)

The rise of identity theft necessitates a foolproof way to verify that the often-unseen individual presenting a number as payment is the rightful owner of that number. That search has taken a quantum leap from the four-digit PIN and the three-digit, printed security number on the back of credit cards. The newest form of identity verification is one thought to be almost invulnerable to the vagaries of human memory and considerably more resistant to most ordinary forms of theft. It replaces “what you have” and “what you know” systems with “who you are”: biometrics.

Biometrics

Biometrics is not yet a mature technology, but it is rapidly developing, expanding with the proliferation of digital media. Some banks already offer thumbprint verification for check-cashing, and biometric identification is being encoded into U.S. passports.

Facial recognition software remains a goal of security system developers, despite its early failures.

In controlled spaces, biometrics already serve to verify the identity of persons seeking entrance into secured and restricted areas. Joined to a network of closed-circuit televisions (CCTV) in both public and private spaces, biometrics represent a capacity for locating wanted persons, even within the seeming anonymity of a crowd.

In biometric security, a short string of numbers (the check number or 16-digit credit card number) is replaced by a long string of ones and zeroes that represent visual patterns of a fingerprint or iris pattern. The technology underlies the Automatic Fingerprint Identification System (AFIS) now in use throughout the United States. Its adaptation to larger use is simply a matter of scale and of social engineering.

Digital representation of a fingerprint or iris pattern is unique to the individual, independent of the possessor's ability to remember, and so lengthy when transformed into computer code that discovery by accident is all but impossible. It has the additional advantage of being less intrusively applied than DNA.

With a sufficiently developed electronic background, a person can change their biometric code much as they would change a computer password. Ten fingerprints and two eyes to choose from (for most people) allow mutiple iris-fingerprint, fingerprint-fingerprint, and iris-iris combinations. Changing from right thumb to left ring-finger, or any other combination, can be done at will, at any participating institution, or according to a predetermined code by the person. There are additional issues related to this, of course, but they are explored in another elsewhere (see Buerger, 200x).

Taking the concept one step further, a biometric security code is simply a concrete string of numbers verifying an abstract and randomly-assigned string. The security code can easily substitute for the intermediate, institutionally assigned numbers.

The lack of accurate, inexpensive, hygenic, and affordable reader devices currently limits the use of the technology. However, once an easily useable biometric verification system is in place, or at a "tipping point" level of use throughout the country, purchases and payments can be made completely electronically, authenticated by biometrics without any intermediate representation of cash or credit.

Each point-of-sale station will be part of a web of direct communication between the point of contact, a network of databases storing previously-encoded biometric "identities," and the repository of each individual's accumulated or potential wealth. Once a fully developed system of electronic transactions is in place, it will be possible to do away with cash.

The changeover will not be immediate, nor all-encompassing. It will be a convenience at first, accommodating the realities of an incompletely-distributed system. Once over the tipping-point, however, the economics of the system will take over; the initially voluntary alternative system will eventually become the only system available.

A parallel "corporometric system" must be developed to enable corporate entities to participate in electronic commerce. It is no more difficult to implement than electronic signatures, or a highly complex UPC code, available to authorized corporate users, though.

Token economies based on cash transactions will survive for a while. During this time, such systems will parallel the biometric system, as long as it is possible to convert physical cash into its electronic equivalent at some point or another (overseas economies are the most likely "other point"). Once the government no longer assures the value of the coin or bill, however, its worth in even local commerce is nil. Forced conversion of even the most hardened resisters will be a matter of simple necessity.

Crime in a Cashless Society

At first blush, the creation of a biometrics-based system would seem to be a boon for the criminal justice system. While it might not curtail all forms of fraud, it holds the promise of drastic reductions in certain types of crime. Street robberies, street-level drug trades, bootlegging of stolen and pirated goods, certain firearms markets, and some forms of welfare fraud all depend to some degree upon the anonymity of the cash economy.

Cash is stolen to buy drugs, or for other personal use. Goods are stolen to be fenced, traded in for a fraction of their value in cash. When cash disappears, such economically-motivated crime will either will disappear – which is highly unlikely -- or be forced into forms of adaptation that should diminish the illicit markets.

Public mayhem of other sorts will still be prevalent, of course. Even a foolproof electronic economy will not quell turf wars among gangs of disenfranchised youth, drive-by revenge shootings, and the like. Domestic assaults, fights created by alcohol and stupidity, hate crimes, and a host of other forms of violence occur independently of financial motives. Nevertheless, we must anticipate both a reduction of crime in some areas, permutations in others, and a shift in criminal enterprise to computer-based theft.

Pawnshops

Pawnshops and second-hand goods dealers have long represented the nexus between street crimes and money. The majority of shops and transactions are legitimate, but overt or tacit fencing operations are the necessary link between criminal activity and the general economy (see, e.g., Klockars, 1983; Steffensmeier, 1986). Most cities have ordinances requiring panwshops to keep records and make them available for regular inspection by the police, in order to identify and recover stolen goods.

Biometric codes would immediately identify anyone attempting to pawn stolen property, linking the transaction to a specific individual, and potentially to a specific crime. The use of confederates is possible, but confederates are unlikely to place themselves at risk once the efficacy of biometric tracking becomes known.

The entire premise of pawning goods -- stolen or otherwise -- currently revolves around the cash economy, and the disappearance of cash may render the pawnshop industry obsolete. Pawning is possible, though, with electronic funds linked to banking accounts. It requires that the owner of the property have such an account, however.

The present parallel economy of "fringe banking" services those who cannot or do not participate in the mainstream economy (see Canskey, 1994). Fringe banking may disappear if cash ceases to be a medium of commercial exchange, but to compensate, a larger "electronic umbrella" will be necessary. All citizens will have to hold accounts in mainstream institutions. Presumably, all mainstream institutions will be required to service all citizens fairly, including those on the economic fringe. Each of these steps represents a fairly major transformation for the respective community.

At the higher end of finance, sham sales, or fees for "consultant services," can easily mask the transfer of large funds from one account to another. Because those events are relatively rare, they are likely to escape the automated pattern analysis that would identify sham transactions at much lower levels. A different level of law enforcement and regulatory diligence will be necessary to cope with such transactions.

Drug Markets

Anonymous, untraceable cash is the life-blood of many criminal enterprises but none more than the illicit drug trade. While sex and other commodities may serve instead of cash at the low end (drugs themselves may serve as an economy, buying sex from "crack whores" and certain other services) the middle and upper reaches of the drug trafficking industry are wedded to money.

Burglaries and robberies now support much of the drug trade at the street level, along with fraudulent conversion of food stamps and other scrip. The interdependent economies of fencing and drug trafficking require the conversion of the tangible object into cash at some point. A certain amount of goods-for-drugs exists under current conditions, but there is always a cash transaction at some point in the barter chain. When that no longer is possible, the nature of the drug trade perforce must change.

When cash disappears, and the only means of purchase is a recorded, traceable electronic transaction, we can anticipate an initial constriction of the drug markets, followed by adaptation. The ideal result is a market constriction severe enough to drive addicts into rehabilitation programs. The documented history of short-term drug market constrictions is not hopeful in this regard, although at least one alternative – changing from one drug type to another – would be far less available in a non-cash economy than in the current one.

Short-Term Adaptation. Four primary alternatives are available in the short term: a switch to "home-grown" or self-produced drugs; targeted burglaries for legal drugs; drug tourism; and the use of foreign monies (while they remain in use) as a black-market currency. Eventually, we should anticipate that the drug trade will become an electronic chameleon, disguising its transactions through an ever-changing series of false fronts, (discussed below under

"Adaptation") because the issue applies to more crime than just drugs.

Self-Production. "Home-grown" marijuana has been a staple of the American drug scene for decades. Hydroponics and indoor production capacities accelerated the marijuana market, boosting THC content and overcoming the physical limitations of non-tropical climate and soil. Pot remains a relatively mild drug, however, and is an unlikely alternative to harder drugs.

The transformation of methamphetamine (meth) manufacturing from a product of clandestine laboratories to a "do-it-yourself" industry remains a problematic possibility. The process is widely understood and involves the use of chemicals commonly employed for other purposes. A limited number of addicts will probably attempt to create similar processes, the modern-day equivalent of "bathtub gin," for their drug of choice.

While sales of medicines can be tracked, the pharmaceutical industry remains vulnerable to a variety of other threats: shrinkage at the manufacturing source, hijacking in transit, and shrinkage at the retail source are major sources. Shrinkage can be controlled through surveillance and competent inventory control measures, though such measures are themselves vulnerable to corrupt insiders. Hijacking can be curtailed by GPS and RFID tracking, and additional security measures can make theft more difficult for individuals acting alone. All of these additional measures come at considerable cost, which likely will be passed on to consumers.

Targeted burglaries for legal drugs. "Scrip mills" – doctors who write prescriptions for legal drugs in high volume, with no medical justification (the recent Oxycontin indictments are one example) – will remain a route through which addicts can obtain drugs. However, if paper money disappears, it is probable that paper scrip will do so also (paper scrip is one potential form of alternate currency for the drug-dependent subculture). Prescriptions forwarded directly to pharmacies from physicians' offices bring the physician, the pharmacy, and the patient under greater and automatic electronic scrutiny. At most, the scrip mill will be a short-term accommodation, as any large influx of addicts from the street will draw attention to the mill very quickly. More circumspect operations will remain a boutique industry.

The next most vulnerable target will be the homes of those who have purchased drugs legally for legitimate medical purposes. There are three broad models for this level of adaptation. The first is simply serial burglary until drugs are discovered. The second is a variation of the first (serial burglaries that obtain drugs) where individuals target specific residences for return visits after the stolen drugs are replaced. Both are relatively low-skill approaches that leave the predator vulnerable to law enforcement.

The third involves a greater skill level in computer hacking, targeting either doctors' offices or pharmacies to obtain prescription data. Burgling addresses known to have desirable drugs, but with sufficient diversity of addresses to avoid or forestall capture, may be the mark of the higher-functioning addict.

At the present time, such a resort would be limited to higher-functioning addicts, who have greater-than-normal computer skill level combined with reasonably sophisticated burglary prowess. (Drug-sharing between hackers and accomplished burglars is one possible networking adaptation, of course.) As more of the population grows up with computer skills beyond those of the transitional generation, that equation may change. Police should anticipate a spike in burglaries, and of incidental violence associated with home invasions.

Drug Tourism. If drug tourism is possible, it means that there are cash transactions for drugs somewhere in the world, and the drug traffickers remain in business on the old model in other parts of the world. Those with the means to travel will do so, converting American electronic money to local cash equivalents to purchase drugs in foreign locales. A quasi-legal variant of that has already been observed in the border-crossing into Canada for cheaper pharmaceuticals. Returning to the country with sufficient quantities of drugs for long-term personal use will remain problematic.

Drug tourism, whether foreign or domestic, is a speculative adaptation. It would require the acquisition and importation of large amounts of foreign currency on a fairly regular basis. It might temporarily deflect fraud, burglaries, and robberies to foreign lands but would also have a ripple effect on border areas in the U.S. Drug dealers might encourage the practice in order to retain their markets, but such a system is fraught with additional potential risks that might imperil their business model.

Token economies. It might be possible for token economies, based upon foreign currency, to emerge in pocket areas of the United States, particularly near ports of entry: land borders, cities, and metropolitan areas with major international airports, etc. If that phenomenon develops, it may well be accompanied by internal drug-seeking migration, creating concentrations of addicts in the zones where alternative economies allow open drug markets to survive.

Since precious metals and jewels have served as safeguards against currency fluctuations through the ages, we can anticipate that they would constitute the first resort of an alternative currency for street level markets. The logical result would be an upswing in burglaries and street robberies, at least in the short term.

Street Robberies

Street robberies would no longer yield cash, credit or debit cards, food stamps, or welfare cash cards. The proportion of robberies committed to gain cash for drugs is largely undocumented, but they likely constitute a fairly large proportion. Robbery for jewelry or high-end sneakers remains a possibility, as anything that has immediate value to the robber would still be a target.

We would not expect robbery reports to disappear entirely, but they could become a category dominated by the fringe elements of society that operate purely local, token economies. A homeless person hitting another homeless person over the head for a blanket or a whiskey bottle still constitutes a robbery.

The most important impact would likely be the reduction in violence attending street robbery. Incidental injuries that attend the low-violence crime of purse-snatching will be reduced to a minimum, even if purse-snatching continues for other reasons, such as obtaining prescription drugs (see note 2).

Welfare Fraud A secondary benefit in this area may be the reduction in welfare fraud. The crime spike associated with "Mothers' Day" – robberies and burglaries for the cash obtained when welfare checks are cashed -- would be abated. Direct linkage of appropriated funds to the individual client via biometrics makes it impossible to claim that a welfare check, card, or scrip was stolen, in hopes of obtaining a replacement (or a second check to augment the first one).

Burglaries

It would be rash to anticipate the end of burglary. We tend to associate burglary with the theft of goods for resale for cash, but burglaries are also committed ancillary to assault, rape, and murder. Certain goods may also be stolen for their own use, especially liquor, jewelry, fetish items, and small electronics; the targeted burgalries for drugs discussed above fit this category. Thrill-seeking burglaries, those committed to install eavesdropping equipment (for salacious purposes, blackmail, or other purposes), and break-ins of vacant premises for partying or other illicit activities will still occur.

New motivations for burglary may arise. Since computer-based financial transactions can be tracked, the smarter thief will not use his or her own computer to attempt to use stolen codes. Concealing the trail initially will not long delay the identification – indeed, the ownership of the receiving account will be more important than the IP number of the origin of the transfer – but it provides a small cushion of time for the robber to move.

Firearms

On the surface, a cashless economy could be seen as a barrier to the unrestrained firearms market, leading to a reduction of firearms violence. Whether that would be the result is not clear, although it is not unrealistic to hope for market constriction. Political resistance is a predictable countermeasure (an extension of the current political debate over gun control); the value of firearms in an underground token economy is another variable.

Having to purchase firearms in a biometric system, automatically linking the buyer to their particular weapons, would constitute a *de facto* registration process in the view of the Individual Right of Ownership movement. The impact on gun shows, currently an end-run around the requirements of the Brady Law, is uncertain, although as long as parallel systems exist, we would expect firearms sellers and buyers to use the most anonymous form of exchange available.

Perhaps the staunchest resistance to biometric commerce will come from the NRA and other activists who interpret the Second Amendment as permitting individual ownership of firearms. The political clout of the movement is likely to endure, forestalling additional gun registration and tracking legislation. It is less likely that the movement can require the existence of cash solely for the purposes of permitting untraceable firearms purchases. The political emphasis would probably shift to fostering legislation that exempted firearms purchases from data-mining and certain types of government review, an ephemeral gain at best.

Firearms will be highly prized commodities in any token economy, and gun "swaps" – forearms traded for other firearms – is a likely countermeasure.

Adaptation

The logical implication of the foregoing issue is that the focus of crime will shift to beating the system or corrupting it. The former will probably continue to be the province of the lone hacker or small hacker network; the latter will become the provenance of organized crime.

