ORGANIZED CRIMES AND INTERNET INVESTIGATIONS

Insp. Mike Ryan, B.B.A., LL.B.
Organized Crime Agency of B.C.

Generally, it seems to be a fair statement that criminal investigations involving the Internet can be grouped into two categories, although its important to note that the second category is not mutually exclusive from the first.

The first is where the Internet is used to advance criminal offences as the result of its unique capability as a very efficient communication device. In historical terms law enforcement must have struggled with similar issues on the emergence of the telegraph and the telephone. All of these technologies allow the transfer of information which by the nature of its content, or connotation of it meaning, is illegal or advances some illegal act.

Considering the Internet only from this perspective, examples of the unlawful acts which it can facilitate are the distribution of child pornography, inciting hatred, conveying stolen information or the conveying criminal information (such as directions in furtherance of a drug deal, information to advance a theft, or some other criminal purpose). From this first category, the main challenge for law enforcement is to maintain a position on the technology curve in order to intercept these criminal communications, despite encryption and jurisdictional questions.

The second category is where the Internet is being used in the broader sense, to support or advance, more completely, the elements of a criminal offence. Some examples of these are instances large scale theft, fraudulent marketing schemes where goods are pledged but not delivered, stock market frauds, money laundering and illegal gaming. The first category can be, and often is a component of the second.

Both of these require very different resource requirements and present very different investigational challenges. Traditional investigational methods can be more easily applied to deal with first situation where the Internet is used as to assist in the commission of the offence, but the second set of examples engage a broader discussion.

In either example, all investigational efforts must be complaint with constitutional guarantees and proper evidence gathering methods. The public aspect of the World Wide Web is widely considered to be analogous with displays such as newspapers, magazines and radio or TV, and therefore it may seem unlikely to generate any serious or reasonable expectation of privacy.

However, certain web sites and chat rooms may establish a different expectation. While it would likely be insufficient to simply post a banner stating that the contents of a web site are "private" or "confidential" thereby removing it from the public domain, investigators should be cognizant of situations where the user has to obtain a password to gain access. Instances where the password is generated by the user may not be problematic, as the privacy interest is defined by the user.

But, consider where the user is issued with a password by the operator of the web site. Then it may be argued that there was an expectation of privacy, as the operator intended to limit the communication to a select individual or group of individuals. Here as well, any web site operated behind a firewall or an Intranet network, which limits access to a defined group or class of users using a login identification process, would clearly be considered private.

Also it is possible for the expectation of privacy to change - midstream - by creating some limitation to access, with perhaps unexpected consequences to law enforcement. Consider the analogy of police surveillance. When observing the actions of a suspect in public the surveillance generally ends when the suspect enters a private place.

Current technology (and even more so the probable developments of future technology) will permit law enforcement to conduct Internet surveillance to continue any where and any time. Either by inadvertence on the part of the investigator or by deliberate mischief of the accused, "privacy traps" might be encountered which could either render evidence inadmissible, or through the speed of technological development, create serious problems to law enforcement in attempting to secure the appropriate judicial authorization.

If this analysis is correct, the challenge to the investigator is to recognize any heightened privacy interest and to expeditiously obtain an authorization to continue. Also, it is of more than a passing concern that legal challenges to the propriety of police surveillance in the physical world could, if successful, affect even passive web site monitoring by police.

The distinction made earlier in regard to the degree to which the investigation is to find itself dependent upon evidence recoverable over the Internet, raises issues of evidence gathering and storage, reproduction and disclosure, and presentation for court.

Evidence gathering at the basic level, in that category of offences where the Internet is used only to facilitate a criminal offence, can be accomplished by converting the screen image into a digital stream transferable to at VHS tape, hard copy screen prints and augmenting those with extensive investigational reports. In that second category of crimes, where the Internet is used to advance more completely, many of the elements of the offence, the challenge is not only to capture the information being transmitted through this very efficient communication medium, but also to demonstrate the creation, configuration and control of the system, by some entity, which ultimately bears criminal responsibility.

Obviously it is this second category of crimes which creates the greater challenge, and it is here that the paradox of the Internet being simultaneously the most public and private of places is demonstrated. In Canada, consistent with the constitutional necessity for law enforcement to gather evidence within acceptable boundaries, the discussion has to distinguish between non-invasive and invasive investigational methods.

On the non-invasive side there are trace route analysis, name server look up and " whois" queries, all of which attempt to identify location and control points of the suspect system.

