Intelligence as an Investigative Function

Robert Metscher
CPP, CISSP, CSS, CPO, MBA

Brion Gilbride
CPO, CSS

August 2005

Table of Contents

In our society today we hear regular mention in the news about "intelligence." Unfortunately, many of those mentioning it are relatively unaware of the nature of "intelligence" or the role it plays in national defense, law enforcement, and security operations. Although intelligence is most commonly thought of in terms of national security, conjuring up images of CIA agents in trench coats standing in the shadows and spy-satellites relentlessly recording an adversary's every action, it is none the less an important part of both law enforcement and private protection operations. So then what is intelligence, where does it come from, how is it used, and why is it important to an investigator? How can an investigator gain an understanding of the skills necessary for intelligence operations and what legal concerns exist for these activities?

First, how does intelligence relate to investigations and vice-versa? Intelligence and investigations utilize many of the same skills and techniques. Both utilize inductive and deductive reasoning to reach conclusions, but the single biggest difference is likely to be the nature of those conclusions. An investigator must present facts as they are received and discovered, while avoiding making final assumptions concerning culpability, liability or fault (Dempsey, 2003). All of these must ultimately be established by a legal or quasi-legal process, and may be based largely on the investigator's work. An Intelligence Analyst must present their information with conclusions based on the information obtained. Analysts may be expected to provide probabilities that an event *will* happen at some point in the future. So another inherent difference is the purpose of the final product. An investigation report will most often be presented to a finder of fact, such as a jury, arbitrator, referee, and so on. However, intelligence reports will most often be provided to decision-makers to help guide future actions. In law enforcement, a well-formed intelligence function will help guide investigative activity by analyzing crime trends in the jurisdiction and any migrating activities heading toward the jurisdiction. In the National Security realm intelligence affects foreign policy and how nations interact. In the private sector intelligence is used for understanding the business environment, including the competition, and for improving protection efforts. For the sake of conceptual continuity concerning the private sector, we will not discuss competitive intelligence in any depth[1], although it follows the same process, but instead we will consider only protective or enforcement intelligence operations.

To better understand our discussion and how it is presented here, there are a few distinctions that must be made concerning intelligence, who creates it and who consumes it. There are many reasons for collecting intelligence, with just a few being: national security, law enforcement, protective operations, and business or economic competition. Both government agencies and private entities may conduct collection efforts for any of these purposes with the most significant differences being their available resources and the different legal restrictions that each face. With this in mind we will focus our discussion on law enforcement and protective operations. However just as with investigations, it is not the context as it is the process that makes for worthwhile intelligence efforts.

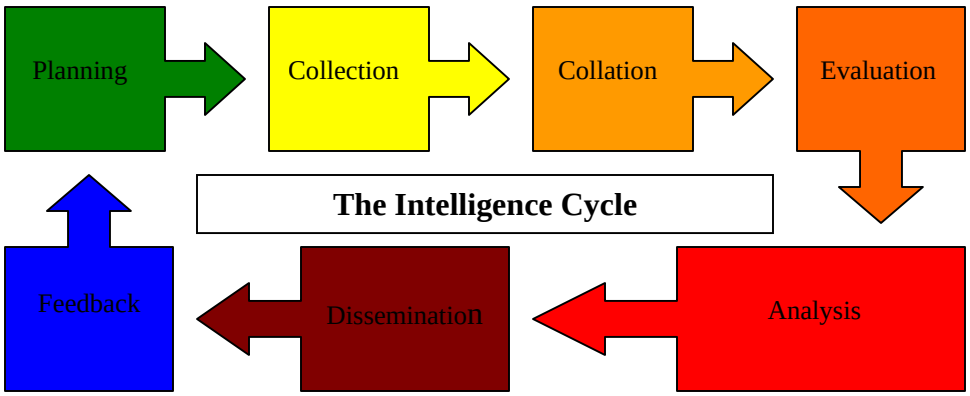
What is Intelligence?

> *Intelligence is a product created through the process of collecting, collating, and analyzing data, for dissemination as usable information that typically assesses events, locations or adversaries, to allow the appropriate deployment of resources to reach a desired outcome.*[2]

Nearly every agency and textbook offers a different definition of intelligence; however they tend to agree on one point. Analysis! Intelligence cannot be called intelligence without analysis. And herein is the single greatest difference between intelligence and investigations. Whereas an investigator will certainly analyze the facts of an investigation he or she should not provide any speculation outside of the facts. Conversely, the value of an intelligence analyst is not realized until they make such inferences. We cannot count on any one piece of data explicitly spelling out the intentions of a person or group, nor can we expect all relevant facts to be disclosed prior to anyone's actions. As such, it takes an analyst to make an inference based on the available information as to the adversary's future actions. To illustrate this let's consider the relationship between data, information and intelligence.

Data is the fundamental building block of intelligence. It is the phone number gleaned from caller ID; the quote from a newspaper, all of the vehicles in your rear view mirror during a trip, the network firewall log, or the snippet of conversation overhead on a bus ride. Data is literally all around us constantly. It is precisely because of the disorganized nature of all of this data that before it can be very useful it must be developed into intelligence. With our relatively newfound ability to acquire, share, store and retrieve information through the Internet and our other networked information systems, the problem is often no longer whether we have the data we need but whether we can distinguish it from the rest of the available data.

Information is data usable or applicable to the current context. In other words, information is what remains after everything that is irrelevant is discarded. It is the phone number gleaned from caller ID and matched with a person known to dislike us or our charge, the presence of the same vehicle in your rear view mirror for much of a trip, or the portion of the firewall log identifying the specific IP address of our attacker. Information is the data that we will use as we refine our forecasts, predictions and estimates.



LEAS, 2004

If an intelligence analyst were an abstract artist then the data would be the canvas, paints and brushes; the information would be the painted image, but the description of the finished image is the intelligence. The analyst does not *create* the intelligence; he or she interprets the information and provides an analysis as to its meaning. Just as the placing of the different colors and textures of paint are what the artist creates with the supplies available. In the truest sense an analyst will work with the information that is provided and not be involved in data collection. This can be found more often within government agencies; however in the private sector, where budgets, productivity, and investment return are deciding factors, the analyst is often required to be directly involved with collection efforts. This should not be discouraging since quite often private efforts are more narrowly focused and general involvement may add excitement to the work. A government analyst may be required to work with data and information acquired through many sources, while in the private sector there may only be a handful of researchers and other sources. Now let's consider a few relevant distinctions before we move on to data collection.