Countermeasures. Gaming the system with false accounts and purchases is the first probable countermeasure for laundering money in a, supposedly, all-seeing system. Shell corporation and sham buyers are already well-known features in the landscape of fraud and money-laundering; the new criminal science will be the creation of algorithms that can fool whatever automated scanning system is used to assure system integrity.

One potential change in this arena may be the nature of political corruption. Cash is the primary grease of most political corruption (blackmail, the threat of exposure, is another), but electronic transfers cannot be stored separately in a freezer or a safe-deposit box. They have to be available to the candidate or office-holder, and thus are vulnerable to scrutiny (unless the payments are made to an avatar).

The end-game remains that all electronic transfers can be tracked, eventually. To be a criminal in the electronic economy will require one to shift from one false identity to another with sufficient speed and agility to forestall discovery by human investigators or an Artificial Intelligence system. Although older forms of criminal coercion will not disappear, the new criminal elite will be those who can command expertise in rapidly-evolving electronic technologies.

We should anticipate a brisk business in the creation and maintenance of false on-line identities, both for individuals and for corporate entities. There may even be a new market for dissolution, "electronic acid"; it is far easier, and considerably less painful, to alter digital fingerprints than physical ones. Corruption of enforcement officials at all levels is a potential countermeasure, but the currency of such corruption would still be electronic (absent elements of blackmail and other forms of coercion). From the perspective of the criminal elite, the best defense will be the corruption or control of the system's guardians.

Second Life is already drawing attention as its on-line economy has already "broken the fourth wall (see note 3), merging real funds with the token on-line economy. While probably not yet so well-developed that it could serve as a money-laundering network for illegal drug trafficking or other criminal enterprise, it represents a plausible future. Though avatars are still anchored in their flesh-and-blood creators, Second Life represents a potential multiverse of rapid-fire transfers, bifurcations, and recombination of funds. That we, in our relatively abstract contemplation, cannot envision exactly how it will be managed does not mean that entrepreneurial criminal minds are not already hard at work creating the possibilities.

NOTES

1 - The Social Security Number is a "complementary" system because was originally established for a single, exclusive purpose. It has since become the *de facto* universal identification number for the Internal Revenue Service. Though nominally not to be used for identification purposes, the SSN is required for all financial accounts as a way of monitoring income and tax responsibility. As such, it is embedded in the customer databases of all financial institutions.

2 - In legitimate pawning, the rightful owner surrenders the property; when the pawnshop serves as a fence (witting or otherwise), the thief presents the property. The two actions are otherwise fairly similar: the cash value of a pawned item is approximately 30 percent of the item's market (Fernandez, 2007). The most accessible source of information about stolen property lies in Steffensmeier's (1985) study of fences; his sources indicated that fences paid a price for "warm" goods ranging from 25 to 33 percent of market value. Fernandez's more recent report suggests that the market constraints have not changed significantly over the last quarter-century.

The nexus between the value physical property and its electronic representation has intriguing potential for crime prevention. Applying a biometric code to identify property (most likely in the form of an RFID-encoded chip, at least in terms of current technology) makes no more sense than using the Social Security Number (SSN) in the current system: the frequency can be captured, the number stolen, converted, and subsequently employed in fraudulent transactions. The system is effective only if it identifies the person exclusively.

That said, however, the transaction itself may inextricably link the property to the buyer, certainly in the first instance and as long as the item is resold through electronic channels. Item-for-item exchanges would not enter the mainstream data records, of course, but one of the interesting areas for speculation (and perhaps for the writing of law) is the means by which legitimate ownership of any property may be transferred within an economic system defined and monitored by biometric assurances. Whether the law would recognize informal transfers, or require formal transfers of property for legal exchange, is a matter of speculation.

Canskey's (1994) examination of "fringe banking" focused upon the provision of economic services to a socially disenfranchised layer of society. The attendant crime of pawning stolen goods was acknowledged, but not fully explored. Nevertheless, police in every major city routinely examine local pawnshop records in an effort to recover stolen property. The anonymity of cash transactions is somewhat mitigated by registration requirements, but a biometric economic system virtually guarantees identification of the thief.

3– “Breaking the fourth wall” is a theatrical term for those moments when an on-stage character addresses the audience directly, through the invisible “fourth wall” of the stage setting. (While we understand that our colleagues are fully aware of the meaning, we are conditioned to explain obvious-to-us terms by our students, who seem to have been sheltered from the liberal arts of our upbringing.) Here the term is used in a parallel setting, casting Second Life in the role of an ongoing Shakespeare play, and its real-world participants as the audience. The primary difference is that the fourth wall is permeable in both directions, a form previously found only in a limited way in interactive experimental theater. Where experimental theater was constrained by time, however, the electronic stage of Second Life is enduring, allowing for longer-term interactions, the formation of relationships and their evolution…. in short, a community sprung from the union of a masquerade ball and social networking.

REFERENCES

Associated Press (2007, August 10). Toll records trip up philanderers. *The New York Times.* Retrieved August 10, 2007, from http://www.nytime.com/aponline/us/AP-E-Z-Divorces.html.

Bequai, A. (1981). *The cashless society: EFTs at the crossroads.* New York: John Wiley & Sons.

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004). *Guide to biometrics.* New York: Springer.

Brin, D. (1998). *The transparent society: Will technology force use to choose between privacy and freedom?* Reading, MA: Addison-Wesley.

Fernandex, M. (2007, September 14). Cash to get by is still pawnshop’s stock in trade. *The New York Times.* Retrieved September 14, 2007, from http://www.nytimes.com/2007/09/14/nyregion/14pawn.html?ref=nyregion.

Frazer, P. (1985). *Plastic and electronic money: New payment system and their implications.* Cambridge, UK: Woodhead-Faulkner.

Good, B. A. (2000). *The changing face of money: Will electronic money be adopted in the United States?* New York: Garland.

Goolsbee, A. (2007, February 1). Now that a penny isn’t work much, it’s time to make it worth 5 cents. *The New York Times.* Retrieved February 1, 2007, from http://www.nytime.com/2007/02/01/business/01scenes.html.

Guttman, R. (2003). *Cybercash: The coming era of electronic money.* New York: Palgrave Macmillan.

Kent, S. T., & Millett, L. I. (Eds.). (2002). *IDs-Not that easy: Questions about nationwide identity systems.* Washington, DC: National Academy Press.

Kingson, J. A. (2004). Float time on checks shortens, as of Thursday. *The New York Times.* Retrieved October 28, 2004, from http://www.nytimes.com/2004/10/28/business/28/float.html.

Klockars, Carl B. (19xx). The Fence: Thirty Years of Wheelin' and Dealin'.

Orwell, G. (1949). *1984.* London: Secker and Warburg.

Ross, A. A., Nandakumar, K., & Jian, A. K. (2006). *Handbook of multibiometrics.* New York: Springer.

Solomon, E. H. (Ed.). (1987). *Electronic funds transfers and payments: The public policy issues.* Boston: Kluwer-Nijhoff.

Steffensmeier, D. J. (1986). *The fence: In the shadow of two worlds.* Totaw, NJ: Rowman & Littlefield.

Vacca, J. R. (2007). *Biometric technologies and verification systems.* Amsterdam: Elsevier.

Vielhauser, C. (2006). *Biometric user authentication for IT security: From fundamentals to handwriting.* New York: Springer.

Woodward, J. D., Jr., Orlans, N. M., & Higgins, P. T. (2003). *Biometrics: Identity assurance in the information age.* New York: McGraw-Hill/Osborne.

Yanushkevich, S. N., Stoica, A., Shmerko, V. P., & Popel, D. V. (2005). *Biometric inverse problems.* Boca Raton, FL: Taylor & Francis.

Sociology of the Internet: Effects of Social Technology on Policing

John Jackson
Bud Levin

The Internet provides virtual space for both activities and relationships. In many cases, the parallel to physical space is compelling. This short essay lays out some of those parallels, some differences, and some implications for police and policing.

In 1998, Kraut and colleagues (Kraut, Patterson, Lundmark, Kiesler, Mukopadhyay & Scherlis, 1998), published an interesting paper entitled, "Internet paradox: A social technology that reduces social involvement and psychological well-being?" The question mark is still with us.

Kraut et al. (1998) found that, "… greater use of the Internet was associated with declines in participants' communication with family members in the household, declines in the size of their social circle, and increases in their depression and loneliness." (p. 1017). These authors were appropriately cautious about generalizing their findings.

The article has attracted a fair amount of interest – it has been cited in more than 700 publications in the ensuing years. While some of the underlying issues have not been laid to rest, more recent research seems in general to support the earlier conclusions, e.g., "Longitudinal analyses from a large national panel of Americans suggest that using the Internet may lead to declines in visiting with friends and family. This effect is largest for those who initially had most social contact, i.e., the extroverts."(Shklovski, Kraut & Rainie, 2004).

The above should not shock; time spent doing one thing generally is time that cannot be spent doing something else. At the very least, it is likely that the more time we spend on the Internet, the less time we spend building connections with our household members and our neighbors. Given the connections between community and crime prevention, it should be clear that our increasingly networked society creates the potential for vulnerability to crime.

Happiness, too, is threatened by the Internet and other rapidly changing features of modern life. For example:

> "One of the key insights of happiness studies is that people have a very hard time being content with what they have, at least when they know that others have more. Today, technological change is so rapid that when you buy something, you do so knowing that in a few months there's going to be a better, faster version of the product and that you're going to be stuck with the old one. Someone else, in other words, has it better. It's as if disappointment were built into acquisition from the very beginning (unless you're buying a 70-inch plasma screen, in which case you should be fine for at least a couple of years). There's no way to circumvent this drooping of the spirit, which creates dissatisfaction in the heart of the modern consumer." (Surowiecki, 2005, unpaginated).

Few police prefer to work with or “serve” unhappy people. Increasingly, thanks to the Internet and other rapidly changing domains, that will be our lot.

The above putative effects of the Internet are the tip of the iceberg. Consider the following, as they apply to policing:

1. How are the anchoring effects of reference groups, perceived normality, mores and norms affected by participation in virtual “communities”?

2. How are identities, privacy, confidentiality, secrecy, the “personal” affected by such participation?

3. How do communities and networks morph as we shift from physical to virtual realms – and back? Dimensions one might consider include formal/informal, dynamic/static, adaptive/maladaptive behavior, the mutual influences of physical and virtual interaction, etc?

4. What are the implications for life and for policing of the differential use of the Internet by different social strata, e.g., the Pew datasets?

5. Technology increasingly is the way the world works, but like the physical world the virtual world filters both passively (effort required) and actively (banning, expulsion, triangulation, etc).

6. When we talk about the “global” (economy, migration, etc), what is the virtual equivalent? Is the Internet a solution to problems of jurisdiction or just another problem?

7. Is the Internet a conduit or [social] process? If it is process, it is not content-neutral. Rather, it shapes what passes through it. Consider how that might influence social relationships, both temporally and qualitatively. Also consider whether the Internet can function as a “safety net” versus merely as a set of “knowledge resources”

8. Huntington’s (1993) clash of civilizations has implications for the digital world as well. Consider again both conduit and [social] process.

9. The umwelt of the line dog has changed markedly. Cops have always been about relationships, including relationships with other cops. Increasingly, those relationships are becoming virtual rather than physical and external to the organization or organizational unit. Those new relationships enhance the flow of information. Information breeds power. Power to the line dogs will likely affect power relationships within the agency but also have implications for training and other professional development, cultural change, and officer marketability.

References

Huntington, S. P. (1993). The clash of civilizations. *Foreign Affairs 72*(3), 22. Retrieved September 15, 2006, from http://www.foreignaffairs.org/19930601faessay5188/Samuel-p-huntington/the-clash-of-civilizations.html.

Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukopadhyay, T. and Scherlis, W. (1998). Internet paradox: A social technology that reduces social involvement and psychological well-being? *American Psychologist*, *53*(9), 1017-1031.

Shklovski, I, Kraut, R. & Rainie, L. (2004). The Internet and Social Participation: Contrasting Cross-Sectional and Longitudinal Analyses. *Journal of Computer-mediated Education, 10*(1). Retrieved September 15, 2006, from http://jcmc.indiana.edu/vol10/issue1/shklovski_kraut.html.

Surowiecki, J. (2005). Technology and happiness: Why getting more gadgets won't necessarily increase our well-being. *Technology Review*. Retrieved September 15, 2006, from http://www.technologyreview.com/printer_friendly_article.aspx?id=1401.

Insights into the Hacking Underground

Michael Bachmann & Jay Corzine

The Exigency of Cyber-Crime Research and Intervention

Estonia, April 26, 2007. In retaliation for the removal of a World War II-era statue of a Soviet soldier, pro-Russian hackers launched a month-long campaign that has become known as the first war in cyberspace. Using a technique known as distributed denial-of-service (DDoS) attack on a hitherto-unprecedented scale, the attackers managed to effectively shut down vital parts of Estonia's digital infrastructures. In a coordinated effort, an estimated one million remote-controlled computers from around the world were used to bombard the web sites of the President, the Prime Minister, Parliament and other government agencies, Estonia's biggest bank, and several national newspapers with requests. The attacks were so massive that NATO rushed a cyber-warfare team of international security experts to assist the Estonian government, and Jaak Aaviksoo, the country's defense minister, described the attack as a national security situation and requested that the European Union classify it as an act of terrorism (Landler & Markoff, 2007). In reference to the events in Estonia, Suleyman Anil, the head of NATO's incident response center, later warned attendees of the 2008 E-Crime Congress in London that "cyber defense is now mentioned at the highest level along with missile defense and energy security." According to Anil, "we have seen more of these attacks and we don't think this problem will disappear soon. Unless globally supported measures are taken, it can become a global problem" (Johnson, 2008, p. 1).

The above example is merely one incident of what have become a long series of high-profile hacking attacks (Aguila, 2008). Although warnings of the societal-level threat posed by cyber-attacks on critical network infrastructures have been heralded since the 1980s, it is only in recent years that the problem has made it onto the radar screens of governments. Partly due to the experience of Estonia, the U.S. and other countries around the globe are now reassessing the security situations of their key information systems. They are enacting new security measures to better protect their critical network infrastructures, and they are increasing their readiness to respond to large-scale computer incidents (NCIRC, 2008). In Britain, for example, Conservatives have recently proposed the creation of a new position for a cyber-security minister and a national hi-tech crimes police squad to better combat the "growing and serious threat to individuals, business and government […] that will continue to escalate as technology changes" (Johnston, 2008, p. 1).

The implementation of effective technological countermeasures against hacking attacks is facilitated by the knowledge that has already been accumulated through computer science research (cf. Chirillo, 2001; Curran et al., 2005; Erickson, 2008). Several studies conducted by computer scientists and computer engineers have closely examined the technical details of the various attack methods and have produced a significant body of information that can now be applied to help protect network infrastructures (Casey, 2004). Unfortunately, the guidance provided by these studies is limited to only the technical aspects of hacking attacks and, in contrast to the substantial amount of knowledge already gathered about how the attacks are performed, answers to the questions of who the attackers are and why they engage in hacking activities continue to remain largely speculative. Today, the persons committing the attacks remain mysterious for the most part, and information about them continues to be only fragmentary.