The process referred to as packet sniffing is the analysis of data traffic generated between two or more computers, and is used to determine the number of computers that may be in use, where they are located and the type of functions they are performing. This process seems to come down as being comparable to what in Canada is referred to as a "one party consent". As law enforcement requires judicial authorization to record a private communication even when one party consents, investigators would be encouraged to obtain at the minimum a General Warrant under subsection 487.01 of the *Criminal Code of Canada* before engaging in this process.

However, the argument exists that the packet sniffing process is the recording of "observations" and is not the recording of "communications" as investigators just encounter electronic representations of the routing that the communication is taking through the Internet rather than the communication itself. This argument may be valid where the communication is so

heavily encrypted that its content cannot be determined. But, in another demonstration of the paradox of the Internet being simultaneously the most public and private of places, an immediate duty might be created on law enforcement, to cease monitoring packets and to seek judicial authority as soon as a "communication" becomes discernable.

Clearly on the more invasive side are the investigational tools which should only be used with judicial authorization. Evidence gathering in these areas may be dependent upon the all the forgoing techniques, and also other tools which monitor and report key-strokes, or which surreptitiously enter the suspect system and chart its components.

It should be noted however, that these tools may not have been designed with law enforcement in mind. Many operate recursively, just as water flows when filling an ice cube tray from one compartment to the next. The problem is that investigators may need to avoid certain compartments which the legal authorization does not give them the right to access, and in other instances to return to these compartments but in a direction contrary to the direction of the flowing water.

Now consider the problem from the perspective that some of these compartments will be located in different countries, and it is easy to see the international sovereignty issues that could be awaken. This creates the challenge of drafting extremely accurate and detailed applications for judicial authorization, and securing international agreements which clearly state what information is being sought and where it is located. Unfortunately, absent a parallel criminal investigation in those other countries, the only process available in Canada to compel international assistance is to make a request under the *Mutual Legal Assistance Act*, which is a process that generally takes months to complete.

Still other invasive techniques may include installing hidden programming which would be triggered when certain events occur and would "call home" over the Internet. Equally, the concern here is for the proper crafting of the judicial authorization, but also to ensure that some residual damage is not inflicted upon innocent third parties who may be reliant upon the suspect system, or a down stream Internet user.

Having to this point, been concerned primarily in information collection, the gathering of evidence (usually under the authorization of search warrants) can present containment and data

storage issues. In Canada (due to the rules created by *R. v. Stinchcombe*), the necessity to disclose all investigational material can create the need for data silos which exceed the capacity of even the best equipped law enforcement units.

The containment and preservation of evidence is an issue when ever a computer system can be remotely accessed. The term used is "a root war" and refers to the battle which ensues when control of an operating system is in dispute. Either by direct Internet access, or by pre-programmed codes activated by a cellular phone (from anywhere in the world) it is possible for suspects to interrupt or re-route systems. Law enforcement have relied upon pre-dawn entries while the suspects are asleep, in order to obtain containment when this problem is expected. (It would seem to be a simple matter, however, for the suspect to build a link between the Internet and his alarm clock.)

In a local case where a root war did occur, it was only after advising defence counsel who were on scene at the search site, that investigators would immediately crash the system in order to preserve the evidence (thereby causing irreparable damage) did the suspect cease attempting to thwart the investigation.

Having achieved containment and to return to our analogy, we have assumed to this point that the compartments in our ice cube tray are all the same size. But consider what might occur where some compartments are comparatively as large as a kitchen sink or a bathtub, and it becomes necessary to gather all of the evidence that they contain. The need for pre-search planning cannot be over stated, as investigational budgets and resources could be easily expended without even having approached the objective.

The eventual development of search techniques which permit the online transfer of seized data, either with or without the suspect's knowledge, to commercial storage silos, may not be that far off. Privatized storage of data for court exhibit purposes will become necessary as it will be unlikely that even the best equipped police computer lab would be able to stay abreast of new programming and the individual customization which occurs to each system. Data, once captured must be held secure and uncontaminated with all configuration codes and original parameters intact.

Its been suggested that in technical terms, a year is actually only three or four months in real time. The partnerships required to effectively deal with Internet crime must consider the speed with which technology is effecting change to operating systems. Long term law enforcement initiatives and strategies will be derailed as criminal computer systems are updated at the rate dictated by commercial realities, and police investigational tools are updated at the rate of government funding. Once the evidence is gathered, costly and time consuming reconstructive work is required to ensure that the elements supporting a prosecution can be accurately presented in court. This creates a lag between the successful completion of a long term investigation, and the training and experience required in order for investigators to remain current in the field. Disclosure and presentation of evidence in electronic format is an entire other area of discussion. Under the current disclosure rules in Canada, there is no assurance that electronic disclosure will be adequate for defence or the court.