Intelligence or Counterintelligence

Even though the term counterintelligence is not used nearly as much by the media, it plays a significant role in an overall intelligence program. Loosely defined, counterintelligence is monitoring and interdicting your adversary's ability to monitor and interdict your operations. These are the "spy catchers" of national security programs. The role of counterintelligence is generally separated from intelligence in national security settings, but in the realm of law enforcement and private security any separation would be based on available resources. In some instances this may be not possible at all. The importance of discussing counterintelligence here is the recognition that any techniques of gathering information, legal and illegal, may be used against you and your organization. An extremely well developed counterintelligence program is capable of "feeding" disinformation directly to an adversary's collection efforts while being aware of what "true" information has been collected. This creates phenomenal dangers to operations, and so the importance of protecting your own collection program and organization from hostile collection and infiltration should not be understated. The best collection program in one organization can be undermined by a strong counterintelligence effort in another organization when the analysis process is ultimately contaminated. Remember it is not safe to assume that your adversary will adopt as high an ethical threshold as you and your organization, so appropriate precautions should be taken to guard your organization from hostile collection efforts. This includes Competitive Intelligence in the business realm, which is used by businesses to gain information on their competitor's products and services. That topic is beyond our scope here but should be considered one reason why an adversary would want confidential business information. For more information specific to competitive intelligence visit The Society of Competitive Intelligence Professionals' website (www.scip.org) [3]. Typically the programs and efforts used for preventing information leakage are referred to as Operations Security or OPSEC[4]. As we discuss the role of intelligence within protection programs and law enforcement also consider the parallel role of counterintelligence.

Criminal Intelligence and Crime Analysis

Within Law Enforcement there are at least two different fields of analysis. The most common are criminal intelligence and crime analysis. Although the two are often grouped together in many settings and discussions, there are subtle differences. Crime analysis consists of the techniques and processes for studying crime patterns and trends, their affect on a jurisdiction, and any law enforcement response. Criminal intelligence, however, is more concerned with people, organizations and any relationships between them (IACA, 2005). Our discussion will continue to focus on the use of intelligence, rather than the specific organizational role of the analyst. Due to the similarity of the tools that may be used for either purpose, and that both work toward identifying future criminal events, a distinction will not be made here.[5]

Data Types and Sources

Data, the fundamental building block of intelligence, is collected via "sources" which can be broadly classified into two groups, open source and closed source. Open sources are those generally available to the public and closed sources typically are not available to the public. The concept is simple enough. From this, many may believe that closed source information is what everyone needs, and in some instances that may be true, however the bulk of intelligence is often derived from open sources. It may be hard to believe that a great deal of information is obtained through public sources. Open source information is more readily available, but its limitations are found in tight knit planning groups, criminal operations, and within classified government activities where public releases are not common. This should not indicate that open source information is not useful in these situations. Let's consider this more closely.

It is important to note some of the legal differences in the United States between law enforcement intelligence and intelligence activities in the private sector. As a direct result of abuses over the last several decades, particularly during the Vietnam era, there have been several rulings concerning how law enforcement agencies are allowed to gather intelligence, for what purposes, and how these records must be maintained. In short law enforcement agencies may only collect intelligence on individuals or groups based on a criminal predicate or an articulated belief that future criminal actions will be committed. Agencies may not collect information based on race, ethnicity, political beliefs, religion, or other lawful characteristics (Carter, 2004). Protecting civil liberties is an essential government responsibility in a free society, and as such collection efforts must be based on a "criminal predicate." In the private sector, however, information collection is limited only by imagination, and by few legal constraints. These legal restraints most often deal with wiretap/eavesdropping laws, lying to government or financial institutions, and unlawfully acquiring protected credit data. There are other restrictions as well, and involved in collection efforts should be familiar with all state and local laws. Private investigators often have greater leeway in what information they may collect and how they may collect it. Whereas Law enforcement, in collecting information, takes the risk that its efforts may be attacked by civil libertarians when, for example, attempting to gain access to library circulation records. A private investigator, on the other hand, may be able to gain information through a phone call depending on local legal constraints and their personality.

Data Quality

Sources of information come in all shapes and sizes, but they are not necessarily of the same quality. Information is valuable, but not all information has the same value to us. What affects the value of information? Timeliness, reliability and applicability. If the information we receive is old or outdated, its value is reduced in the context of forecasting a specific future event. Information that cannot be trusted, or is unreliable, is less valuable to us because we must take extra effort to make sure it is accurate. Finally, if the information we collect does not apply to our goals then it will be of little use.

To ensure that the intelligence we provide is accurate, we must first be certain of the data we are using. If we consider data as the fundamental building block of intelligence and information as consisting of smaller components of data, it becomes easier to recognize that poor data makes for poor information and thus flawed intelligence. As a result of poor intelligence, the wrong people may get hurt or killed, and the credibility of future efforts will not be held in high regard.

The timeliness of Information is relatively self explanatory in the context of its value. If you are told that you will receive something the day after it arrives, it's not intelligence it's history. It is easy to become a historian if there is not a constant drive to develop predictive information. It is easier to be a historian but the value of your work is far less. What should be noted about timeliness is that collection efforts occur over time. In some instances, the collection timeline causes earlier data to expire. To avoid this it is sometimes necessary to divulge this information in an interim report or statement to preserve its usefulness. This will be discussed as we discuss the different types of intelligence products. It is, however, important to recognize that the "Time value of information" causes the value of information to dissipate over time. It may be one hour, one day, or one decade, but the value of that particular piece of information is generally reduced.

The importance of accuracy cannot be understated. Inaccurate data will ultimately lead to inaccurate intelligence, not accounting for luck or acts of nature. Accurate information ensures that our organization's actions are proportional. If a retailer is told to expect an enormous theft at their distribution center their response may be equally enormous, however it may be a little disheartening if that attempted theft turned out to be just a few items of moderate value. Resources will be mobilized, causing unnecessary expenditures based, in part, on the intelligence assessment. The intelligence analyst must also be cognizant of the fine line between being an alarmist and being a historian. The alarmist indicates that every future event will be enormous and most of the time they will be incorrect. This is an indicator of either lazy analytical work or an analyst that is out of touch with reality. Regardless of the cause, either will result in poor intelligence products. On the other hand, the historian fails to forecast anything but is more than capable of describing the incident, and its shortcomings, in the past tense. Although past incidents may at times help predict future activities; that should be part of the analysis as a whole, and not the whole analysis. It is important that an analyst avoid being either an alarmist or a historian. Data accuracy must also be examined from the standpoint that the data collected may be *disinformation*, or information that is specifically released and is intentionally wrong. This is a useful counterintelligence tool and one to be wary of if your adversary possesses this capability. While disinformation is used to deliberately mislead adversaries, misinformation is the term used when identifying unintentional errors in presented information. Consider an informant that deliberately releases false and misleading information about someone they have

become angered with. The result could be devastating to that person in the short term, and embarrassing to law enforcement if they rely to heavily on the informant's information. Be aware that information obtained by motivated sources, especially that which is unsolicited, should be weighed carefully before conclusions are drawn. Not only should the data be reviewed for accuracy but the final analyst report should be logically supportable as well.