The current lack of information concerning the sociodemographic characteristics and the motives of cybercrime offenders can be attributed to a number of issues. One of the main reasons can be traced back to the unfortunate circumstance that, until recently, mainstream criminology has underestimated the potentially devastating societal impacts of cybercrimes and has diverted only limited attention to this relatively new type of criminal behavior (Jaishankar, 2007; Jewkes, 2006; Mann & Sutton, 1998). Cyber-criminology is only now beginning to evolve as a distinct field of criminological research, and it has yet to overcome many methodological and theoretical problems that other areas in criminology have already solved (Yar, 2005, 2006). Law enforcement responses have also been slow to develop and are hampered by several characteristics of cybercrimes, notably the frequent location of perpetrator and victim in different states or nations.

A particular challenge for researchers arises from the various methodological obstacles entailed in the sampling of cybercriminals. As a result of these difficulties, available data sources are scarce, and quantitative studies, such as the annual CIS/FBI Computer Crime and Security Survey, are limited to surveys of cybercrime victims. At this point, only a few qualitative case studies (eg. Mitnick & Simon, 2005; Schell, Dodge, & Moutsatsos, 2002; Taylor, 1999, 2000) and biographies (eg. Mitnick, Simon, & Wozniak, 2002; Nuwere & Chanoff, 2003) exist that examine individual hackers; their motivations, preferences, and hacking careers. While such studies are well suited to provide in-depth insights into the lives of a few individuals, they are unfit for providing generalizable information about the population of hackers at large. Yet, just “like in traditional crimes, it’s important to try to understand what motivates these people to get involved in computer crimes in the first place, how they choose their targets and what keeps them in this deviant behavior after the first initial thrill” (Bednarz, 2004, p. 1).

The aim of this paper which is excerpted from the first author’s dissertation research is to begin filling the wide gap in our knowledge about hackers and the hacking community by providing the first quantifiable insights into the hacking underground. Such insights are needed to create a more profound understanding of the nature of the threat and a more complete assessment of the problem and its solutions. The identification of the reasons and motives behind cyberattacks is not only beneficial for the effective direction of investigation and prosecution efforts and resources; it also helps to better identify the actors' behaviors, to develop better countermeasures, and to make IT systems safer.

Research Design

The goals of the study were to provide generalizable answers to the questions of who hackers are and why they hack. To achieve these goals, the research project was designed to produce quantifiable results that are more representative and can be generalized to a wider target population than those from previous qualitative case studies of hackers (Jordan & Taylor, 1998; Taylor, 1999). A survey was developed and used for data collection (Boudreau, Gefen, & Straub, 2001), because surveys are the data-collection method best suited to produce quantitative results that can be generalized to other members of the population of interest and oftentimes even to other similar populations (Newsted, Chin, Ngwenyama, & Lee, 1996). The survey consisted of a total of 72 items and gathered detailed information about the various phases of the respondents' hacking careers. It embodied items pertaining to the initiation of the hacking activity, its habituation, and the eventual desistance from hacking. It further assessed several other details of the respondent's hacking activity, including a variety of involved decisions and motivations.

The survey was fielded during the 2008 ShmooCon convention in Washington D.C. The ShmooCon convention was selected because its profile attracts a wide variety of hackers and security experts (Grecs, 2008), thus making it the ideal candidate to gather information about the larger population of hackers. Since its first convening in 2004, ShmooCon has developed into one of the largest annual conventions worldwide. Today, it is the largest hacker convention on the East Coast, and it is attended by both U.S. and international hackers and security experts. The 2008 convention was held over the weekend from Friday, February 15 to Sunday, February 17 in the Marriott Wardman Park Hotel in Washington D.C. It was attended by a total of 800 hackers and security experts. Of those, only hackers who had broken into computer systems, networks, or websites illegally, i.e. without an explicit permission from an authorized party, were selected for the study. This restriction systematically excluded about one-third of all attendees, who either claimed to hack only when legally contracted for testing purposes or attended the convention simply because they were interested in computer security issues but had never committed an actual hacking attack. The final sample consisted of 124 individuals, yielding a response rate of approximately 25 percent of the eligible attendees.

Findings

The study shows that the common stereotype of the hacker as a clever, but lonesome male adolescent whose computer proficiency compensates social shortcomings barely begins to tell the whole story of hackers' identities. That is not to say that this stereotypical portrayal of hackers is completely mistaken. Several aspects of the stereotype were indeed confirmed by the survey results as well as the researcher’s personal observations during the conference. The participants in this study were indeed highly educated, intelligent persons who focused their intellectual interests on technological developments. Ninety percent of all respondents had at least some college education, and over one-fourth (27 percent) had attained either a Masters or a Ph.D. degree. Many of these technophiles appeared to be equally inventive, creative, and determined. These personality attributes emerged in several findings, including the predominant role of inquisitive motives for hacking activities, hackers’ unusually high confidence in their general decision-making ability, and their typically extensive portfolio of various attack methods.

Consistent with the dominant stereotype, the convention attendees were also predominantly male (94 per cent), and minority hackers were rare exceptions. Over 93 percent of the hackers in the sample were Whites, a fraction that substantially exceeds their percentage in the U.S. population. Another noteworthy finding is the fact that Asians (5 per cent) were the largest minority in the sample. This result reflects the racial distribution in most IT professions (Zarrett & Malanchuk, 2005). The near uniformity with regard to the sex and race distributions, however, stood in sharp contrast to the strong emphasis of many attendees on individualism. Many hackers conveyed their individualistic nature in conversations with the researcher as well as through their physical appearances. Their physical expressions of individualism ranged from extravagant haircuts and hair colors, to unusual clothing styles, to large tattoos on various body parts, sometimes even on faces.

The two most important inadequacies of the hacker stereotype seem to be the notions that hackers are invariably young and that they are socially inept. The average hacker in the sample was 30 years of age, a finding that calls the common notion of the prototypical hacker as a delinquent teenager (Yar, 2005) into question. It is reasonable to assume that the higher average age in this study of convention attendees was caused by the sampling frame of this particular research project. The attendees’ profile at the ShmooCon convention was geared more toward security experts and computer professionals than to teenagers who pursue their hacking interests merely as a leisure-time hobby. Thus, while the distribution in this particular sample is certainly not enough to refute claims that the majority of hackers are teenagers, nevertheless, it indicates that the hacking community is by no means limited to youth. To the contrary, it involves many mature security experts and many seasoned hackers who pursue their hacking activity in a professional manner. The data clearly show that hacking is not just a “young man’s game.” The oldest active hacker in the sample was 52 years old, and he reported to have been hacking for close to three decades. Most importantly, the data also revealed that hackers undergo a maturation process over the course of their hacking careers and that the more experienced and seasoned hackers tend to be the most dangerous ones. They are more likely to attack higher profile targets, and some engage in their illegal hacking activities with financial profits as their primary motivation. Young and inexperienced hackers can certainly cause damage with their activities, but the study shows that these hackers attack primarily private targets and do so out of intellectual curiosity, love for knowledge, experimentation, or boredom. Many hackers first become interested in hacking in their teenage years, and, typically, they are not driven by a pronounced initial criminal intent or the desire to make financial profits. As their hacking activities continue to become habitualized, however, many of them develop into more professional and ambitious hackers. Over the course of their hacking careers, many intensify their hacking activities and begin to also attack higher profile targets such as governmental and corporate information systems. Some hackers even reported having turned their once merely deviant juvenile behavior into a criminal business activity. A total of 15 percent of all respondents said that hacking has become their main source of income and that they would reject a target unless it was profitable. Undoubtedly, these experienced veteran hackers should receive the bulk of attention from law enforcement.

Although the comparatively high fraction of unmarried hackers showed that many of them may indeed be hesitant to engage in serious relationships and commitments, the vast popularity of social hacking methods and their high success rates also indicated that the commonly presumed social incompetence of hackers is misleading. The falseness of this assumption was further reaffirmed by some of the observations the researcher made during the convention. Most attendees appeared to be outgoing and sociable. Many attended the convention together with their friends, and most of the attendees seemed to share a distinct sense of humor and mingled quickly. Certainly, the informal observations during the convention and the finding that hackers are skilled in manipulating and “programming” other persons, oftentimes managing to exploit the trust or carelessness of other computer users for their hacking purposes, are not sufficient evidence to strongly reject of the notion that hackers are social hermits. It might be that the sociability of hackers is limited to interactions with likeminded technophiles and that, although many appear to be skilled manipulators, genuine and affectionate social relations are of lesser importance to them. Additional examinations of the social networks of hackers; including their amount, frequency and quality of interactions with close contacts, the types of contacts they engage in (face-to-face or online), and the importance they attribute to these social contacts, are needed.

The debate about the sociability of hackers aside, one of the most important findings of the study was the significant role of social hacking methods. While many persons think of hacking attacks as performed solely through technical means and exploits, they are in fact more diverse and oftentimes involve a combination of technical methods, social methods, and circulations of different kinds of malicious code, such as viruses or

Trojan horses (Erickson, 2008). In the context of hacking attacks, the term social methods denotes a variety of attacking techniques that can be summarized as attempts to establish and subvert trust relationships with victims or to predict the behaviors of victims. Once such a relationship is established, the attacker tricks the victim into revealing information or performing an action, such as a password reset, for example, that can then be used in the attack. To gain a clearer picture of the prevalence of each of the three types of attacks and to obtain a better understanding of the composition of typical hacking attacks, all three types of attacks were assessed independently.

The separate analyses of the three main hacking techniques showed that many hackers combine social and technical methods and launch attacks that are comprised of both tactics. The more detailed examination of preferences for certain types of technical hacking attacks confirmed that many hackers combine different reconnaissance methods with different intrusion and cover-up techniques. Of the different technical methods to gain access to a system, the various techniques to obtain passwords were the most frequently used. These results suggest that the classic exploitation of password weaknesses remains popular today. Overall, the success rate reported by all respondents showed that, personally, they estimated about half (48 per cent) of all their technical intrusions to have been successful. While a close to 50 percent success rate of all technical intrusions is high, the estimated success rate of social methods was even higher (62 per cent). This very high success rate for social methods was one of the most surprising findings in this study. It demonstrates that the popular image of hackers as social hermits who launch their hacking attacks solely through remote computer and network technology, or even do so mainly to compensate for social deficits, has to be revised. The opposite seems to be the case. Hackers seem to be socially capable persons who know how to successfully manipulate and trick other persons. Moreover, the study showed that hackers who combine social and technical attack methods were the most successful ones. The common perception of hacking attacks as being executed solely through technical means and the perception of hackers as socially incompetent are most likely part of the reason why the danger posed by social engineering attacks is oftentimes underestimated. Unless these perceptions are revised and the awareness of social hacks is raised, social engineering methods will predictably continue to be very successful and will continue to pose a serious threat to individuals and organizations.

Different from social and technical attack strategies, which were very popular and oftentimes used in combination, the reported distribution of malicious codes was rare. Thereby, the surveyed hackers demonstrated having a strong preference for directed attacks on selected targets over widely dispersed and randomly distributed attacks without specific targets. It appears that phishers, spammers and virus coders are a group of cybercriminals that is distinctively different from “traditional” hackers.

Policy Implications

The conclusions that can be derived from this study are not limited to contributions to the scientific discourse about cybercrime offenders. They also hold some important implications for efforts to combat cybercrimes. Experts agree that current strategies to combat this threat face a multitude of challenges that have to be addressed. Aside from the resource shortages and other practical difficulties, law enforcement efforts to combat cybercriminals are also hampered by a shortage of substantive and reliable information that can be used for the creation of offender profiles. Detailed profiles of the different types of cybercriminals, their skill levels, and their motivations are critical because they provide helpful guidance for ongoing investigation of cybercrimes and, thereby, increase the effectiveness of current prosecution efforts. A more effective response by both the criminal justice system and the private sector is urgently needed—not only because it would increase the number of convicted cybercriminals but, more importantly, because it would also have a preventive deterrence effect on the larger hacking community.

In relation to law enforcement, the findings of this study suggest that the creation of a deterrent effect through enhanced apprehension and prosecution is an essential component of efforts to combat cybercrime. Unfortunately, present efforts to curb cybercrimes are hardly suited to accomplish this goal. Despite the annually increasing number of cybercrimes, only a relatively few high profile cases are successfully tried at present, and many of them do not lead to swift or severe punishments (Brenner, 2006). The continuing unlikeliness of punishment is particularly problematic because it severely undermines any efforts to deter criminal behavior in cyberspace. Indeed, the findings of the present study demonstrate that many hackers are aware of the slim chances of being detected and punished. The current improbability of becoming prosecuted even led some hackers to report that they have never been afraid of being apprehended or prosecuted. Furthermore, the risk awareness of most hackers seems to decrease over time as they repeatedly learn that their actions have no negative consequences for them.

Nevertheless, several findings from this study also signify that deterrence can be a successful strategy to prevent cybercrimes. The study revealed that many hackers have a nuanced risk awareness. For example, the majority of hackers report having become more concerned about risks in recent years, a finding that suggests that increased efforts to combat cybercrimes do not go unnoticed in the hacking community. Furthermore, many hackers evidently distinguish between the chances of becoming detected and apprehended and the consequences of these two events. Most importantly, the data also indicate that the most successful hackers are the ones that also have the highest risk awareness. Thus, these hackers seem to be the ones that are most susceptible to changes in risk estimates.

Deterrence undoubtedly is an indispensable component in the control of all criminal behaviors, but is seems to be particularly suited to prevent cybercrimes. Unlike other, less deliberately acting types of criminals, hackers plan their hacking attacks, and they oftentimes do so in an explicitly rational manner. Consequently, they should be more easily dissuaded than criminals who commit their crimes spontaneously when opportunities arise. Taken together, the findings of this study suggest that a more pronounced deterrence perspective needs to become a central addition to the existing technical approaches to cybercrime prevention. However, merely adding deterrence as one separate component will not suffice. To be effective, a deterrence perspective has to be integrated into currently existing national policy efforts beyond the criminal justice system. One promising approach to establish deterrence policies in the private sector could be directed at businesses and organizations. The study showed that most hackers pursue legal careers in legitimate jobs and companies. Organizations and companies that offer IT security services or are otherwise attractive to hackers should be encouraged to promote awareness of the potential consequences of committing cybercrimes. For example, they could distribute information about punishments that have been given to convicted computer criminals as well as other informational materials that directly highlight what constitutes a crime under the law. Other informal control mechanisms, such as extra-legal social stigmata or the systematic introduction of negative effects on job opportunities, might also be strong incentives to prevent particularly young, middle-class computer experts from becoming involved in computer crime. Unquestionably, the establishment of effective deterrence efforts as an integral part of cybercrime prevention strategies will not be an easy undertaking. The vast range of cybercrime activities and the multitude of different offenders considerably complicate the selections of the most appropriate deterrence policies. Strategies that are most effective for leisure-time juvenile hackers will most likely be unfit to deter destructive computer-security experts or other seasoned hackers from attacking computer systems for monetary gains. Nonetheless, deterrence should be pursued as a mitigation strategy, because even limited accomplishments can prevent some crime incidents and provide some protection from an increasingly serious problem. Companies in branches that typically employ hackers can certainly be particularly helpful in deterring computer crimes, but the results of this study also indicate that all companies and organizations need to do more to actively prevent victimization, regardless of their branch. The analysis of the different hacking methods showed that, of the three main types of attack methods, social engineering attacks are the most successful ones. It also revealed that the various methods to obtain user passwords, whether the systematic guessing of weak or standard passwords or the theft of user logins, remain the most common ways hackers gain access to their targets. Thus, it seems that the weakest points of companies and organizations are their employees. Corporations have to educate their employees about social hacking methods. They need to raise awareness of the seriousness and frequency of the problem, educate their staff about the wetware tactics commonly used by hackers, and give them instructions of how to avoid becoming victimized.