No discussion of the challenges to Internet investigations would be complete without some consideration of what the future may bring. In a recently released survey by KPMG Investigation and Security Inc. Of the top one thousand companies for 1999 as ranked by the *Globe and Mail*, it was suggested that most respondents had embraced e-commerce or expected to do so in the near future, and viewed the greatest threat to be via the Internet and other external sources. Interestingly those respondents did not seem to consider the internal threats to their e-commerce systems as significant. External access to confidential customer information and denial of service attacks were the corporate concerns, with the protection of credit card numbers and personal information was the greatest concern to their clients. In that survey encryption technology was considered to be the best preventative security measure.

But comments in the July 2000 issue of *Scientific American*, attributed to a paroled computer hacker who stole the OS source code worth $80 million dollars, were that the basis of most of his exploits was social rather than technical. He stated that in fully sixty percent of his attacks, he was successful through “social engineering” methods which allowed him access by playing one division of a large company off against another, or by using jargon that only an employee would know.

The epidemic of e-mail viruses which are triggered by the user's curiosity to alluring names such as "I LOVE YOU" seem to make the point. Similarly, this same kind of camouflage might cause an employee to unknowingly install a program that sends all of their data to a competitor. As Pogo, the comic-strip character said, "We have met the enemy and he is us"[1]. That seems to be true when we consider replicating hacker software which can turn personal computers against others in targeted distribution denial of service attacks, such as the Code Red infestation this summer.

Internet crime of the future may be very different than what we may expect, when we consider that the U.S. Department of State has confirmed that there are now over 190 virtual countries which make dubious claims to nationhood.[2] While some may be the creation of college kids with too much time on their hands, or arise from a political-science class experiment, others have a more questionable intent.

For at least one such virtual country [3] the claim of a religious origin is being advanced, with land claims, a written constitution, appointment of officers of president and secretary general, and a the creation of a legislative branch complete with a separation of executive powers between church - state - and a judiciary. (What's interesting is that this particular virtual country claims to have an origin founded by its king on the 19th of July in the year 2030 before the birth of Christ. That seem quite remarkable when the designation of "July" as a month of the Julian calendar was not established until 44 BC when Julius Caesar named it after himself.)

Other virtual countries claim to have passed laws with regard to citizenship and naturalization, taxes and financial reporting, the authority to grant licenses, foreign exchange transactions, bankruptcy and trust laws, domestic and foreign banking, and securities

---

[1] Scientific American, "Code Red for the Web", Carolyn Meinel, Oct. 2001, p. 50.

[2] Proximal Consulting Newsletter April 2000, www.proximalconsulting.com.

[3] Dominion of Melchizedek at www.melchizedek.com, (The Melchizedek king of Salem blessed Abraham, the righteous king of peace and history's first monotheistic teacher of the Most High God.) The ancient homeland of the Dominion of Melchizedek is the land south of Lebanon, west of Jordan and north of Egypt, with its capital as Jerusalem.

underwriting, and some claim ambassadors and consul generals in many countries. Some have even gone so far as to declare war consistent with declarations of the United Nations Security Counsel. Perhaps not surprising, several have found it necessary to invoke legislation which permits the licensing of lawyers.

Such presumptuous statements may also have other purposes. Consider one report from the Australian Transaction Reports and Analysis Center (AUSTRAC) which raises concern in regard to the risk of money laundering through these virtual countries. The services offered by virtual countries have been linked to scams in California, Latin America and the Pacific region. Arrests have been made where hundreds of Filipino, Chinese and Bangladesh citizens paid up to $3,500 for worthless travel documents which were held out to be "internationally recognized travel documents". Still others paid to obtain "government jobs" on disputed semi-volcanic knolls located in the Pacific Ocean. Get-rich-quick investment schemes have been associated to a series of world wide swindles, when virtual-bank assets supposedly backed by U.S. Treasury Bonds turned out to be worthless financial instruments. [4]

Still others offer offshore insurance companies, also with phoney financial support, located on sandbars located at the mouth of large rivers, created by the last hurricane that came through and destined to disappear with the next. Some of these suggest an Aboriginal origin, in an attempt to ensure that their claim is rooted in an historical event which is difficult to substantiate, and which cannot be easily dismissed.