It is not always possible to ensure the accuracy of collected data. It is obtained from many different types of sources, and all of these sources have different motivations and idiosyncrasies. To account for potentially inaccurate data, it is necessary to assess the reliability of the source. A source becomes known for reliability over time as data obtained from this source is consistently accurate. One way to determine the reliability of any data is corroboration. Corroborating data is nothing more than obtaining the same information from another unrelated source. In the world of the Internet it is common for persons to claim that they are corroborating information from multiple locations, however upon closer examination it is usually the case that each of these sources obtained their information from the same original source. "Sourcing" data, or tracing it back to the earliest known existence is one way to avoid incorrectly believing that data has been corroborated. Corroborating data allows us to neutralize the "spin" that different sources may put on the same information. To further evaluate why a source "spins" a specific way consider their motivation for generating the data. In those instances for which the data may not be corroborated the reliability of the source becomes even more important. Why was the source motivated in the past, if they provided information previously and why is he or she motivated now? The reason for any changes may indicate a significant change in their reliability.

Data should be challenged to ensure its accuracy, timeliness and validity. Failing to do so may result in unnecessary injuries, expenditures, and embarrassment. The goal is to provide a reliable product to assist in formulating an effective and economical response to a particular issue. Reviewing data from several perspectives allows us to increase our certainty that our analysis will be built on a solid foundation.

Open Source Data

In Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Intelligence Agencies David Carter, Ph.D. states, "The main qualifier that classifies information as open source is that no legal or clandestine collection techniques are required to obtain the data." He further states that, "Open source information is any type of lawfully and ethically obtainable information that describes persons, locations, groups, events, or trends." As accurate as these definitions may be they do not address the question of what are ethical collection methods. The answer to this may be very different when answered by national security, law enforcement, or private security personnel. Each analyst or investigator must decide the answer for themselves and ensure that it conforms to legal, organizational and client requirements. Open source data is the most readily available and includes all media sources, publicly accessible databases, commercially available databases, government reports, and all data available through the Internet. This includes many criminal and civil court records, property records, social security number verification services, and many more. The volume of data available to the public is amazing. Although some countries have attempted to limit the amount of personal information available, there is still an incredible amount of legally obtainable data.

Skillful exploitation of Open Source Information or OSINT is done through well-crafted research. One must know what information is sought, where it is maintained or who may possess it, and how it to reach that data (Cooper, 1996). Two key distinctions of OSINT is the difference between free and pay access data. A considerable amount of online media, discussion groups, and databases are available for free. Some may require registration for marketing and tracking purposes, but the information is none-the-less free. Two common pay access sources include high-end media service databases (I.e. Factiva), and consumer information databases (Ie. Choicepoint). Many others exist primarily for specialized types of information. Currently the most commonly used free-access OSINT resource are Internet search engines. Google, Yahoo, Teoma, Dogpile, MSN, and many others provide near instance access to free information sources on practically any topic. Never before in history have so many people had so much access to information that so many are willing to share. Individuals all over the world with a passion for specific topics have started webpages, discussion groups, databases, and informational sites accessible by anyone with Internet connectivity. Newspapers, magazines, and groups of all flavors have provided web access to their materials. Want to build a home computer network? Why buy a book when it's already carefully documented on many websites, some of which offer discussion group support, and it's free! The same goes for many security and threat related topics. We will discuss how to find this data using structured search criteria a little further on.

Open source information also comes in the form of Covert Channels, which can also create closed source collections as well. Covert Channels are methods of communicating data inadvertently. This is typically an unexpected result of regular activities associated with the information being concealed, or it may be a nearly unavoidable result of support operations. One of the best examples of this is parking lot vacancy. It was long reported that Lockheed, a major U.S. defense contactor, did not have an active government contract, but the parking lot at the Skunkworks, Lockheed's aircraft design division, was always full. Years later, the stealth fighter program being worked on there was made public. Another example mentioned in the news is the increase in food deliveries made to the Pentagon, the headquarters of the U.S. Department of Defense, during wartime preparations. Consider this in relation to your organization. Which employees stay late or arrive early during significant events? Which employees are traveling when a major proposal is being presented to a client? Are visible security efforts increased when your organization has visitors? Are special parking places kept open on those days? Are only IT personnel vehicles present in the parking lot late at night when the network is being upgraded?

Could this information be detrimental to your organization? Maybe not in and of itself, but combined with other information, it could be quite harmful. For instance, a casual conversation in a bar with a security officer revealed that there just aren't enough officers to monitor all the doors when VIP's are visiting because additional personnel are placed in areas to assist the visitor. Couple this with the knowledge that a particular radio channel is only used for drivers assigned to the VIP's. An intruder need only monitor that radio frequency for traffic. Once this radio traffic begins the attacker is instantly aware that an alternate access door may be available for an intrusion. Choose any similar scenario. Maybe the attacker is an employee intent on taking property, such as laptops, and knowing that the security team is focused on a VIP or perhaps a training session, creates the ideal conditions for the theft. What information are you unwittingly providing your adversaries?

Closed Source Data

Closed sources are those which are essentially "non-public" and include information found in any government classification system for information that forbids general distribution, other restricted government records, proprietary information that must be obtained through deceit or misdirection. Information concerning on-going law enforcement investigations, military preparedness, national security issues, and so on may be found in this category. In the corporate sector, this information includes marketing strategies, accounting and finance records, network access information, individual salary information, and any other records that a company would not want publicly available. Obtaining closed source information typically requires that the information be discovered either from persons divulging it or through the review of records (legally or otherwise). Technical methods including electronic eavesdropping and network "sniffing" create greater opportunities for divulging information remotely. Thus the data is either obtained through a person that knows the information or it is acquired after a computer network is penetrated, or obtained through non-technical means such as recovering it from an organization's refuse. Closed sources in law enforcement include the National Crime Information Computer (NCIC), various regional crime reporting networks, their internal files and reports, fingerprint identification databases, and informant networks. In many instances, the informant and undercover officers provide the greatest volume of intelligence on specific issues.

Both law enforcement and private protective operations enjoy field and organizational activity reports. Granted these will generally look very different, but their use is the same. Whether a field agent is a security officer or police officer makes little difference in the fact that they will both generate reports about their activities. Their observations may be important pieces of information, and these sources should be included in the information review process. Moreover, in a business environment there are usually many different types of activity reports from marketing research and service staff interactions to call logs and firewall logs. Information obtained for the organization, and within your collection means, is fair game. If it applies to your efforts, use it.

Many times information obtained through closed sources is classified by the specific source the data was gathered from. A few examples of intelligence source terms include:

- Human Intelligence – (HUMINT) obtained from people often as a result of a ruse other misdirection. People provide information based on their observations and conversations. Their motives are many and varied from revenge to whistleblowing. This information may be little more than an anonymous tip or it may be a very detailed report depending on who is providing it. A tipster may not want to be known and therefore will avoid identification, but an undercover operative is expected to provide a report detailing their efforts. It is not the nature, demeanor or motive of the person providing the data but the manner in which it is obtained that defines Humint.