The education of employers, while definitely an important protective measure, is not the only contribution that will be required from organizations. They also need to start reporting all their victimization incidents to the authorities. The current situation, in which many organizations refrain from reporting incidents to protect their own interests and thereby harm the interest of all businesses, needs to be changed because, unless more incidents are reported, computer crimes are unlikely to become controllable. The benefits and detriments of a mandatory reporting system are debatable, but a reporting requirement would certainly benefit efforts to manage cybercrimes. It would put law enforcement agents in the position to decide which cases to devote their attention to rather than be dependent on the willingness of organizations to submit their cases in order to press charges.

Concluding, it has to be pointed out that cybercriminology is only just beginning to develop and our knowledge about cybercrime offenders remains fragmentary at best. The present study yields some important insights into the composition of the hacking underground, and it sheds some light on the motivations and maturation processes of hackers. Nevertheless, it is but one step toward the establishment of cybercriminology as a distinct subfield of criminological research and the development of successful strategies of prevention and apprehension by law enforcement and prosecution by the courts.

References

Aguila, N. (2008). The fifteen greatest hacking exploits: The birth of hacking. March 16. Retrieved from http://www.tomshardware.com/2008/03/14/the_fifteen_greatest_hacking_exploits/index.html.

Bednarz, A. (2004). Profiling cybercriminals: A promising but immature science. May 3. Retrieved from http://www.networkworld.com/supp/2004/cybercrime/112904profile.html.

Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly, 11*(1), 1-16.

Brenner, S. (2006). Defining cybercrime: A review of state and federal Law. In R. D. Clifford (Ed.), *Cybercrime: The investigation, prosecution, and defense of a computer-related crime* (pp. 13-94). Durham, NC: Carolina Academic Press.

Chirillo, J. (2001). *Hack attacks revealed: A complete reference with custom security hacking toolkit*. New York: John Wiley.

Curran, K., Morrissey, C., Fagan, C., Murphy, C., O'Donnell, B., Firzpatrick, G., et al. (2005). Monitoring hacker activity with a honeynet. *International Journal of Network Management, 15*(2), 123-134.

Erickson, J. (2008). *Hacking: The art of exploitation* (2nd ed.). San Francisco: No Starch Press.

Grecs. (2008). ShmooCon 2008 infosec conference event. April 25. Retrieved from http://www.novainfosecportal.com/2008/02/18/shmoocon-2008-infosec-conference-event-saturday/.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology, 1*(1), 1-6.

Jewkes, Y. (2006). Comment on the book 'Cyber crime and society' by Majid Yar. September 09. Retrieved from http://www.sagepub.co.uk/booksProdDesc.nav?prodId=Book227351.

Johnson, B. (2008). Nato says cyber warfare poses as great a threat as a missile attack. May 2. Retrieved from http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity.

Johnston, P. (2008). Tories want new cybercrime police unit. March 07. Retrieved from http://www.crime-research.org/news/06.03.2008/3236/.

Jordan, T., & Taylor, P. A. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757-780.

Landler, M., & Markoff, J. (2007). Digital fears emerge After data siege in Estonia. *The New York Times*. August 25. Retrieved from http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=1&ei=5070&en=15ee9940d96714da&ex=1188187200.

Mann, D., & Sutton, M. (1998). Netcrime. More change in the organisation of thieving. *British Journal of Criminology, 38*(2), 210-229.

Mitnick, K. D., & Simon, W. L. (2005). *The art of intrusion: The real stories behind the exploits of hackers, intruders & deceivers*. New York: John Wiley.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). *The art of deception: Controlling the human element of security*. New York: John Wiley.

NCIRC. (2008). NATO opens new centre of excellence on cyber defense. May 3. Retrieved from http://www.nato.int/docu/update/2008/05-may/e0514a.html.

Newsted, P. R., Chin, W., Ngwenyama, O., & Lee, A. (1996). *Resolved: Surveys have outlived their usefulness in IS research.* Paper presented at the Seventeenth International Conference on Information Systems, Cleveland, OH.

Nuwere, E., & Chanoff, D. (2003). *Hacker cracker: A journey from the mean streets of Brooklyn to the frontiers of cyberspace*. New York: Harper Collins.

Schell, B. H., Dodge, J. L., & Moutsatsos, S. (2002). *The hacking of America: Who's doing it, why, and how*. New York: Quorum.

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. London and New York: Routledge.

Taylor, P. A. (2000). Hackers - cyberpunks or microserfs. In D. Thomas & B. Loader (Eds.), *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

Yar, M. (2006). *Cybercrime and Society*. London: Sage.

Zarrett, N. R., & Malanchuk, O. (2005). Who's computing? Gender and race differences in young adults' decisions to pursue an information technology career. *New Directions for Child and Adolescent Development, 2005*(110), 65-84

CYBERVICTIMIZATION

Jeri N. Roberts
Tina Jaeckle
Thomas A. Petee
John P. Jarvis

One aspect of computer crime that has been underdeveloped in the cybercrime literature is victimization. More specifically, there has been a paucity of information on the victimology of cybercrime – characteristics and demographics on those individuals and organizations that are victimized by cybercriminals. Do they look like the victims of conventional crime, or are they different in some respects? Moreover, as the cyber landscape continues to evolve, will victim characteristics change to any significant degree?

TYPES OF CYBERVICTIMIZATION

The nature and variety of victimization with cybercrime in some ways parallels the complexity we see with conventional criminality. A long standing distinction has often been made in criminology between *crimes against persons* and *crimes against property*. That same distinction can be made with computer-related crime, although there are some unique elements that occur with cybercrime that blur that distinction and which may change the nature of criminal victimization in the future.

Personal Forms of Cybercrime

Crimes against persons, or personal crimes, usually involve situations where the offender uses some conception of force or coercion against a victim. What constitutes "force" for these offenses is somewhat flexible but commonly will involve a physical element. Consequently, "crimes against persons" is sometimes used interchangeably with "violent crime", although they are not fully synonymous. With conventional criminality, there is a notion that personal crimes require a certain degree of propinquity between the offender and victim, as is the case with most instances of crimes such as assault, murder, rape or kidnapping. Although there are exceptions (e.g., a situation where a sniper shoots a victim at some significant distance), the vast majority of these types of personal crime do involve direct contact between the offender and the victim. Computer-related crime, almost by its very nature, can be devoid of this type of physical contact. A cybercriminal can use computer technology in such a way as to at least initially remove him/herself from direct contact with the victim. Consequently, personal cybercrime to some degree becomes a misnomer, so that these offenses could be almost described as "impersonal" personal crimes.

There are a wide variety of behaviors that could be classified as personal cybercrime, ranging from relatively minor vandalism-type offenses to more serious, threatening behavior. More specifically, there are a number of personal forms of cybercrime which have generated a good deal of attention:

● Cyberstalking: generally defined as the use of the internet, e-mail or other electronic communication devices to repeatedly harass or threaten an individual (Department of Justice, 1999). Some experts view cyberstalking as an extension of offline stalking – a preexisting problem exacerbated by technology (Ellison & Akdeniz, 1998).

● Online threat-related extortion: where an offender uses threats sent through e-mail in order to extort money from the victim.

● Disruption of services: where individuals are targeted for the disruption of computer-related telecommunication services through techniques such as mass spamming or the transmission of computer viruses.

● Online sexual predation: primarily situations where pedophiles and other sexual predators solicit underage children online, usually in chat rooms (see, for example, any of the cases featured on Dateline NBC's "To Catch a Predator" series).

The volume of personal cybercrime victimization is likely to increase in the coming years. As more and more people gain access to computers, and particularly to online forms of communication, they will find themselves at risk for being victimized by some form of personal cybercrime. The popularity of chat rooms, instant messaging and other online communication forms increase the likelihood of exposure to potential victimization by predatory individuals.

Economic and Property-related Cybercrime

Crimes against property usually involve situations where the victim suffers some type of economic loss or property damage. Economic loss can be something that is tangible, as with most situations classified as theft, or more abstract, as would be the case with the loss of productivity resulting from criminal activity. Property damage certainly involves an economic element but is usually related to the replacement or restoration of the damaged property.

With cybercrime, property-related offenses encompass many of the same types of behavior seen with more conventional types of crime but involve the use of computer technology to facilitate the offense, often in new and innovative ways:

● Phishing: "Phishing" is a general term for criminals' creation and use of e-mails and websites – designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords. The "phishers" then take that information and use it for criminal purposes, such as identity theft and fraud (Department of Justice, 2007).

● Identity Theft and Identity Fraud: Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain (Department of Justice, 2007a)

- Hacking: Hacking is a term used to describe situations where a secure computer system is breached and perhaps altered. The best analogy in conventional crime for hacking would be criminal trespass and vandalism.

- Cloned Websites: This usually involves the creation of a mirror version of an authorized website, where internet users are lured into the cloned website believing that they are entering the actual authorized website. Information obtained from the users (i.e., credit card information or personal identifiers) can then be used for fraudulent purposes.

- 419 Scams: The “419” in the name of this type of cybercrime refers to Section 419 of the Nigerian Criminal Code. This is a reworking of the classic “bait and hook” scheme where the e-mail recipient is lured into providing personal information such as bank account numbers with the promise that they will be given a share of millions of dollars if they help the sender move funds out of the country. The 419 scams typically depend on the greed of the e-mail recipient, although they sometimes also prey on the goodwill of the intended victim by framing their story around some catastrophic event (e.g., the source claims to have recently lost his/her parents, or alleges that they are dying of some disease). There numerous variations on this scam, with more recent examples seemingly originating from the United Kingdom.

- Hijacked Websites- This type of cybercrime involves situations where attempts to view a website (most commonly a popular webpage or a search engine) are redirected to an alternative website designated by the hijacker without the consent of the user. There are any number of motivations for this type of offense, most frequently those associated with hacking and computer-related fraud, but recent incidents include hijacking perpetrated for political retaliation, such as the case in 2007 where Chinese hackers hijacked several popular search engines and redirected them to Chinese websites after President Bush warmly welcomed the Dalai Lama to the United States.

All of these exploits noted above both continue to be descriptive of the nature of cybervictimizations today and will likely continue into the foreseeable future. The character of these victimizations may change, but the use and exploitation of individuals that utilize computing devices is a virtual certainty that law enforcement and the communities they serve will confront in the future.

References

Department of Justice. (2007a). *Identity theft and fraud.* Retrieved September 27, 2007, from http://www.usdoj.gov/criminal/fraud/websites/idtheft.html.

Department of Justice. (2007b). *Special report on “phishing.”* Retrieved September 27, 2007, from http://www.usdoj.gov/criminal/fraud/docs/phishing.pdf.

Department of Justice. (1999). Report on cyberstalking. Cyberstalking: A new challenge for law enforcement and industry. A report from the Attorney General to the Vice President. Retrieved September 27, 2007, from http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

Ellison, L., & Akdeniz, Y. (1998). Cyber-stalking: The regulation of harassment on the Internet. *Criminal Law Review, Special Edition: Crime, Criminal Justice and the Internet*, 29-48.

What Role and Responsibility Does the Government Have in Protecting Consumer's Rights to Privacy/Security on the Internet?

Andy Bringuel
Wayne Rich

Consumer privacy and Internet security are not mutually exclusive concepts, as it is often the consumer's privacy/security that is threatened by actions taken sometimes intentionally, sometimes not. The government has tried a couple of times to legislate Internet privacy with the Communications Decency Act of 1996, which was ruled unconstitutional by U.S. District Court Judge Dalzell who stated: ". . . the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects."

If Judge Dalzell is correct that the strength of the Internet is chaos, then the strongest users are those who understand how to exploit that chaos. If that is the position of government, that chaos is an acceptable state for the Internet, then it follows that the government should be responsible for at least warning those who venture into this chaotic environment. Those interested in regulating the Internet are aware that personal information, like medical records, credit card information, and information used by minors, can be easily used by unscrupulous marketers or identity thieves. These pieces of personal information are frequently protected only by a simple password which can be accessed by a clever cracker. New Internet users, particularly the old and young, are not able to give meaningful consent to the use of their personal information and are not aware of the consequences when they respond to requests for it on-line.

Ask most people if the government should be responsible for warning the public about possible threats to their privacy/security and they will give you a quick answer in the affirmative. The public expects warnings on all known and potential threats whether natural or man-made. Should the public expect the government to warn them about the threat posed on the Internet? Should the casual Internet user be warned that their identity can be easily stolen, or that they could be propositioned or taken advantage of by visiting certain websites, opening certain files, or answering certain emails, participating in drawings, etc? At what point does the government's responsibility end, and how effective are these warnings anyway?

The government does warn people not to break the law through public service announcements. We know through these messages not to drink and drive, to wear a seatbelt, and not to copy licensed materials for personal use or profit. Certainly, having the government warn us about possible threats to our personal privacy/security is not new. Perhaps the first warning from our fledgling government could be attributed to Paul Revere who warned colonists Samuel Adams and John Hancock that the British were on the march. In today's government there are the modern day equivalents of Paul Revere. These agencies, like the Department of Homeland Security, have a responsibility for issuing terrorist threat warnings through the color-coded terrorist warning system. There are other regulatory agencies warning the American public about a number of possible threats, including not to eat bagged spinach and the dangers of smoking. No doubt millions of taxpayer dollars are spent every year in developing, drafting, and disseminating these messages from Uncle Sam.

There are precedents for the government issuing warnings to the public on issues that the populace might be ignorant about or where there is a direct threat. In natural disasters, the government's ability to provide warnings has been greatly enhanced by technologies, the result being fewer fatalities. It is now an expected role of our government to warn its populations being threatened by hurricanes and impending severe storms. If the government fails in this area, agencies are severely criticized and politicians are voted out of office, as was seen in New Orleans after Hurricane Katrina. Tornado warnings also are issued by the government and disseminated through the public, as well as private, sources. In fact, it is good and "big business" for local and national T.V. stations, like the Weather Channel, to pass along weather related warnings to the public

Perhaps computer companies like Dell, Compaq, Gateway, and Hewlett Packard would be willing to bundle a government sponsored educational program on protecting personal privacy/security while online. They then could have the "bragging" rights for future marketing campaigns.

What about man-made threats? Historically, these warnings come well after the threat has become real and the victims or families of victims demand the government act more proactively. Groups like Mothers Against Drunk Drivers (MADD), who lobbied for stronger penalties against drunk drivers, also promoted a public awareness campaign warning people about the evils of driving while intoxicated (DWI). The direct result might have been an increase in DWI arrests, but the indirect result was more lives saved. Many special interest groups might not be as altruistic in their motives. The Motion Picture Industry of America (MPIA) is interested in protecting the profits of the motion picture industry and successfully lobbied for legislation mandating warnings labels that state copying protected materials is a felony punishable by fine and prison.