By obtaining company registrations in jurisdictions which do not restrict the use of words such as "Bank " in company names, it is possible for the virtual country to open an account at a real bank in that jurisdiction. The result is access to the credibility of the financial sector, by a corporate entity which is nothing more than a shoe-box full of official looking documents in an offshore safe-haven. The magic of the Internet then allows visual images to be attached , to create the visual impression of credibility and stability.

---

[4]Bertil Lintner (lintner@loxinfo.co.th), Thailand based correspondent and author who has written extensively about the international drug trade and organized crime, from an article as part of a larger project supported by a grant from the John D. and Catherine T. MacArthur Foundation.

In a local example, documents seized at the Vancouver International Airport suggested that accompanying bearer bonds had been issued by a bank in a nation which emerged from the Former Soviet Union. The associated web site presented images of tall stately buildings with green grass and lawns - but in an area of the world which is war torn and troubled by political instability. Aside from the fact the IP address registered to that web site indicated that it was being operated out of Philadelphia, an enlargement of an Ohio license plate on a vehicle parked out side the bank, suggested that there were some serious inaccuracies.

We are at risk of seeing the creation of "data havens" which would emerge in remote geographical regions, and would market Internet secrecy for a price. Probably the only reason that these have not more fully emerged to date, is that the necessary communication infrastructure has not yet reached the remote regions which would be willing to enter into this industry. The experience to date has been that attempts to locate large criminal Internet systems in these remote areas is initially effective, but inevitably parts of these systems are driven out - not by the threat of prosecution - but by the reason that the systems have grown to be so successful that they cannot continue to find technical support and bandwidth, and are forced to relocate all or a major part of the system somewhere closer to the center lane of the communication highway.

If we were to confine the discussion to only money laundering, its an easy reach to see where the risk lies. Money laundering can be generally described as operating in three phases - placement - layering - and integration. These three describe the act of placing ill gotten gains into the financial system, the act of layering the proceeds of crime into a myriad of international investment vehicles, and finally integrating the now co-mingled funds back into personal use.

The creation of virtual entities which may be relied upon by other legitimate deposit taking institutions, even if only momentarily, is sufficient to place large amounts of criminal capital into the financial system. Its not necessary even to reach into the realm of virtual counties, to recognize the opportunity for laundering vast amounts of criminal proceeds - consider Internet gambling for example.

Franchised Internet gaming systems may appear to be licensed in some remove jurisdiction which permits this activity, but the investor is often relying upon a centralized operator who designs and operates the system, and provides all operating systems, technical

support, odds and betting line feeds, credit card validation, game servers, random number generators, customer service and support, accounting, wager payments. The investor brings in the development capital, but the operator provides all services, and collects up to 40% of all revenues based upon the volume of traffic through the casino.

In those instances, there is no real need for the investor, as the operator is just attempting to insulate himself from criminal prosecution by foisting that liability onto the investor. While the operator declines to accept wagers from the North American gaming public, the investor who is incorporated in some secrecy haven, is caused to believe that he has found a loop hole and cannot be prosecuted as his casino is operated by an off-shore corporation.

Aside from the risk of an investor or operator being found criminally responsible for running an illegal gaming operation, the Internet gaming industry presents significant opportunities for organized crime. If organized crime was represented by an operator or investor, seeking a portal to place proceeds of crime into the financial system, Internet gaming provides placement - layering - and integration opportunities by loading cash into offshore bank accounts and running it through their casinos for disbursement to anywhere in the world. Organized crime, represented by the individual gambler, can easily layer and integrate proceeds of crime by wagering on event which pay, close to, or even money.[5]

If the Internet gaming operator or investor were fronts for international terrorist groups, political acts of violence could be funded from revenue earned from Internet entertainment, and paid for by the unsuspecting citizens that the terrorist group intended to attack.

In conclusion, the challenges of the future are:

1. for law enforcement is to establish true partnerships within the public and private sectors and to expand investigational horizons into areas where law enforcement has not previously ventured.

[5] Investigators found that by wagering on both sides of sporting events to keep expenses low, they had a stable rate of return less the vigorish charged by the house. A similar result can be obtained by wagering on black and red in roulette.

2. for government is to recognize the need for this type of enforcement, to fund it adequately, and to establish international agreements which will allow information exchange and evidence gathering.
3. for legislators is to pass laws which will permit law enforcement to go to where technology is taking us.