- Signal Intelligence – (SIGINT) this may include radio frequency (RF), microwave, cellular phone, and even computer network traffic when obtained directly from the electronic system. This could be obtained through a radio scanner, TEMPEST attack, or a network sniffer. It can be monitored live or captured for later review. SIGINT has many sub-disciplines including Communications Intelligence (COMINT),

Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT),

- Imagery Intelligence – (IMINT) Imagery includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics (OSITH, 1996).

It is very easy to believe that only government entities will have access to closed sources, although this is not accurate. Closed sources are those sources not available to the public. In addition to government entities, think tanks, defense contractors, and private firms doing business directly with the government might be given limited access to government closed source information. Because closed source information is information that is not available to the public, there is a considerable amount of information within private sector organizations that is also not available to the pubic. Government agencies, in turn, will not normally have access to these closed sources, unless of course, there is a statutory reporting requirement. Consequently, there is often a very real opportunity to develop a partnership to assist both in meeting their protection goals.

Hidden in Plain Sight

The news media regularly reports that international terrorists use coded messages through public websites for communications. We hear of computer programs hiding data within image pixels and artists that have concealed text within their artwork. Computer experts regularly assail us with the importance of encrypting our files. We learn that dissidents have secretly gotten word to friends by concealing it in a letter. Who could have guessed that phrases in World War II like, “It is hot in Suez; The dice are on the table,” (Edmonston, 2002) informed the French resistance and undercover agents that an assault was coming. These are all examples of information concealed in plain sight. There are several commonly discussed ways to do this. Encoding, encrypting, covert channels and steganography are a few we will discuss. These methods are similar in that it usually requires some sort of code key to decode and understand the information being communicated.

Creating codes for communicating information without sharing it unnecessarily is quite possibly the most common form of protected communication. We learn to do it as children by developing secret messages with our friends. The simplest form might be the statement, “Meet me at the usual place.” Who else knows where this is? Security and law enforcement, among others, use radio 10-codes and duress phrases to communicate specific information. True duress words or phrases allow us to signal the need for immediate assistance without informing our adversary that help is on the way, or that we requested it. The more outlandish the code the less likely an eavesdropper will be able to understand the message. However, the more often it is used then the more likely it will be broken. Duress codes are good examples since they are almost never used, and so they are not readily recognized. In addition, a good duress code is hidden in the form of a normal message. On the other hand, when we use a code word on a regular basis then it becomes known over time. To make things more complicated, there may be several similar codes that are rotated on a daily, weekly, or monthly basis, to make decoding even more difficult.

Ciphers have been around for many years and, until the spread of the Internet, they were most commonly associated with government communications. Scrambled or secure phones were once almost exclusive to governments. But with the Internet data traffic has become something everyone uses, knowingly or otherwise. Simply put, messages are encrypted using a cipher, which alters the message in some predetermined manner so that someone unaware of the method used for changing the message cannot change it back to a readable format. Put more technically, a message is encrypted by way of a mathematical algorithm using a controlled factor, or key, so that the resulting message is unreadable until the message is decrypted with the cipher key. A person not possessing the key is unable, in theory, to decipher the message. Although, there are variations on this process, including the private key and the public key methods, what is important to know is that a cipher is composed of an algorithm and a key or a set of keys. Algorithms are typically publicly known and cipher keys, or just keys, are not. The algorithms are constructed to be mathematically strong enough to prevent "brute force" attacks, or simply trying every key combination until the cipher is broken. What is even more important is that although a message may be secure and unreadable its existence may be publicly known, or at least known to an attacker with access. As a result, a covert channel may be created by the very existence of the encrypted message traffic. Encryption requires resources to encrypt and decrypt messages in a timely fashion; therefore in most instances only important messages are encrypted. This in turn creates a covert channel, and an eavesdropper now knows to record or capture that specific traffic for later analysis. Encryption is an important tool in protected communications, but it is not an end unto itself but one means towards end. When dealing with encrypted information it may be worthwhile to store captured messages until they can be deciphered later when a key is obtained. Or, resources permitting, a brute force attack can be mounted against the captured message until the key is discovered.

Sending an undetectable message within a data stream in any communications medium is the essence of a Covert channel. Specifically a covert channel is a communication channel that may be exploited to transfer information in such a way as to violate the communication system's security policy. Arguably this could include many different concepts. The duress codes discussed earlier, if embedded in an innocuous message, may qualify, however covert channels are normally discussed in the context of electronic systems. As a result it is far too easy for this discussion to become extremely technical. There is much information on the topic and even a book structured around a fictional scenario entitled, "Hacking a Terror Network," by Russ Rogers, from Syngress. There are two important questions to ask yourself and your team in regards to covert channels. What are you communicating unintentionally to your adversaries? And, what potential sources of information are available from your adversaries either through their intentional or unintentional activities?

Steganography, a specific intentional covert channel method, is the concept of concealed writing. Specifically, it is the art and science of hiding information by embedding messages within other, seemingly harmless messages (Steganography, 2004). It can be found in cultures throughout history and its study is fascinating in itself. Consider passing a message, picture or diagram with a message hidden in such a way that it will not be detected except by the person it is intended. Such a method provides an easy cover and a defense from accusations when engaged in espionage activities. In today's electronic world it involved the replacement of specific bits of data with the desired information. In the past, information may be microdotted or microprinted, where the printing is reduced to appear as a dot or line, and today it can be embedded into nearly

any sort of electronic file for a computer. The messages are literally in plain site, but made to appear as a feature of the document or data file. Just conducting a few searches of the World Wide Web for steganography will yield a large volume of examples.

Need to know, Right to know, and Third-party information sharing

Intelligence of all forms should be controlled to ensure that it is disclosed only to the appropriate individuals. Though some reports may not contain any information that may be detrimental if revealed unnecessarily, the report itself will provide insight into your organization's capabilities. Consequently, all collected data, processing information and analysis reports should be carefully controlled. Documented procedures should exist to specify what is disseminated, to whom it is disseminated, in what format it may be disseminated, who has the authority to make alterations to the dissemination lists and formats, and who is responsible for ensuring procedural compliance. Essential to this aspect of controlled dissemination are the concepts of Need-to-know, Right-to-know, and Third party information sharing.

Whenever a person's job or duties require access to intelligence products to be effective they may be considered to have a Need-to-know. Need-to-know applies in many situations; for our purposes information that falls under Need-to-Know if the analyst that requires the information would fail at his/her task without it. If this were the only consideration in determining who should receive intelligence products then it would simplify things. They need it so they get it, but it is not so simple. In some instances persons may benefit from the information but they are not allowed to receive it because they do not have a Right-to-know. By Right-to-know, the analyst would likely need the information, but if the analyst knew how the information was obtained it might corrupt his research, thereby wasting already limited resources. This could be due to how the information was obtained or how the information is presented. If this is an issue then it may be possible to develop a modified version of the product that either conceals how information was obtained or presents it an acceptable fashion. "Sanitizing" a document involves removing any information that is not to be disseminated. This diluted version of the report is frequently sufficient for the receiving individuals to fulfill their duties while protecting the collection and analysis process. It may also involve substituting code words and phrases for specific pieces of information in such a way as to make the document more difficult to understand by a casual observer.