So an Internet Personal Security campaign that provides education and a warning to the public about the evils of blindly or ignorantly surfing the Internet might serve the interests of business as well as educating the general public. Companies like AOL and Comcast do provide their users some free software to help protect from unwanted materials found on the Internet, including filters to keep out pornography and blockers to keep away annoying pop-up ads, but should the government legislate that these companies and others do more?

There are really three areas where the government could require warnings regarding Internet dangers. Legislation could be passed requiring that all manufactures of computer equipment include a Personal Internet Security users learners' guide that would include warnings and an educational module before allowing the computer's web browser to operate. Could there be ways around this requirement? The new user could easily have an experienced user take the test to unlock the computer, or a program could be loaded that writes over the existing web browser.

Secondly, the government could also require that any software which allows access to the Internet to have a simple warning about the threat to personal privacy/security on the Internet. But what is a simple warning good for? How would a warning cover all the potential threats on the Internet? The U.S. tobacco industry started carrying warnings in 1965, and the government had a few different warnings. The liquor industry was required on November 18, 1989 to have a warning on all alcoholic beverages that reads:

> GOVERNMENT WARNING: (1) According to the Surgeon general, women should not drink alcoholic beverages during pregnancy because of the risk of birth defects. (2) Consumption of alcoholic beverages impairs your ability to drive a car or operate machinery, and may cause health problems.

Perhaps an Internet warning would read something like:

> GOVERNMENT WARNING: (1) According to the Attorney General, use of the Internet poses a substantial threat of personal identity theft, fraud, and unsolicited pornography. (2) The government encourages all users to access www.http://ilearn.isafe.org to take a Personal Internet Security educational training class before using the Internet.

Thirdly, the government could require or encourage all Internet-based Services (IBS) to comply with a certification system wherein users see a familiar logo or trademark indicating approved membership in trade organizations sensitive to consumer privacy/security issues (Liberto, 1998). The consumer would be educated to do business only with members of reputable trade organizations who display this seal of approval. It would be up to the IBS to earn the seal of approval by adopting and posting one of several security warnings.

So if there were warnings regarding security threats would they make any difference in terms of consumer's use? In the summer of 1993, four major television networks adopted a warning for televisions shows that read: "Due to some violent content, parental discretion advised." A survey (Stacy and MacKinnon, 2000) of high school students from a county in the Midwest measuring their exposure to, beliefs about, and memory for the TV advisory found the majority had seen the advisory. The students' awareness of and memory for the advisory increased over time. However, students' advisory-related beliefs and the amount of violence they watched on television remained unchanged.

So if that study holds any truth, then any government, private industry, or special interest group sponsored warning system must have security training to go along with the warning for it to be effective. A training module, like the ones offered by www.http://ilearn.isafe.org, should be imbedded in software or on a particular digital device.

References

Gerend, M.A., MacKinnon, D.P., & Nohre, L. (2000). Awareness and memory for television advisory warnings among high school students. *Journal of Applied Communication Research, 28*, 291-308.

Liberto S. M. (1998). *WWWiz magazine.* Retrieved September 23, 2006, from http://www.libertolaw.com/11-98.html.

The Not-So-Distant Average School Day

Mary O’Dea
Wayne Rich

Sixteen year-old Harris is beginning his school day in Buffalo, New York. He’s scheduled to meet with his art group this morning at 10:00 AM. His group consists of five students who are roughly the same age as Harris. They are lead by their instructor, Ms. Rodriguez, who is just finishing her early morning cup of coffee in Santa Fe. Harris enjoys the work he does for the course, and he’s looking forward to sharing his latest interactive video project with his group.

As Harris finishes his breakfast, he takes a seat at his laptop – the one his school provided – and boots it up. This morning he’ll meet his group in the classes’ assigned chat room, at the scheduled time. His teacher, of course, will be there, as will his classmates, even though they live scattered hundreds of miles apart. This school has no traditional walls other than those used for administrative purposes, yet it graduates hundreds of students each year and offers classes to other students who must fulfill their own schools’ graduation requirements. It is, of course, a completely paperless environment. All of the schools’ courses are taught this way, and the school is typical of the times.

As Harris logs on to his laptop, he must complete a series of steps to get onto the Internet and then into his classes’ chat room. Earlier this year, when he opened the new computer from his high school, he had to complete an Internet Safety course – which included getting a parent’s signature – before he could log on to the Internet. He was issued a certificate upon completion and the information from that completion had to be sent to his school before he was allowed to participate in classes. He will have to do this each time he begins a new class, or set of classes, with the school. If he wants to use a computer other than his own, it will be necessary that he use his certification information to use the Internet.

Several hours pass, and Harris finishes his time with his classmates. He’ll head downtown now for his business class. He’s interning at a local shop, earning credit for school while he’s learning basic accounting and business skills. He’ll log his intern hours every day with the school, via the Internet, and weekly his supervisor will communicate with his instructor in Birmingham to make sure Harris is gaining the necessary skills. Every two weeks, Harris will take an online test as part of his class requirements. Once again, before logging onto his school account, he’ll need to supply the necessary certificate information before he will be allowed to go online.

Harris’ week continues in the same vein. He won’t set foot in the type of classroom our generation is accustomed to. At times, his classes may meet at odd hours in order to accommodate schedules and classes offered around the world. Internet and varied communications technologies will be necessary for any child to complete a school education. Harris’ elementary-aged sister spends several hours a day at the “school” provided by her mother’s business as her mother works.

Basically, this is a gathering of elementary-aged children, too young to be unsupervised, who will accomplish work at the facility just as Harris did at home. These children, too, will have taken an age-appropriate Internet safety certification course prior to getting online to do school work. Much of the youngsters' work will be completed from home, as their parents and older siblings will spend much of their time working from home as well.

While this scenario is certainly only one of many possibilities, it provides modest insight into the realization that technology will play an ever-increasing role in our children's lives as in their educations. As we continue to increase the use of technology in our lives, and our children's lives, we must increase our awareness and preparation for the increasing threats posed to our children by criminals familiar with the cyber world.

> *"The more that we use the Internet, the more likely we are to forget to do the things necessary to keep our data, ourselves, and our family safe online. It is this* complacency *that we must struggle with every time we sign online."*
> *(www.Secureflorida.com).*

A Double Edged Sword: Technology and School Children

There is little doubt that in the near and far-term future, technology will be increasingly available to children of all ages. Clearly the availability of technology to our youngsters is a boon to learning, education, and open communications. For obvious reasons, though, it creates the possibility of an ever increasing threat to the personal security of anyone naïve to the methods of cyber criminals. It stands to reason that as the use and availability of technology increases, a logical way to begin to ensure awareness is through our schools. It's an old, but true, premise that the best place to begin social awareness is with our children. As we teach our children – and their parents – about safety on the internet, for example, we begin a cycle of awareness that perpetuates through the ages.

In both traditional and non-traditional constructs of schools, technology will increasingly be used as an educational tool in the foreseeable future. In one example, in a first of its kind program, the state of Maine has partnered with Apple Computers in order to supply all of the states' seventh and eight grade public school students with laptops. Virginia is following suit with negotiations for computers from Apple and Dell, and Philadelphia partnered with Microsoft to open its School of the Future: a no-paper, no-textbook, high-tech high school. Maine's program, now in its second year, is working well, and is a success for the state and the students. The laptops are wonderful educational devices, but experience also tells us that putting laptops into the hands of school-aged children, or anyone unaware of personal security safety problems, can be a dangerous prospect.

The answer, of course, is not to stem the flow of technology to our children but to work to protect them. It's imperative that we arm our children

– and their parents – with the ability to protect themselves against cyber crime. With laptops and PC's in the hands of, or at least available to, nearly every child in the U.S. right now, internet security is an ever increasing issue that schools, counties, and governments will become progressively more involved with.

Awareness is the most important aspect of ensuring safety for our children and their children. Society is in a state of technological transition. As adults and parents, how many of us recall pre-computer and pre-ATM days? While many of us utilize computers on a daily basis, how many of us are fully aware of the techniques needed to protect ourselves, let alone our children? We may be continuously bombarded with virus warnings on our computers, and we may witness cyber stalkers being arrested on our televisions, but are we actively doing enough to protect our youngsters and to teach them how to protect their own children when the time comes? How many of us don't keep up – or are even aware of – parental blocks we can use to protect our kids? How often do our children go unsupervised in front of a computer screen?

As in many other educational domains, the most evident place to begin helping our children to protect themselves against cyber crime is in the schools. It also follows that because cyber crime is a criminal act, some of our strongest lines of defenses against it are our police departments and law enforcement agencies.

Right now, school districts and counties across the country are encouraging students and parents to practice cyber safety. They're offering classes and websites to help people learn how to take care of themselves and children in the cyber realm. This is the first step in protecting and teaching our children and ourselves. The FBI and the Office of Juvenile Justice and Delinquency Prevention (through the Internet Crimes Against ChildrenTask Force) both offer very insightful and informative information via their websites regarding internet crimes against children, how to prevent them, statistics regarding the crimes, and state and local offices.

While no one can deny these, and many more across the country, are powerful weapons against cyber crime, encouraging education may not be enough. After all, many parents who are concerned for their children's safety are already aware of how to protect their children, or they are likely to find out by voluntarily attending school or local seminars regarding the subject. It is those children and their parents who are unaware of the need to take precautions or how to take those precautions who are most vulnerable. These are the people who we most need to target. Perhaps, then, it is a wise choice to mandate cyber safety education whenever possible.

Maine Is Doing It

In Maine's prototype program, during the first years, the state brought laptops into public middle school classrooms (2002-2006). Schools were encouraged to implement Internet safety programs, but they were not required to do so. The lack of a mandate was more a reflection of the political climate at the start of the project than of a value statement about Internet safety.

Last year, the Attorney General's Office and the Department of Education teamed up with NetSmartz.org, a well-known Internet safety group. Since then, “as part of the participation agreement, [the state] mandated that schools implement an Internet Safety program, [and they] continue to work with the AG’s office and with NetSmartz” says Jeff Mao of the Maine Department of Education.

If Maine serves as precedent, we should be working to mandate Internet safety programs in our schools. This is easy enough to do, as Maine did, as part of a participation program, and parents can be brought into this fold. If not as a requirement for participation, then local, state and/or federal authorities can mandate this education as curriculum required to maintain accreditation or funding.   Requiring students and parents to complete at least a basic awareness program (which could be done online, at local libraries, etc) will assure that we educate more students than on a voluntary basis. Additionally, this requirement need not be tied to only those schools supplying students with their own computers. Since schools are sometimes the main source of computer exposure for some students, it is a natural place to require safety training prior to allowing computer use.

The Role of Police Departments

Since 1983, the D.A.R.E. (Drug Abuse Resistance Education) program has worked to give “kids the skills they need to avoid involvement in drugs, gangs, and violence.” (www.dare.com). Why not use this program as a model for educating children about Internet safety? Training police officers to help children become aware of and avoid Internet safety problems seems an obvious place to begin, and it promotes interaction between police and children at the same time it helps prevent terrible kinds of crimes. The D.A.R.E. program is widely accepted as having very positive results with school children. As a well established program, we suggest either adding cyber crime to the D.A.R.E. program curricula or building a similar program for cyber crime. Another advantage of “merging” with the D.A.R.E. program is the long list of supporters and sponsors that help to finance the ongoing project, making cyber crime education more affordable, thus more readily available, to a variety of clients. Ideally, programs such as D.A.R.E. will be coupled with consistent, recurrent programs within schools to ensure that students of all ages, abilities, and backgrounds are provided the tools necessary to protect themselves against a variety of cyber criminals.

Although there is no way to guarantee the prevention of cyber crime, there is much hope in raising awareness. As today’s children mature, our society will become more attentive to the hazards of cyber crime as well as the skills needed to help prevent it. Today, our job must be to immediately educate people of all ages about potential dangers to cyber space users. We must remember that technology changes “faster than the speed of light,” and the future may hold even more pitfalls for the next generations in the cyber world. Still, with any luck, education today will sustain our children through adulthood, and they will have the ability to protect the children of the future.

Related Websites

http://bob.nap.edu/html/youth_internet/
www.dare.com
http://www.fbi.gov/publications/pguide/pguidee.htm
http://www.globalgateway.org.uk/Default.aspx?page=390
http://www.hackerhighschool.org/
http://www.icactraining.org/default.htm
http://www.lhric.org/security/desk/letter7.html
http://www.isecom.org/
http://www.netsmartz.org
http://www.npr.org/templates/story/story.php?storyId=6210622
http://www.secureflorida.org/
http://www.state.me.us/mlte/
http://www.whitehouse.gov/news/releases/2002/10/20021023.html
http://www.whitehouse.gov/news/releases/2002/12/20021204-1.html
http://www.whsv.com/news/headlines/4308577.html

College-Level Education for Cyber Security

Jay Corzine

Colleges and universities provide an additional venue for the delivery of educational programs to enhance both individual and institutional levels of cyber security for a large cross-section of the younger population. A significant percentage of graduating high schools seniors enter a college or university within 4 years of completing high school. Besides the provision of a useful service for their student populations, colleges and universities have an enlightened self-interest in enhancing the cyber security literacy of their undergraduate students. The contemporary university is “wired” and highly dependent on the operation of complex computer networks for teaching, research, and management functions. Each fall semester, dependent on its size, a college admits several hundred to several thousand first-year students who will almost immediately be granted access to university email accounts and online systems for browsing library holdings, monitoring student records, completing course assignments, and so on. Similarly, higher education must take steps to limit the incidence of illegal downloads by students. Simply stated, it is in the best interest of the colleges and universities to provide mandatory education that will decrease the risk of students infecting computer systems with viruses, worms, and spyware. Programs that impart knowledge designed to protect the university’s networks can also be used to convey information that will lower students’ risk of identity theft and other cybercrimes that target individuals.

Although education to increase individuals’ cyber security is necessary for students in the K-12 system, there is an important added risk for becoming a cybercrime victim when individuals become legal adults at the age of 18, namely the credit card. . The stuffing of mail boxes with credit card offers coincides with the entry of traditional-age college students into institutions of higher education and is widely supported by colleges and universities through their selling of student lists to companies hawking credit card companies as well as a laundry list of others products and services. In fact, some universities sell the excusive right for a credit card company to distribute application forms on their campuses. The possession of one or more credit cards increases the risk of being a victim of frauds perpetrated through computers, and it can be argued that colleges and universities who facilitate their acquisition by student have a moral obligation to provide education to reduce the risk. One innovative approach would be for institutions of higher education to require credit card companies to provide cyber-security education, perhaps in an online format, to students prior to the issuing of a credit card or forego access to student lists.

Cyber security for incoming first-year students can easily be introduced through the new student orientations that are increasingly required by most large state universities prior to enrollment for courses. Typically one-to-two day events structured to introduce the student to the campus and complete bureaucratic paper work, most colleges and universities have sufficient flexibility in orientation schedules to require attendance at a 30 minute segment on cyber security. Although some time can be devoted to reinforcing strategies to protect against viruses and worms, precautions that were hopefully part of students' K-12 education, attention should also be focused on identity theft, including phishing and pharming. The information can be provided through lecture and/or videotape format with some provision for a Q&A period. In fact, some universities have moved in this direction. Many colleges now include short 15 – 20 video presentations on cyber security often produced by its computer security technology departments as part of its orientation sessions for new students. Including cyber security as a topic in student orientations has the advantage of reaching all incoming students before they have access to university computer systems.

An alternative to including cyber-security education as part of orientation would be to require the completion of a training program before allowing students to obtain a university computer account. This would allow for a more comprehensive package of information that could be delivered in an online format and would be a reasonable alternative for colleges and schools that do not require students to complete an orientation program. An additional advantage is that a sequence of training programs could be developed with the specific requirements tied to the type of accounts desired by a student. In order for information on individual cyber security to be widely disseminated, there would have to be an introductory-level training module required for all students, however. The completion of the base module could be tied to the issuance of a student ID.

To attain a higher level of national cyber security, it is vital that higher education closely examine the content of introductory courses in computer science programs. Presently, these courses rarely include material relevant to cyber security. Although not all students take these courses, they are increasingly a mandatory or elective requirement for general education programs and enroll a significant percentage of undergraduates in many colleges and universities. They would provide a forum for more detailed readings and discussion focused on cyber security, and it is reasonable to expect that in schools where they are elective, these courses enroll those students who are likely to both have a greater interest in and to make more use of computers. These courses would be a logical place to cover precautions directly tied to network security, a growing concern for all organizations, including colleges and universities.

Of course, there are two primary limitations to an over reliance on colleges and universities to provide education about cybercrime and cyber security. First, not all people attend institutions of higher education. Second, and perhaps more importantly, the risk of victimization from some types of cybercrime, e.g., cyber stalking, occurs prior to high school graduation. But colleges and universities can provide an important part of a comprehensive, national educational program designed to reduce cybercrime victimization.

Seniors and Cyber Space

Wayne Rich

We have talked about education with regards to children and young adults, but one of the largest populations in our society with a growing number of Internet users is our senior population.

More and more seniors are entering the world of cyber space, drawn to it for various reasons. Some enter the cyber space world as a form of additional entertainment. Having retired from the day-to-day work force allows many retirees large blocks of time to dedicate to surfing the web. Keeping in touch with friends and loved ones via email is a chief reason many retirees become connected to the web, their first computers probably being provided by their grown children.

Seniors don’t just use the Internet for keeping in touch, though. We find seniors shopping on the web for everything from personnel items to recreational items, clothing, furnishings, and even groceries, all of which require them to use a credit card to complete a purchase. Using the credit card is where the trouble begins!

While many of our seniors have the means, time, and capability to become cyberspacers, they have not inherently been nurtured regarding the pitfalls of cyber space, with the years of hands on experience, systematic awareness training, and learning from mistakes that has become common among the younger generations

Seniors are no strangers to credit card fraud, identity theft, and scams traditionally committed by unscrupulous individuals contacting them via telephone and through elaborate schemes obtaining their credit card and personnel information. These days, though, con men and scammers are using similar and even more sophisticated tactics via the Internet.

For example, the Centers for Medicare & Medicaid Services (CMS) is warning Medicare recipients to be wary of schemes being played off the new Medicare prescription drug program. In one scheme, people shopping for a Medicare prescription drug plan are asked to withdraw money from their checking account to pay for a plan that does not exist. A more recent scam involves a new Medicare card instead of a prescription drug plan. As part of the new scams, callers are now asking for bank information or telling beneficiaries they can provide a new Medicare card for a fee. The new Medicare card or prescription drug plan they claim to be selling is not legitimate. Scammers may use the name of a fictitious company such as Pharma Corp., National Medical Office, Medicare National Office, and National Medicare. However, it is against Medicare's rules to telephone and ask for a bank account number, other personal information, or a cash payment over the telephone. No beneficiary should ever provide that kind of information to someone who calls.

It is easy to see how this scam, traditionally accomplished over the telephone, is being adapted by scammers who use the Internet. Once a scammer, or “phisher” gets hold of a senior’s email address, he can make an email look even more official than a telephone call sounds. Bank account numbers, personal information, and money transactions then get handed over to cyber criminals by innocent elders who believe they are looking out for their own health.

An Internet Personal Security campaign tailored specifically for seniors which provides education and warns about connecting to the web should be included when designing any personal awareness program. Additionally, legislation passing a requirement that all manufactures of computer equipment include a Personal Internet Security users learners' guide that includes warnings and an educational module would be a good start. These modules would need to be concluded before allowing the computer's web browser to operate. The government must require that any software which allows access to the Internet have a simple warning about the threat to personal privacy/security on the Internet along with the requirement that all Internet-based Services (IBS) comply with a certification system wherein users see a familiar logo or trademark indicating approved membership in trade organizations sensitive to consumer privacy/security issues.

The D.A.R.E. program, which is widely accepted as having very positive results with school children, could easily be modified to address seniors, since the basic learning curve for both age groups on cyber crime is very similar.

Protecting and Strengthening Societies[22]

Jeff Frazier

Before their arrests for the “Beltway sniper” attacks, which occurred in the mid-Atlantic United States in 2002, the license plate of the car driven by John Allen Muhammad and Lee Boyd Malvo was, in the space of a month, spotted and queried by different U.S. police organizations on 13 separate occasions. But the individual officers running checks on the car had no idea that other police agencies also were on the lookout for the snipers.

If technology had been used to gather information from other jurisdictional sources, that information would have revealed more details, such as the number of license plate queries made by other police agencies. Knowing this may have expedited the search.

Using technology in this way would also have benefited police in the 2004 Madrid train bombings. The primary suspect, Jamal Zougam, had been tracked and followed by five different crime and intelligence agencies since 2001. He was finally detained two days after the attack.

In both examples, the agencies’ access to information stopped in line with their jurisdictional boundaries. Information did not become knowledge because it was not shared across those lines.

Government is moving into the information age but not fast enough. Effective government is faced with a 21st-century governance paradox—minimizing the complexity of administrative protocols to determine who is responsible for what. How, to whom, when, and where information is available can fundamentally influence the success or failure of public institutions charged with safeguarding communities. The need to reconfigure how information is created and disseminated is critical in the face of a whole new world of threat. This need is what Sir Ian Blair, London’s metropolitan police commissioner, refers to as the “new normality,” which describes the tremendous rise in nonroutine problems, such as terrorism and non-natural disasters, that threaten every society.

Senator Richard Shelby, former vice chairman of the U.S. Senate Select Committee on Intelligence, made a similar argument in his investigative report on the September 11 terrorist attacks. Shelby pointed out that all the missed, or misinterpreted, signals (information) that led up to the attack were not shared among the CIA, FBI, or the National Security Council. The information was there, but U.S. intelligence agencies were unable to “connect the dots” of information, as Shelby put it, to possibly intercept the attacks.

Traditional Approaches

A number of social scientists and public safety experts have conducted experiments and research to understand

[22] Jeff Frazier did not attend the FWG conference but provided this entry after the conclusion of the conference. His contribution was accepted due to his affiliation with FWG group members. Mr. Frazier works for CISCO Systems, Inc. and this entry reflects only Mr. Frazier’s viewpoints and not necessarily those of CISCO Systems, Inc.

how threats against societies begin and escalate. In 1982, James Wilson, Ronald Reagan professor of public policy at Pepperdine University in California and a former chairman of the White House Task Force on Crime, and George Kelling, an adjunct fellow at the Manhattan Institute for Policy Research, developed the "Broken Windows" thesis, which acknowledges the connection between disorder, fear, crime, and urban decay that have plagued communities for decades. The theory behind the thesis is that if you leave a window broken, it will invite more crime.

The Broken Windows thesis was the inspiration for the cleanup of the New York City subway system in the late 1980s and early 1990s. Removing graffiti and cracking down on the people who leaped over turnstiles without paying would solve two "trivial" problems that were thought to encourage more serious crimes. Not only did this strategy work (since 1990, felonies have fallen more than 50 percent), but one of its architects, Chief of Transit Police William Bratton, would later take his ideas about preventing crime to the city when he became commissioner of the New York City Police Department (Bratton is currently chief of the Los Angeles Police Department).

In Bratton's approach to connecting the dots, he used a system called CompStat,[23] which was influenced by Broken Windows. CompStat (short for COMParative STATistics) organizes computer statistics in a particular way to predict and combat crime in communities. This approach is used today by many public safety agencies; it is limited to a community, however, and by the usefulness of the organization and its capacity to share knowledge with other organizations. But what if the problem is larger than a community? What if the problem exists within a region or country?

Nature of Sovereignties

Because the dangers we face today mutate from one place and source to another, the prevalent approach is to address each threat discretely with a separate agency. But the resources available to each agency are finite and subject to increasing demands and competition. Our inability to piece together information hints at the problem of governance—that is, the attitude of government officials/agencies that if the problem is not in their community, it is not their problem.

Although technology can provide a basis for improved interaction among governments and increased citizen engagement, getting it to work in practice depends first on adopting a new mind-set. This can be a challenging prospect for agencies hampered by poor management, siloed cultures, and inadequate communication. Old hierarchies and control structures are not flexible enough to predict and respond to threats quickly. These inherent behaviors prevent agencies from operating effectively in the new, information-rich environment.

Organizations need to change and work with new, emerging models that demonstrate the power of connectivity to turn information into intelligence and make it available where, when, and for whom it is needed.

[23] www.gladwell.com/2003/2003_03_10_a_dots.html .

Organizations must also understand how collaboration can traverse traditional boundaries and develop levers for action—both technological and organizational—that will accelerate progress in protecting communities.

Of course, making information available (capturing and sharing what we know) to the right people at the right time is the fundamental basis for strengthening our communities. But the constantly changing nature of threats posed by a multitude of different criminal, terrorist, and natural catastrophes increasingly means that traditional approaches to information gathering and communication are no longer effective. This is especially true when dealing with criminality and terrorism, which operate across borders and through loose coalitions of networked cells and individuals. Hierarchies and control structures have mutated into much looser and disparate matrices and networks. Effective 21st-century government requires a new approach to "connecting the dots" by coordinating activities across traditional jurisdictional boundaries.

A Shift in Thinking: Power at the Periphery

All information is quickly becoming digital. Take e-commerce, for example; 90 percent of online communications involve connections—connecting people to businesses, businesses to machines, and machines to machines. But, these connections are not enough. It is critical to connect information to people and organizations at the "edge"—those people who are closest to and may have answers to a given problem or risk, such as the policemen in the examples above. The more we connect the right information to the right people at the right time, the smarter we are about anticipating risks, solving problems, and ensuring public safeguards. In other words, it is the "wisdom of the crowd" that has the power to resolve problems and effect change.

The wisdom-of-the-crowd mentality is true not only for human networking but also for computer communications networks—those that allow several hundred major communications stations to talk to one another, especially prior to and after an enemy attack or natural disaster. Without an increase in the size of agencies or their budgets, it becomes a challenge to transform thinking about strengthening our communities and improving our public safety and security.

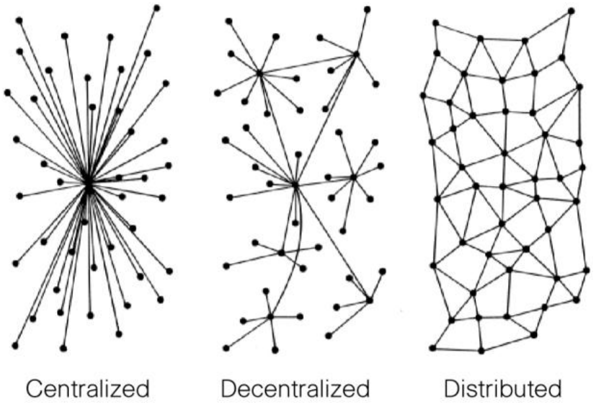
Distributing the Power

Social scientists and public safety researchers are taking a new look at this age-old problem. With the evolution of increasingly intelligent networking and developments in next-generation Internet technologies (including Web 2.0), the model for effective public safety and security must shift from centralized, command-and-control networks to shared, relational systems in a distributed framework that comprises "small pieces loosely joined."

This distributed framework was created by Paul Baran, who developed packet-switched networks to provide a communications solution that would withstand a nuclear attack. While this approach was important to the defense strategy of the United States, it later developed into what is known today as the Internet. Baran's theory of connecting the dots in a distributed, horizontal way is the basis for connecting communities, governments, and public safety agencies as never before.

Although there are a wide variety of network configurations, all can be categorized as centralized (star), decentralized (starbursts), or distributed (grid or mesh), as shown in Figure 1.

Figure 1. Network Configurations



Source: Paul Baran, "On Distributed Communications Series," Introduction to Distributed Communications Networks (chapter 1),
RAND Corporation, 1964

Unlike centralized and decentralized networks, which are loosely sewn together and open to attacks, distributed networks are strong, tightly sewn, self-supporting infrastructures that enable better collaboration. The value of a distributed environment is that the network learns faster and gathers more intelligence and information than any individual or organization and shares information with other networks. A distributed network then pushes knowledge to the periphery, or the edge, so that people closest to the problem have the best information to solve the problem. This approach is more resilient and effective than any other.

This new way of thinking seems ideal, but how do we achieve it? We do so by establishing a policy agenda that focuses more on problems than on organizational structure, which is imperative for a knowledge-based organization. Creating such a policy can be achieved easily through Net Learning, an organizational process through which people seek affinity and collateral relationships and then exercise their influence to share information. Adopting this approach allows organizations to recognize the dangers of overclassifying and compartmentalizing knowledge.

The Right Platform

Before we can create the right distributed communications platform, we must answer two questions: How can we create open standards that allow communities to collaborate? How can we address the growing need for nonhierarchical solutions?

Rather than focusing on specific problems in isolation, looking at them in a distributed manner creates a single, flexible platform that can respond and adapt to a multitude of problems. The basis for this approach is the network or, more specifically, a distributed network that achieves resilience and flexibility by maximizing the ability of agencies and citizens to interact, collaborate, learn, and share information directly with one another. In other words, we need to capture what we know, or don’t know; analyze what we know; share what we know; and improve what we know to increase our knowledge about a problem so that we can solve it.

Agencies have vastly improved their ability to gather and use information. The next stage is to pool together all information so that separate pockets of knowledge are connected, rapidly increasing the amount of intelligence that security services can address during a threat.

This approach is starting to emerge in projects such as Intellipedia, established by the Office of the Director of National Intelligence in the United States, using the same technology that powers the online encyclopedia Wikipedia. Intellipedia allows authorized users from 16 government intelligence agencies in the United States to contribute, review, and edit security-related information and build resources and analysis relevant to particular threats. To date, more than 3,600 analysts have contributed more than 28,000 pages. Although there is no public access to the three “wikis” (collaborative software) Intellipedia comprises, it is easy to see how this framework could be adapted to link a wide range of official and public users and sources to build a new and powerful intelligence community.

Additional advances in IP (Internet Protocol) technology mean that investments in older (analog) communications equipment for voice, video, and data can be converted into digital assets that use an existing platform based on Internet technology. These advances are critical for leaders who access investments in this area. It has only now become both technically and economically feasible to implement a common platform approach without writing off past investments in communication systems and equipment.