Information sharing among organizations is an effective method of augmenting the intelligence apparatus; however it must come with a very high level of trust. In the government sector, inappropriately shared information could jeopardize the lives of officers, agents and informants. Such extreme threats could occur in the private sector but more commonly it may result in the loss of client trust or industry black-listing. This trust should ALWAYS come in the form of written agreement, Letter of Understanding or formal contract between the two parties that may share information. In some instances within the private sector reports are transmitted between attorneys to receive the protection afforded the privileged quality of Attorney Work Product. To further protect such an agreement it should include provisions routinely known as the Third Party or Third Agency Rule. The common form of this rule states that an organization may not share information received by another without their specific permission. This protection can have some far reaching implications but is absolutely necessary to preserve some control over the

information after it has left your organization. Simply put, make sure all of your agreements are in writing and your employees can be held accountable for any unauthorized disclosures.

It is also important to recognize that even a product developed entirely from open sources should be controlled. There are two specific reasons for this. Firstly, the product contains the results of an analysis. The information obtained during the research may be obtainable by anyone, but the analysis is not. Furthermore, just the compilation of the information represents a considerable amount of effort whose value should not be underestimated. Secondly, the report describes your intelligence capabilities and their understanding of the situational environment. Making an adversary aware of this may provide additional opportunities that would not have existed without the report. Do not underestimate the value of your products to either your organization or any adversaries.

Data Collection

How do I get the information, you ask? Your imagination is the limit, with a few legal constraints, and of course your own ethical standards. Violating the law while collecting data does not "make the report better," instead it unnecessarily places yourself and your organization in danger of both criminal and civil actions. Furthermore, sacrificing, bending, or making exceptions, even "just this once," in regards to your ethical standards is a slippery slope. Set your standards and hold fast. This cannot be stressed enough early in the discussion on collecting data. If it's in the public domain, it's yours, otherwise stand by your beliefs and any applicable laws.

In the realm of private security operations the first step generally is to establish what assets you are responsible for protecting. Within the role of intelligence, this plays into understanding yourself to better understand your adversary. Be aware of your organization's own weaknesses, and recognize that whatever you are doing to someone else, they may very well be doing right back at you. Know what assets your organization is protecting and how they are being protected to better understand where an adversary may direct their intelligence efforts. Now, put on your "Black Hat" or join the "Red Team," whichever you prefer, and begin considering how YOU, with perfect intelligence of your organization's assets and protection programs, would target your own organization. From this you should develop some worst case scenarios, and they should make you sweat. Ultimately, this is what you will be developing intelligence to avoid! Who would do it, how would they do it, and most importantly when and with what resources will they do it! By devising ways to penetrate your own organization, you will learn where best to apply your resources and/or staffing allocation.

Prior to collecting any data, it is essential to define adversaries, or targets. Otherwise, how would you know what data to collect? This is not to say that it is necessary to specifically identify adversaries at this point, but it is important to define what constitutes an adversary, or target. For instance, an adversary may be defined as, "any entity that attempts to disrupt client operations by other than fair market means." This is pretty broad, even for an example, but it is important to show that adversaries must be defined in order to direct collection efforts. This example excludes competitors involved in routine market activities, but not sabotage or economic espionage. Adversaries represent threats to your organization, but it is important to understand what constitutes a threat. A common equation to define a threat is:

Threat = Capability * Intent [7]

There may be some debate over this equation, but it is useful. Without intent an individual or organization is not a threat, but they could become one if their motives and drives changed. Without the capability to carry out a specific action an organization cannot be considered a threat, but it is possibly, even likely that they are seeking such a capability. And the difference is? Lead-time to successfully carrying out an action based on the amount of time needed to alter their motives or to develop a capability. In other words, even though they may not pose an imminent threat, they may still be adversaries worthy of your attention.

Now, identify specific types of information that will be the focus of the collection effort. Answer these questions:

What do we currently know?
What don't we know?
What do we need to know?
What would we like to know?

Does this sound similar to an investigation? This creates a hierarchy of information and a wish list. The hierarchy becomes useful later in the process as information is broken into components for easier collection. We will address data components shortly. The wish list, or "what we would like to know," assists when collection methods go exceptionally well. A good example is a pretext telephone call during which the target individual gets so comfortable on the call that they begin revealing greater and greater amounts of information.

Separate the desired information into its component parts. Many times information that is considered to be non-public can be re-created when several, or all, of the components have been made public separately. This one step may significantly limit the amount of non-public, or slightly obfuscated information that must be gathered. Using the hierarchy of information, divided into data components, determine the population size of individuals that may have access to each component. You now have a list of information sought, who may have it, and a several potential combinations of ways to acquire the targeted whole by collecting the components. Focusing on components also works to protect any sources that are developed since many individuals may have access to different components but only one person may have access to the whole (Cooper, 1996).

As noted previously it is essential to learn the systems that are available within your organization for collecting data. Common examples might be Web research, other online research, media subscriptions, network news, field reports, informant contact reports, interviews, and internal and pertinent activity reports. The latter being any internal information reporting system within your organization. This may be lookout information or crime reporting information within a law enforcement agency, or receptionist telephone logs and IT network activity logs in a private entity. Effectively exploiting all available information sources is the best way to creating insightful and worthwhile intelligence products.

Open Source Collections

Collecting open source information is relatively straightforward. Either you collect it actively or passively. The difference between the two is you level of continued effort. Active research includes entering search criteria into a search engine, reading through articles in print media, or making "open cover" telephone calls. With active research, the researcher must enter search criteria and review the results, or dial a phone number to determine if it is a voice or data line. It is custom research by nature and can be as flexible and directed as is necessary. Although this flexibility is an advantage in many situations, it takes a greater amount of time.

Passive research, on the other hand, is conducted using automated processes, with some offered free of charge. Using refined, relatively focused search criteria with an automated process provides useful results with minimal "noise." The key here is *refined* search criteria. Although the process may be automated, truly intelligent search applications can get expensive, so the less expensive (or free) applications require a little more front-end effort obtain the same results. The basic service is typically a "news alert" offered by a search engine with varying amounts of customization, and at the high end are either pay access media databases offering intelligent agent features or a local software application that crawls the web, or any other designated network, in search of matching data. Other useful passive research tools are Website and Web log (Blog) monitors. These applications will monitor specific websites or Blogs and give notification when the content of the site changes. Such applications, some of which are free, let a researcher keep tabs on many websites and Blogs without spending time conducting routine reviews of their content.

Some of the most common collection methods include:

- Web searches – This is simply entering criteria into a search engine and sifting through the results. Well constructed search criteria will result in less "noise" being returned in the search. It may allow the researcher to discover data that an automated process would have overlooked, however it is time consuming.

- Online media research – These are distinguished from basic web searches because these database services will offer content not generally available on the web. These pay access databases may use a web browser interface for convenience but they usually offer extensive search, collection and storage features, and they will catalog media sources that are not found on the web. Services like Factiva or Lexis-Nexis will search through over 3,000 media publications.