Advances in IP enable the ability to learn and turn knowledge into quick, decisive, and intelligent action, and are at the heart of successful organizations, systems, and societies. Public safety is no exception. A networked organization gathers and uses information much faster than a non-networked organization, and in the world of crisis management and homeland security, seconds count and can make the difference between success and failure. Taking a distributed network approach gives each organization infinite opportunities to define and implement new capabilities. These include the ability to detect and analyze relevant information where and when it is needed, share voice/radio communications efficiently, and improve response to crises as well as management of day-to-day operations.

It is important, too, that this approach focus on how information is organized and distributed rather than on how it is acquired. An enormous amount of information already exists within and flows through political and civil organizations. The challenge, therefore, lies in the ability to manage, coordinate, control, and communicate information already available. A distributed network platform provides great value in connecting the following elements:

- **Right information.** Major decisions about which information is “right” often compromise local needs and knowledge. Too much information is as bad as too little. The distributed network's ability to empower people at the edge of the network to gather the information they need in a standardized environment is critical and goes a long way toward avoiding the trap of centralizing knowledge.

- **Right place, right person.** Only authorized individuals should have certain privileges for access to information and responsibilities for command-and-control operations.
- **Right time.** As a situation changes, the network platform provides the capability to self-synchronize and provide information instantaneously.

Resolving the Paradox

A distributed environment using Internet technologies provides remarkable, new opportunities for government and citizen interaction and involvement. It also creates a paradox: the actions of citizens and, regretfully, of our adversaries are moving faster than the governments' abilities to keep up. Technology alone won't solve this challenge. It takes cooperation among governments, stakeholders, agencies, and others. Knowledge and the power to act, therefore, must move to the edge of the organization, away from centralized control.

It is also vital to have a coordinated plan and to forge agreements with all stakeholders at national, state, and local levels. Articulating this principle is one thing; putting it into practice is another. It is increasingly clear that barriers must be overcome to connect pockets of knowledge and achieve the flexibility and breadth required to strengthen our communities. Protecting public safeguards and ensuring public trust are issues much larger than any individual or organization. Using a distributed network platform for collaboration and cooperating in tandem creates a net effect—the wisdom of the crowd. A network, if empowered by the right people at the periphery, is far more effective at anticipating and solving problems than a single source. Essentially, the sum of a number of people is infinitely smarter than a single person. Now that we have a roadmap, it is time to take action.

Partnering With Others To Address Cybercrime

Gerald Konkler

As should be evident from the other chapters in this volume, cybercrime is a present and increasing concern for policing and society. With existing levels of personnel, expertise, and equipment, most agencies are hard-pressed to address even the current incidence level of these crimes. Most police agencies do not have the resources to effectively or efficiently detect, prevent, or investigate many technology-related crimes, particularly cybercrime. This paper will suggest some strategies for local police to more effectively address cybercrime in the future by identifying and utilizing resources both without and outside their agency.

Some assumptions:

- → The use of computers in criminal activity will continue to increase.
- → Local agencies are behind the curve in addressing cybercrime and computer related crime.
- → Local agencies will continue to investigate cybercrimes at least to the degree they are capable (i.e., we will not totally abdicate our responsibilities to citizens and will attempt to respond in some manner to these types of calls for service).

The policing industry has historically resisted involving outside entities in policing efforts. Coupled with the sluggish nature exhibited by the police in adapting to change and embracing technology (or at least, resistance to technology that does not directly relate to catching criminal offenders), and there is little wonder there is much room for improvement in how policing responds to cybercrime and computer related crime. It has been said that every crisis brings opportunity. Policing has an opportunity to partner with others and improve services to the community.

For decades, community policing has pushed us toward involving others in policing efforts. In some cases, to varying degrees, we have at least given lip service to the value of the expertise and opinions of others. In order to effectively and efficiently address computer-related crime, policing must become more willing to involve others by utilizing their expertise while still protecting the rights of those accused and adhering to the vision, mission, and values of the agency.

An initial question might be whether an agency needs a specialized unit or section devoted to investigating cybercrimes. While this is a decision driven by agency size, local politics, and resources, it seems axiomatic that citizens who need to report a crime will at least start with their local police agency. If an agency opts not to create a special unit/section/position, at the very least it will need to identify resources or agencies to whom the agency can refer those who report cybercrime.

At a conference held by the FBI in July 2000, it was forecast that more police departments, even smaller agencies, would have personnel trained in the investigation of computer crimes

(Futuristics, 2000)[24]. While this has likely occurred, one could question whether the levels of training are sufficient. Are agencies simply using decoys to troll for online predators? As laudable and necessary as this may be, it does not require the level of training that is necessary to address cyber scams committed by organized crime syndicates or sophisticated denial of service attacks or to do forensic examinations of computers to search for evidence.

This then leads to another question to be answered by the agency: what level of expertise should be (or can be) identified or developed internally? Does the agency have the ability to investigate "cybercrime," i.e., where a computer is used to attack another computer or network? The investigation of denial of service attacks would be an example and, as noted, would require a high level of expertise. Or should the agency concentrate on "computer related crime," those instances where the computer is used to store evidence of a crime or used as a communication tool to commit a more traditional crime? Examples of this type include fraud schemes, child pornography, and online sexual predators. Does the agency have the expertise to conduct forensic examinations of computer systems? Obviously the effective and efficient investigation of either of the types of crimes will hinge on the ability to do so. These are questions that the agency head should consider before the need arises.

Whether an agency has a unit or elects to create a section, it is imperative that they be aware of what expertise currently exists in the agency. Without a doubt, police have more technologically savvy personnel now than in the past (as does society—and as does the criminal element!). Smaller agencies perhaps will already be aware if they have someone already employed who has computer expertise and/or a technical background. Larger agencies may have personnel who possess needed skills or at least a level of skill which the agency can enhance to meet their needs. Some agencies may have self-taught personnel who have some expertise in computers. Unless the agency has a personnel management system that identifies those with various skills/talents, an agency-wide survey of talents should be considered. Because of their interest in the subject matter, these personnel may have contacts with others in the field, either practical or academic. These contacts can be beneficial in establishing partnerships.

Even if skilled personnel are available internally, levels of expertise vary and may not be sufficient for the more complex investigations. To effectively deal with the variety of cybercrimes, an agency needs to have access to forensic computing experts and equipment and experts in tracking other types of cybercrime. Hence, there is still a need for partnerships. There

[24] In addition to identifying the trend, the Conference also suggested strategies. Two strategies are noteworthy and pertinent to the topic. First, the Conference stated one of the highest strategies for the future of policing was for agencies to develop tools and expertise in the investigation of cybercrimes. Second, it was suggested that agencies form partnerships with academic institutions (in a variety of disciplines) to educate and train personnel in emerging technologies which impact the policing profession.

have been well-publicized incidents where agencies with limited expertise and/or equipment have attempted to examine computers and allegedly overlooked critical evidence (Ellis, 2004).[25]

Whatever the level of involvement in cyber investigations, an agency is obligated to collect evidence in a lawful and competent manner. Evidence of traditional crimes as well as cybercrimes is frequently found on computers. Officers who are involved in virtually any investigation could face the risk of destroying evidence by either illegally seizing it or causing it to be physically destroyed because of traps laid by the suspect. Agencies that are accredited through CALEA are required to have a written directive that establishes procedures for the seizure of computer equipment and other electronic data storage devices. Improper recovery can result in the loss of data (Standards, 83.2.5, 2006). If an agency does not possess a level of expertise, local resources, private or public, must be identified.

STINGS

Apprehending online predators is an area where policing has received assistance from other entities. Perverted Justice is a private group that was started with a goal of cleaning up internet chat rooms. It has evolved to what they call a lead internet resource for combating sexual predators online. This group uses volunteers posing as children to go into chat rooms and wait for sexual predators to initiate conversations with them. As viewers of NBC's Dateline are aware, these contacts can evolve into actual attempts by the predators to meet their target and arrests of these predators (Perverted Justice, 2006). Initially, the television show did not involve law enforcement and simply broadcast Chris Hansen's interview with the offender in a sort of 'public shaming' reminiscent of medieval stocks. Because of viewer complaints/comments about letting the potential pedophiles escape punishment, police were involved and began arresting suspects as they left the house used in the sting. (McCollum, 2007). This resulted in an alliance between NBC, Perverted Justice, and various local police agencies that opted to assist in these televised stings.

It could be argued that there has

[25] For example, see "Mom's sleuthing helped find missing daughter," by Ellis above. In that case a 14 year old female was reported missing. The Sheriff's Office was criticized for treating the case as a runaway rather than an Internet related abduction and for failing to conduct a forensic examination of the girl's computer even though it was believed she was with someone she'd met online. The mother checked websites the girl had visited and ultimately contacted Perverted Justice. The director of Perverted Justice expressed shock that a forensic examination of the girl's computer had not been conducted. Perverted Justice contacted the Internet provider who would only provide information to the law enforcement agency. At the urging of Perverted Justice, the investigator contacted the Internet provider and discovered the name of the suspect. It was discovered that the girl had been kidnapped by someone she had met when she posted her poetry online. The suspect was charged with kidnapping, rape of a child, and sexual exploitation of a minor. The investigator noted that they had difficulty examining the girl's computer because the County's firewalls blocked many of the sites the girl visited.

been a blurring of the line between television news and ‘show business.’ Now, the lines between show business, law enforcement, and policing have become muddied. To long time observers of the police industry, it could be said that this blurring started with other police reality shows such as COPS. It seems clear, at least in some instances, that officers behave differently when on camera. While this sometimes might result in more restrained behavior of the part of both the police and citizens, it can also result in behavior that veteran police officers see as ‘pure and simple TV’ but tactically flawed (Dittrich, 2007).[26]

Partnerships of this nature can result in unique problems and criticisms for the police agency that becomes involved in these shows. A variety of allegations have surfaced after one of the show’s targets killed himself. A 56 year-old long time county prosecutor, Louis Conradt, Jr., is alleged to have communicated with a Perverted Justice decoy posing as 13 year-old boy in a Murphy Texas sting. These communications were sexually explicit and under Texas law constituted a felony even though Conradt never went to the target house. Warrants were obtained, and after police forcibly entered Conradt’s residence, he shot himself in the head and died. Resulting criticisms of the operation include allegations that the investigation was botched (the search warrant had the wrong date and county for service), that sexual predators were actually drawn to the community by the sting, and that the arrest was rushed in order to allow NBC to get the arrest on tape (McCollum, 2007). It is noteworthy that local prosecutors originally declined to assist with the show, saying they were not involved in ‘show business.’ Even more interesting is the fact that charges on the twenty-three men arrested during the sting were not pursued when the district attorney ultimately found that “the Murphy Police Department was merely a player in the show and had no real law enforcement position. Other people are doing the work, and the police are just there like potted plants, to make the scenery” (Dittrich, 2007).

Police agencies should explore the motivation behind those with whom they partner and should carefully check the background of those who assist them. If, as in the case of Perverted Justice, they are being paid for their participation, careful thought should be given to how that will impact the legality of any arrests and the public perception. Prior to engaging in operations with others, the agencies should liaison with appropriate prosecuting authorities and heed their advice and warnings. To do otherwise invites failure and second

[26] In the Murphy, Texas Dateline sting, a veteran SWAT officer who was working off duty to provide security at the undercover house observed questionable tactics in the takedowns of the suspects, particularly the drawn guns and potential cross-fire situations and intensity of the takedowns. The article notes: “All that business—the guns, the tackling, the shouting—struck Detective Patterson as pure and simple TV: It might look good on camera, but if you’re letting a camera influence how you do your takedowns, you’ve got a problem.”

guessing. An operations plan should be prepared detailing the duties and responsibilities of all parties. During operations the CEO must ensure constant supervision to avoid the tendency to take shortcuts. Periodic updates should be required and an after action report should be prepared to critique the operation.

UNIVERSITIES

Other, perhaps less controversial, sources that policing should liaison more frequently with in the future are universities and colleges. Forensic computing degrees are being offered by a number of institutions. Forensic computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable (McKemmish, 1999). Partnering with a university that offers a degree in computer forensics offers a number of benefits. The University of Tulsa (TU) provides assistance to the Tulsa Police Department, the Oklahoma State Bureau of Investigation, and the Secret Service. Members of these agencies are provided workspace in the Tulsa Digital Forensics Laboratory on the University campus to allow them to work together on cyber criminals. The lab, funded by grants, has advanced computers and more space than the agencies are able to provide. In addition, twenty TU students a year intern and assist the law enforcement agencies in investigations (Marciszewski, 2005).

The University Police Department (UPD) at California Polytechnic State University was the driving force behind the creation of a high tech resource group which includes local law enforcement from 5 counties, state agencies, the FBI, the district attorney's office, and private corporations. The group provides high tech training to the members and share expertise in high tech crime investigation. The forensic expertise of the university officers and the support and assistance of the faculty and staff has resulted in the successful conclusion of numerous investigations (Aeilts, 2005).

In addition to the immediate benefits of assistance with investigations and training, partnerships with academic institutions can also result in fertile recruiting ground for the agency interested in recruiting personnel with computer/technological expertise. An agency with a reputation for being technologically friendly and advanced is much more attractive to recruits than one with a traditional view of policing.

INFRAGARD

Agencies should consider joining Infragard, a program of the Federal Bureau of Investigation, started in 1996. Infragard is an association of businesses, academic institutions, state and local law enforcement, and others dedicated to sharing information and intelligence about potential hostile acts against the country. Of the top 100 firms in the Fortune 500, 83 have an Infragard representative. The group initially was directed toward cyber-infrastructure protection but after the terrorist attacks of 9/11, the emphasis was broadened to include both physical and cyber threats to critical infrastructure. Local chapters hold regular meetings to discuss issues, potential threats, and other issues that impact their industries. Local chapters provide training, local newsletters, and contingency plans in the event of attacks on the information infrastructure. (Infragard, 2007). The networking opportunities available with this group can be beneficial to both large and small agencies.

CONCLUSION

As in most areas of policing, partnering with others can be of assistance in addressing cybercrime. It is critical that CEOs of police agencies not be seduced by the quick fix (as we are too often in policing) and that any partnership and operations be consistent with the agencies vision, mission and values. Careful planning and proper supervision can help in addressing the pitfalls.

Strategies for local agencies to combat cybercrime:

*establish liaison with local universities or colleges which have resources

*identify local/regional/state/federal resources that can assist them as needed

*identify personnel within the agency who have computer expertise

*recruit new employees with the needed skills

*train personnel in cyber crime and computer related crime

*identify companies/private entities which have the skills, equipment, and desire to assist the agency with cybercrime investigations.

*have directives in place to ensure computer evidence is legally, properly seized

*keep abreast of the threat. Some ways to do this include joining Infragard and reading the annual CSI/FBI Computer Crime and Security Survey.

References

Aeilts, T. (2005). Defending against cybercrime and terrorism: A new role for universities. *FBI Law Enforcement Bulletin*, *74*(1), 14-20.