- Consumer Information databases – These databases are also pay access and provide number of services ranging from Social Security Number verification, address histories, neighborhood demographics, criminal database searches, and so on. Providers such as Choicepoint and IRB have an ever expanding amount of data. Be aware that there is no guarantee on the accuracy of the data within the database. Errors, omissions and timeliness are factors that affect these services.

- Internal data searches – Mining data from your organization's own information can often provide unexpected results. Many tools exist for this; some bundled with Windows, and others available on the web.

- Print media review – Arguably the last choice if the information is available in an electronic format. This process is slow and painstaking, but some publications just are not available online or in a database. If your research includes underground groups of any king, you can count on at least some print media review in your efforts.

- Telephone calls – These calls would be for information that is already publicly available. This may be information available at local libraries (but not local to you), requests for investor information, or directions to a location. Keep in mind that this information is increasingly available on the Internet.

Regardless of whether the effort is passive or active, the skill necessary for effective online research is the ability to create and refine effective search criteria. Criteria development is the process of determining what pieces of data the search engine/utility should match within the search location. The typical search location is the World Wide Web, however other locations may be used to refine or expedite a search. The search criteria is composed of search elements that contain terms and operators. Search elements include the terms the researcher wishes to appear within their designated search location. These terms may be restricted using operators such as "or," "and," "not," as well as a variety of others. Some search utilities utilize Boolean operators while others do not. It is important to develop expertise with the search tools used within the utilities employed by you and your organization. The available operators are often found by looking for an "advanced tools" link, help, or in a user manual.

The Search Criteria development process should start with at least one test search using broad criteria. Subsequent test searches should seek to refine the results until the greatest amount of excess returned data (or noise) is eliminated. Further test searches may be conducted using slightly broader Criteria to ensure pertinent data has not been missed unnecessarily over time.

Sample Search Criteria

Miami AND *(Florida* OR FL) AND (*[client name]* OR *[protected site name]*) AND

(*crime* OR *robbery* OR *burglary* OR *arson* OR *theft* OR *larceny* OR *murder* OR *homicide* OR *suicide OR Assault OR Battery*) AND (*"store name"* OR "*shopping center name*")

In this example, parenthesis are used for grouping terms into grand elements that are acted upon as one element by the "AND" and "OR" operators.

Each search ELEMENT has been underlined and each search TERM has been italicized.

As shown above, operators may either be part of elements or used to separate them.

The sample search criteria may have begun simply as, "(Miami) AND ((Florida OR FL) AND crime). The volume of return from this criterion would be extensive and consequently valuable information will be buried. Refining the search criteria reduces the amount of wasted research time.

Another important point concerning the collection of open source data, particularly from the World Wide Web, is the likelihood that data may change or become unavailable. Consequently, this requires the individual collecting the data to archive or make original copies of the data. This may be in a hardcopy printed format, or in a locally stored electronic format. Web pages, emails, message boards, and other electronic media may be saved in their entirety or printed out to ensure the availability of the data. The ideal storage or archive format will provide a searchable index or database that provides a rapid means of retrieval for assisting all collation and analysis efforts in your organization. Furthermore, additional tools are available that monitor specific websites for content changes. Such a tool offers two useful features: on the front end the analyst no longer needs to visit the website to determine whether the available information has changed, and once a notification is made that a change has occurred and the new website is saved locally, the analyst should have an easier time finding the changes. Comparing the old and new versions may provide worthwhile clues concerning changes in tactical/strategic direction, removal of information accidentally placed in public access, and level of activity and attentiveness to their web content.

Open Source Collection Exercises

1. Conduct a search of you own name. Try slightly different search criteria beginning with just your name (john jones). Followed by your name in quotations ("john jones"). Then try other variations with initials, middle names, and different quotation positions. Keep track of your search results with notes and comments.

2. Try opening a word processing document and copy and pasting the IP address of the search results into the document. Make it a hyperlink and you can always return to current results for that search criteria.

3. Try each of theses searches in different search engines. Try Google, Teoma, Yahoo, MSN, and Dogpile. Try searching for the criteria, "search engine". (www.google.com, www.msn.com, www.teoma.com, www.yahoo.com, www.dogpile.com)

4. Now try conducting searches with a topic of your interest. Try using someone else's name. Consider an obscure event in history, or pick a name at random to see if someone with that name is on the web.

5. Use the information gained in the searches in #4 to refine the search criteria until you are receiving information nearly entirely for the target of your search.

Closed Source Collections

Private, covert or otherwise non-public information sources exist in a wide variety. Consequently, this extremely broad topic will be broken into three primary categories using the source of the collection authority. The source of the authority for collections is important for considering Law Enforcement and National Security intelligence by dividing all activity into Court Action and Non-court Action, or in other words whether a warrant or other legal decree is used to preempt constitutional protections for accumulating the data. With a few exceptions, private security personnel will not be involved in accumulating intelligence from court actions. Not to fret, though, this sort of intelligence is arguably of greatest value in dealing with crime and national security issues. Furthermore, we will also include subdivisions of legal and illegal methods under the Non-court Action heading. Non-court Action collections may be undertaken by either public or private entities and can either be legal or illegal.

Court Action collections are typically used for developing information in furthering an investigation. Warrants and other court orders permit government agencies to deprive individuals of some of their constitutional protections including property, privacy, and of course liberty in the case of detentions. Since a warrant normally requires that "probable cause" be established before it is issued, the threshold for already developed information is relatively high for substantiating the need for the warrant. An issuing authority, such as judge or magistrate, must believe that there is sufficient information to believe that executing the warrant and depriving the individual of their rights will result in gaining necessary evidence in an investigation. With that said, Court Actions may include activities like intercepting telephonic information including conversations, phone numbers involved and the corresponding information. With the internet we now have traffic captures in which streams of data packets are captured for review. There may also be document seizures including bank records, propaganda materials, and other items material to a crime. Court-action collections are significant in that they provide needed information for an ongoing investigation, but once the information is collected it may be relevant to other investigations, or provide data used to develop intelligence that ultimately directs another investigation. It should also be recognized that, with some exceptions, Court-action collections are legal, in that a duly constituted authority has given permission for impinging on an individual's legal rights. Most methods that can be accomplished legally under a court action can also be accomplished illegally. Understanding this fact should be of interest to anyone responsible for the protection of an organization so that appropriate countermeasures are implemented.