Commission on Accreditation for Law Enforcement Agencies. (2006). *Standards for law enforcement agencies: The standards manual of the law enforcement agency accreditation program* (5th ed.). Fairfax, VA: Author.

Dittrich, L. (2007). Tonight on Dateline this man will die. *Esquire.* Retrieved September 23, 2007, from http://www.esquire.com/features/predator0907#story.

Ellis, M. (2004). Mom’s sleuthing helped find missing daughter. *The Columbian*. Retrieved September 23, 2007, from http://www.genderberg.com/phpNuke/modules.php?name=News&file=article&sid=98.

Futuristics & Law Enforcement. (2000). *The Millennium Conference*. Retrieved September 30, 2006, from http://www.fbi.gov/hq/td/fwg/conference.htm.

Infragard. (n.d.). *Infragard.* Retrieved September 26, 2007, from http://www.Infragard.net/about_us_facts.htm.

Marciszewski, A. (2005, May 1). Students provide know-how for cops. *Tulsa World*, A19.

McCollum, D. (2007). The shame game: “To catch a predator” is propping up NBC’s Dateline but at what cost? *Columbia Journalism Review*. Retrieved September 23, 2007, from http://www.cjr.org/feature/the_shame_game.php.

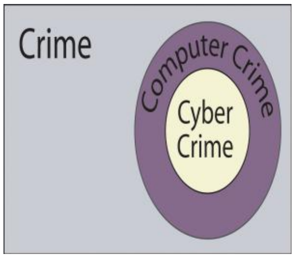
McKemmish, R. (1999). *What is forensic computing?* Canberra, Australia: Australian Institute of Criminology. Retrieved September 30, 2006, from http://www.aic.gov.au/publications/tandi/ti118.pdf.

Perverted Justice. (n.d.). *The PeeJ guide: For parents and first-time visitors to Perverted-Justice.com*. Retrieved September 30, 2006, from http://www.perverted-justice.com/guide/.

The Future of Cybercrime

Earl Moulton

Those of us in the Law Enforcement community have seen vast changes in our world in these past few years: changes in the demographics of our society, changes within our own agencies, and changes in the types and volumes of crime that we deal with, the kinds of suspects that commit those crimes and the victims that they create. Our legal environments have changed every bit as much as the physical environment that surrounds us. Given that state of flux, what can we possibly predict for the future that can have sufficient credibility to base our decisions on today?



One of the most significant changes has been the advent of cybercrime. While we may say that we know what it is when we see it, the term “cybercrime” has not been used with any degree of precision. For the purposes of this article, I will use “cybercrime” to mean “crime committed in relation to networked digital technology.” To illustrate, it is helpful to think in terms of a Venn diagram.

Where all legislatively prohibited behaviour constitutes the complete set of crime, there is a subset which is committed in relation to digital technology. It is this subset which is more commonly described as “computer crime.” A further subset is described where those digital technologies are linked in some manner so as to create a network. It is this ability to inter-connect, which I view as the *sine qua non* of cybercrime. For example, we can see that the keeping of a collection of child pornography on a standalone computer is both a crime and a computer crime. It only becomes a cybercrime when the computer storing the collection is connected to other computers and that connection is utilized to acquire, trade, sell, produce or otherwise deal with the pornographic images.

No matter where we are heading or how fast we’re travelling, it is possible to get a sense of our direction and of our velocity by looking in the rear view mirror. What does our recent past tell us about that direction and velocity? Veteran cybernauts will recall that in 1996, less than a mere decade ago, there were approximately 16 million Internet users in the world. That number grew to 513 million by 2001 and is now thought to be about 650 million. Recall, too, that the ‘80's and early ‘90's were characterized by standalone personal computers, both in the workplace and at home. The growth since then of the Internet has been matched by the intranets that are equally ubiquitous at work and, increasingly, in the home and home-office environments. The mid-‘90's also saw a somewhat brief discussion, now seemingly quaint, whether there really ought to be a “dot-com” domain on the Net and what constraints should be placed on it. As we move into the 21st century, the networked world continues to expand from wired to wireless. With convergence, telephony has become simply another aspect of our interconnectedness.

Parallel to the changes in our network environment have come advances in the digital technology that we connect. In the ‘80's, we marvelled at the speed of our 8088 based machines working at 4.77 Megahertz, which we connected to local bulletin boards by means of 300 baud modems - but we could hit the “turbo” switch to get all the way up to eight Megahertz! Now we use three Gigahertz motherboards to connect via T1 lines to terabytes of storage and demand even better performance.

Simply stated we are travelling at ever greater speeds into an ever more networked world.

While looking in the rear view mirror has predictive value, extending the automotive analogy also tells us that looking in the rear view mirror is a very bad way to drive a car. Clearly, although informed by our past, our focus needs to be on the future. What might it hold?

The Macro Context

As we look down the road, we can make some well-founded guesses about where the road will go based on the topography we see before us. In the cybercrime context, that topography is determined by the interaction of changing technology and changing networks with the human side of our society. This is the topography that lies outside of the Venn diagram discussed above.

In society at large, there are some general themes that are very apparent and will have equally apparent impacts on cybercrime.

It is becoming a truism to say that digital technology has collapsed both time and distance. Both information and money now travel around the globe virtually instantaneously. What happens in Afghanistan is instantly known in Tokyo, causing comment in London and causing reaction in Washington. Just as significantly, that same information is reflected on the Hang Seng, the Bourse, and the New York Stock Exchange. And each of those is always “on” – connected 24/7. While law enforcement has always been 24/7, what is new today is that it is always rush hour somewhere.

In 1965, Moore’s Law postulated data density will double about every 18 months. It is still true today. About every 18 months, one will get twice the memory and twice the speed from computers for the same price. With the advent of nanotechnology, there is absolutely no reason to believe that Moore’s Law will cease to apply for the foreseeable future. The velocity that we perceived in the rear view mirror will continue. And recall, speed is distance over time while velocity includes acceleration. We are not just going faster, we’re going faster *faster*.

Another aspect of general application is the demand by the general public for both greater transparency and greater accountability. For the Law Enforcement community, we see this in the increased levels of civilian oversight, in the demands for the disclosure of both the processes and the products of our investigations and, perhaps most apparently, on the nightly news. As technology enables greater and greater sharing of information, there will continue to be greater and greater demands to act effectively and efficiently on that information. Those demands will make ever greater inroads on our resources and continue to reduce the resources available to prevent and investigate crime.

Finally, we need to consider an anti-intuitive outcome of the digital revolution. In *1984*, George Orwell posited a future entirely controlled by an omnipresent and seemingly omniscient government. That very compelling view is reflected in our latter day discussions of privacy and, in most prognostications, of the future. The reality, however, is entirely different. Rather than controlling more, governments actually control relatively much less. This is seen most notably with the Internet itself which continues to resist efforts by governments to control its content, reach and form. Indeed, one of the greatest challenges to the Department of Homeland Security is the fact that so much of today's critical infrastructure is held by private, corporate interests. Lessening even further the reach of governmental intervention are the twin realities that private interests are both transnational and often larger than governments themselves. The true Big Brother is not Big Government; it's Equifax. As a function, and as a creature, of government, the influence of the Law Enforcement community has been lessened to an equal degree.

The Specific Context

There are specific aspects of cybercrime about which we can make some educated guesses as to their likely role in the future.

Target Hardening

In the traditional crimefighting world, target hardening generally means making it more difficult for someone to commit a particular crime. It is also a maxim that things can never be made foolproof because fools are so ingenious. The same can be said of crooks. In the world of cybercrime, we see the introduction of new technologies and applications followed closely by criminals creating new scams taking advantage of those advances. Ultimately, security holes are plugged, business processes are changed and operating systems, protocols and applications are re-written, and the targets are 'hardened.' This modern day equivalent to the development of better bullets and better bullet-proofing is likely to continue - with the cybercops condemned to eternal second place in the race.

Two other facets of this race are of note. First, the length of time between the introduction of a new technology or application and someone taking criminal advantage is likely to decrease sharply. This phenomenon is already being seen in the virus arena. The time between the identification of a vulnerability and the release of an exploit has decreased dramatically in the past two years or so. The result has been the need to develop increasingly more sophisticated tools to deliver timely patches, and, thereby circumvents system administration ignorance and indolence. The second facet is that havoc wreaked on 'soft' targets before they can be 'hardened,' is likely to be much greater simply based on the sheer numbers of possible targets.

Nonetheless, we ought not to lose complete hope. We need only recall the huge balloon of fraud that occurred shortly after the introduction of cell phones. Fairly quickly, however, there were technological responses and a more informed user cadre, and those levels of fraud returned to normal background levels. Tools to track offences occurring in P2P networks, over the IRC, and by 'spoofing' have become increasingly robust and offer a similar basis for optimism.

Anonymity

One of the contributors to cybercriminality is the anonymity that an Internet user experiences on the Net. While that anonymity is to some degree mythical, there is a very clear user ethos that holds that the use of the Net is, must be, should be, and need always be anonymous. Both our current experience of Internet use and broader social science experiments have shown that the perception of being anonymous lowers the barriers to criminal activity. Some have suggested that this may explain the otherwise unfathomable increases in child pornography activity. This "nobody will ever know that it's me" syndrome will only increase as the level of Internet use rises from its' current 10% worldwide level to levels approaching 50%.

Size of victim/suspect/target population

It is a concomitant of the rising participation level that the size of the possible victim population will also rise. So, too, will the absolute numbers of cybercriminals increase. What will the likely impact be on law enforcement? An answer to that question can be found in a reality that is all too often ignored. Early studies are showing that the profile of a typical cybercriminal is not at all like that of what we now think of as an ordinary criminal. We don't need statistical analysis of offender populations to tell law enforcement a truth we know from the streets - the levels of traditional crime are not falling off due to cybercrime. Bank robbers and burglars are not acquiring new skills sets to enter this new and exciting field. Cybercrime is an additional burden on law enforcement. Nothing in my experience as either a police officer or a futurist suggests that this is going to change.

There is special significance for raising the question of targets in addition to both victim and suspect populations. In the world of cybercrime, machines and devices controlled by individual victims are themselves separate targets. Where there used to be a single bank to be targeted by the bank robber, we now have automated teller machines located wherever there is a power source. Each of those machines are themselves targets for what they contain—cash—but also for the fact that they are avenues of access into banking networks and sources of access information—card and PIN information. Additionally, individuals now carry multiple targets. We have multiple, networked home computers, Web-enabled cell phones, Blackberrys, Palm devices, laptops, and cars communicating via satellites. Again, each of these target possibilities are in addition to existing targets and never simply replacing existing ones.

Timeliness

We considered briefly above the impact technology has had on the collapse of previous concepts of time.

This area, however, has special relevance to a number of specific aspects of cybercrime.

Fundamental to every criminal investigation is the acquisition of evidence. In the cybercrime world that evidence is exceedingly ephemeral. Network traffic logs, IP address assignments, random access memory, and Internet history files all pose special problems of timeliness. To the extent that current legal procedures, such as search warrants, require an inordinate amount of time to acquire and execute, the likelihood of evidence destruction, either deliberate or inadvertent, increases. When we layer an evidence request with the Mutual Legal Assistance Treaty process, the concept of timeliness loses all practical meaning.

Timeliness is also important to the identification of the *modus operandi* of a cybercrime. When thousands or millions of similarly situated possible victims exist, it becomes extremely important that the manner and means by which a cybercrime has been committed is discovered. That discovery must be then be made widely known to protect those possible victims.

Like traditional crime, much, if not most, cybercrime is committed for personal gain. Unlike traditional crime, the proceeds are not television sets, cash, or cars. Rather the proceeds of cybercrime are bits and bytes which, instantly, turn into credits in accounts, which get transferred into other accounts in other forms, in other institutions, in other countries, in other time zones, in other legal systems. The likelihood of ever extracting the profit from cybercrime becomes almost zero and raises the attractiveness of cybercrime in exact inverse proportion.

What is a Cybercrime 9-1-1?

In traditional policing, we all know how to priorize our calls for service. Just like with the media, 'if it bleeds, it leads.' If there is any risk of bodily harm occurring, the call goes to the top of the list. The same can be said of most budgeting processes. If there is a physically harmed victim involved, getting money into the policing budget to take action is seldom difficult. The final chapter in this phenomena is played out in sentencing proceedings in court. The sentencing of white collar criminals is notoriously lenient and can be understood in the absence of a bleeding victim. The experience to date suggests that cybercriminality is treated as simply another form of white collar crime and receives equally light sentences. Each of these implications compound themselves to make the future resourcing needs of law enforcement very difficult to meet.

There are many other aspects of cybercrime that will impact its future. Suffice to say at this point, that each of those factors leads to the inevitable conclusion that the challenge that will face the law enforcement community will be bigger, badder, more resource intensive, and more overwhelming than anything we have faced before.

Necessary Responses

If the situation is that critical, what can we do now to reduce the impact of cybercrime in the future?

One of the few things that has remained unchanged in the law enforcement world is the fundamental and essential importance of our human resources. This fact of life will not change. How, then, do we ensure that our personnel have the necessary knowledge, skills, and abilities to cope with the cybercrime challenge? The likely answer lies in the same technology that poses the challenge. The use of computer-based training, distance learning, and the adoption of 'just-in-time' training models will all work to ensure that timely information gets into the proper hands. Some of these innovations will require changes in our institutional and educational mindsets. Nonetheless, initiatives such as the Canadian Police Knowledge Network are showing that there are real alternatives to simply sitting and wringing our hands in anguished worry.

It is also important to note that our new personnel come to us with a significantly different technological background than our existing personnel. For our new people, there is no such thing as a world without the Internet or 24/7 connectivity. They arrive on the job with skills and abilities that were not even dreamt of when we were recruited.

Dealing adequately with the challenge of cybercrime may also require the law enforcement world to modify what we consider to be our goal posts. For most agencies, success is marked by the arrest, prosecution and sentencing of an offender for an offence affecting one, or relatively few victims. In many cybercrimes, it may be more appropriate to place the emphasis on the determination of how a crime is committed and then taking the necessary prophylactic measures to prevent thousands, perhaps millions, of other victims being created. Such an approach might also address the existing difficulty in getting the corporate world to report cybercrime. Knowing that the primary focus is on cybercrime prevention and the proactive hardening of systems and processes would go a long way to alleviate current anxieties.

One reality that is shared by every agency that now supports a 'high tech' response capability is that these are very costly units to create and maintain. That phenomenon will not go away. We need to prepare our funding sources for a very significant and ongoing cost centre. The analogy that can be used is the different scale of funding that was required to move from riding horses to driving cars.

Finally, we need to apply a lesson from the traditional crime fighting arsenal. Crime rates for particular offence types really only change when there is fundamental change in the outlook of the general public. We need to educate the public about the 'dark places' on the Net. We need to get people to understand the importance of firewalls and secure passwords. We need an educated public to understand the risk to their private information and to their very identity that is posed by cyberspace. We need an informed and engaged public to demand, either as consumers or as an electorate, that industry supply the cyberworld equivalents of air bags and seat belts. It is that same electorate that will need to demand that laws be made effective and that artificial and archaic concepts of jurisdiction be removed.

As Sir Robert Peel understood centuries ago "the police are the public and the public are the police."

Some things don't change.