Non-court action collections include many of the same methods found in Court Action collections. This is significant since a Court Action is required for a government agency to infringe on an individual's constitutional protections, while in many cases a private agency is not legally prevented employing such methods. For instance, government agencies are required, in the U.S., to establish a predicate of crime before collecting specific information concerning an individual. And if that predicate should not prove out then the information may no longer be retained. A private organization, however, is not prevented from collecting data concerning an individual it considers a threat, or hiring private investigators to monitor their activities. This could become a harassment issue at a later time, but simply collecting publicly available information is permitted without court permission. Legal collections may include monitoring an online discussion forum, conducting pretext telephone calls for eliciting information, conducting

undercover operations, or "dumpster diving." Although it should be noted, some legal restrictions apply to all of these activities in the U.S. For instance, it is illegal to misrepresent yourself to a financial institution or a law enforcement agency. This is not to say that these methods are not still used, but they are illegal and their disclosure could ultimately result in criminal legal actions. Again it is important to establish in advance policies for the use of various collection methods and have these reviewed by legal counsel prior to actively conducting collection efforts.

Recognizing that information may be collected legally or illegally using the same method under different circumstances is important to avoiding incurring criminal penalties or civil remedies. So to better describe the non-public collection methods we have divided them into Electronic, Infiltration, and Direct Collections. Each of these will include some Court Actions and Non-court Actions of both the legal and illegal persuasion. The divisions represent differing amounts of personal interactions with targets, varying levels of potential personal threat, and data reliability.[8]

Electronic Collections

Electronic collections offer greater personal distance from targets along with the most reliable raw data. This raw data is collected directly from the target as they interact with their employees, agents, comrades, friends, and vendors. Electronic collections may include:

- Telephonic eavesdropping – Often referred to as "tapping the line," this method may provide considerable information concerning the plans, capabilities and co-conspirators of the target. This involves intercepting the signal from one, or more, telephone units or service points and either monitoring it as it happens (live) or recording it for later review and presentation.

- Telephone "Trap and Trace" and "Pen Registers" – These establish who is calling a specific number and which numbers are being called. Significant information may be developed by knowing who is calling whom. Times of calls and the length of each call can assist in placing individuals at specific locations, and potentially identify co-conspirators.

- Traffic Capture – Network traffic "sniffing" allows the sniffer to observe data packet traffic as it crosses a designated point in a network. Packets are then captured for review. The capture can be covert in which copies of the packets are made and the original sent on to its destination or it may interdict the traffic and simply take the packets. This is most easily accomplished on today's wireless networks, legally or illegally.

- Cellular Telephone Activity Logs – These are the cellular equivalent of legacy phone line pen registers and trap and traces.

It is not difficult to recognize the legality of this sort of activity or the need for proper authorization. But, authorization may not necessarily come in the form of a Court Action. Many organizations maintain an electronic usage policy that permits the employer to observe or

eavesdrop on the activities of their employees when they are using company-owned or maintained equipment and services. How many automated voice prompts are heard that state that conversations may be monitored or recorded for customer service. An agreement exists when the caller stays on the line. In the United States each state has their own laws concerning the recording of voice conversations. States are generally referred to as a "one-party" or a "two-party" state. A "one-party" state only requires that one party consent that a conversation be recorded, while a "two-party," better described as an "all-party" state, requires that everyone in a conversation consent to the recording. The only limitation on "one-party" consent is that the one party be a part of the conversation. Thus recording a conversation without being a party to it is still illegal. This can easily become a problem while conducting covert video surveillance. Electronic collections provide some of most reliable data, often directly from the target, with minimal risk of detection. The one caveat to this statement is *IF* the target somehow discovers that their communications have been compromised. In this event, this method may have the greatest amount of risk since disinformation may be provided to draw resources into useless or illegal action. Simply put, don't get overconfident about the reliability of your source.

Infiltration Collections

As the name implies, these methods require some type of movement "behind enemy lines" into an environment in which the operator, or person seeking the information and possibly developing an informant, has little or no control. The researcher, operative, or whatever name they work under is often at greatest risk using these methods. Informants can turn and lead the operative into a trap, their cover can be exposed during undercover operations, and a savvy person receiving a pretext call may "reverse engineer" it to gain information about the caller. Electronic infiltration requires that a person actively move through a target network, exposing themselves to backtracing and identification. This is not to say that every undercover activity or network intrusion carries such severe risk, but some do. The reliability of the information obtained here varies since the actual source is likely to be someone other than the specific target. The target of a pretext may present dated or biased information, and informants may be more interested in their reward than the accuracy of their product.

A key concern in developing an infiltration plan is to determine the lifetime of the effort. This determines how many times intrusions or contacts must be made. If the lifetime is indeterminate then any individual cover identities, online aliases, phone numbers, addresses, should be durable. Durability of a cover identity describes the level of scrutiny that the identity can withstand before they begin to break down. Identities will generally be classified under roughly four categories[9]. Each organization will have different methods of classifying their cover identities, and some will not be applicable at all to some organizations. These types of cover identities may include:

> ***Online Alias*** – The Internet has brought us many new phenomena including extensive online, and worldwide, communication and conversation mediums. The online alias cover allows information gathering without exposing the researcher or their organization. Varying degrees of protection may go into such an alias including the use of open proxy servers, separate broadband access, and spoofed MAC addresses. Some services that support anonymous Internet activity are offered free of charge.

Tactical – A tactical cover is meant to be used only for an extremely short period of time; for instance to get out of a tight situation. It will sound plausible but generally will not stand up to any scrutiny. Negotiators may use such ruse information or persons attempting to exit a facility quickly, for which they are not authorized to be in. Although they may seem to be "off the cuff" they should be created ahead of time and tailored to specific situations with a maximum of unverifiable information.

Short, intermediate, and long-term – These covers will stand up to varying levels of scrutiny. The quality of the cover is built for the length of the operation and should include an exit plan. The cover may leave the city, state, or country, but the event should be relatively unverifiable. A short term cover may include disconnected phone numbers or cell phones and no true address, while a long-term cover may include a true false identity with an occupied address, working phone and verifiable contacts.

Legends – Nearly every spy novel discusses the Legend or extremely long-term cover. A true legend will stand up to extensive scrutiny and may be based on a living person that is in a safe location. The term Legend is also often used as slang to describe any strong cover.

Infiltration is, as defined by Princeton University's WordNet (2003):

1. a process in which individuals (or small groups) penetrate an area (especially the military penetration of enemy positions without detection)

2. the slow passage of a liquid through a filtering medium; "the percolation of rainwater through the soil"; "the infiltration of seawater through the lava"

Infiltration efforts may be either sudden and seemingly aggressive or slow and insidious. Neither is best suited to all situations, and so each infiltration should be carefully planned and orchestrated to ensure that the objective is met. The objective of any infiltration method is to gain access undetected or in such a way that once discovered the discovery no longer matters. In some instances, those conducting operations of National Security overseas will violate local laws for any number of reasons. As some of those methods are discussed here, their uses will primarily be confined to domestic intelligence as required by law enforcement and private protection teams. Below are a few commonly thought of infiltration methods:

- **Undercover operations (UC)** – Modern folklore provides many examples of undercover activity. This is commonly used by law enforcement for gaining access to drug and other organized crime operations. In private investigations UC operations are often conducted to identify employee misconduct, such as theft and sabotage. On the other hand, Eco-activists will get hired into companies to observe, document and report on animal research and mistreatment. UC operations may last a few days or months, and in some instances years depending on the objective and available resources.

- **Informants/Sources** – Developing informants and information sources within organizations can be an exceptional means of acquiring valuable information.

Information obtained this way should be treated very carefully since in some cases acting on it indiscriminately could compromise, or "burn," the informant which could put them at risk or simply ruin their access to information. It may be prudent to use their information to develop a creative means for achieving your goal. Informants may provide information for many reasons, commonly referred to as their motivation, including:

- Vanity
- Civic-mindedness
- Fear
- Repentance
- Avoidance of Punishment
- Gratitude or Gain
- Competition
- Revenge
- Jealousy
- Remuneration (O'Hara, 1994).

- **Social Engineering** – Also known as Pretexts or ruses, involve conversing with persons to accomplish a goal. The term has gained relatively recent popularity within Hacker/Cracker communities as a method for gaining or expanding network access. Social engineering can be as simple as convincing someone on the other end of the phone to provide employee names and internal phone extensions or as complex as working through several individuals to have them provide you with internal documentation or other services. The following are some methods used by those engaging in Social Engineering.

- **Phone calls** – Probably the most common forms of Social Engineering deal with the phone. This is simply because using the phone lowers the immediate risk to the engineer. They can simply hang up and walk away if they are discovered, or create a new ruse and try again. Telephone calls can be exceptionally dangerous to the target since they will ultimately have limited means of discovering the identity of their attacker. Although Caller ID services provide some protection against the least capable Social Engineers.

- **Interviews** – Pretext interviews, or conversations, are pre-arranged meetings for whatever the pretext reason might be, and this is quite often somewhat different from the information that is sought. For instance, a job interview may be attended by a person seeking information concerning an organization, or a vendor may do the same. It would not be too surprising for a "fire suppression" vendor to obtain a tour of a facility in order to learn valuable information about the IT department. After all, while standing in the server room it would not be at all inappropriate to ask how many servers need to be protected or what protective measures have been taken. Perhaps further discussion of the "confusing types of operating systems out there" – what are they and what are you using here? Interviews are risky for the engineer since they must expose themselves personally to being identified, and in the wrong environment detained.

- **Chance meetings** – The "Change Meeting" is anything but that! It is typically planned around a known event in the "mark" or target's life, commonly known as habits. A person may buy a newspaper out of a machine every morning, so the machine is emptied ahead of time with just one paper left, and the engineer happens to get to the machine just before the target. A conversation ensues, rapport is built, and at some point in the future, information is obtained.

- **Network interaction** – Here is the most common use of on line aliases. Using this method, a researcher may gain valuable insight into organizations or an individual's existence. People tend to believe what they are being "told" online, and even enjoy a little embellishment, but still believe the underlying purpose of the interaction. As a result, it is possible to gain a person or organization's confidence and begin obtaining information. This is different than open source collections through online discussion groups in that this method has the researcher actively interacting with the target. This is anything but passive, the intent is to develop online rapport and trust to gain information or get into the "inner circle."

- **Unauthorized Network Access** – In other words, hacking, in all its shapes and manners. This is the art of gaining access to a target network without the permission of the owner. It can be done entirely technically, or with a little physical infiltration to assist in the process. One example of this would be for a person visiting the facility to attach a "rogue" wireless access device to the network. A purely technical hack intrusion would be to gain access from the Internet through a firewall or router as a result of software vulnerabilities. Being inside the network is akin to being inside a building, some doors will still be locked, but much of the information will be accessible by one means or another.

- **Physical Break-ins** – As the name implies, this is actually entering a facility, hotel room, office, or some other location by defeating the access control devices to search for and obtain data within. Picking a lock, tricking an alarm system, or just breaking a window to gain access are all forms of this method. Clearly this would ordinarily be against the law and so should not be considered without special permission or court order.

- **Surreptitious Entry** – This is the epitome of infiltration – Entering a facility during business hours and moving amongst the employees to obtain information. Many workplaces do not have strong access controls and so during normal business hours it may be rather easy to do this. Depending on the circumstances, signage and local laws this may not be illegal.

As this list shows there are many basic ways to infiltrate a group or the trust of an individual. The ethical and legal concerns to each may seem straightforward; however the line can be made hazy. Consider this: While involved in something else, the investigator turns on their laptop and discovers a wireless network, configured for open access, which is part of an organization for which collection efforts have been initiated. This is the electronic equivalent of shouting in public. Laws aside, knowing that the traffic can be captured for later analysis, do you do it? Certainly it is possible to keep this information out of any analysis, or to use it to find another

means for discovering the information. The answer is… It depends. It depends on who you are working for and under what constraints you are working, legal and ethical. That would be those pesky guidelines that were developed prior to the collection process. Setting internal constraints early that comply with legal and customer requirements is essential to avoiding later dilemmas, and, of course, potential criminal or civil litigation. If a meeting or discussion group is successfully infiltrated then remember that the goal is to collect data. It is *NOT* to actively subvert the target organization's efforts. In some cases this is illegal, otherwise it is simply inappropriate. Even worse, it is also *NOT* appropriate to become an "agent provocateur" to encourage illegal or inappropriate activity to get the group members arrested.

Direct Collections

Our final classification of collection methods has to do with everything that has not been considered so far. Direct collections are not done using an undercover identity, or an online alias, and they are not done at a distance. These collections of conducted in relatively controlled environments but use information resources that are not generally available to the public. Here are some Direct Collection methods:

- **Warrant searches and seizures –** This is primarily used by Law Enforcement and includes all information or items obtained as a result of a search warrant. Documents, drugs, weapons, stolen credit cards, counterfeiting equipment, and any other criminal tools. The warrants will typically be for an investigation, but the information obtained can be of great use to the intelligence team.

- **Warrant-less searches** – Also known as consent searches are conducted by both law enforcement and security personnel. This is simply any search conducted with the consent of the person being searched or the owner of the property being searched.

- **Prisoner/detainee interviews –** Persons being held legally, for whatever reason, can offer considerable information. Many times this information is obtained without their knowledge. The information obtained may include known modus operandi, identifying other criminals, after theft markets, counter-detection methods employed, and so on.

- **Dumpster Diving –** This could very well be placed under the Infiltration heading, however it more appropriately resides here. Reviewing a target's garbage can yield incredible amounts of data in many formats. It should come as no surprise that in addition to documents there may be CD's and other forms of removable storage that have been discarded. Of significant note here is that any local laws must be followed, especially those pertaining to trespassing and theft. Typically that means the trash may only be taken if it is no longer on private property. Otherwise, it may be necessary to contact the target's refuse vendor and offer to purchase the trash. So long as there is not a clause preventing this in the target's contract, the vendor can normally dispose of the refuse as they see fit. And this includes selling it. Data that can be found in dumpsters include passwords, source code, system architecture maps, financial statements, internal phone books, general work papers and internal procedures manuals.

- **Field Reports –** Whether in law enforcement or security, there are often reports that are created by officers as they go about their duties. These may include suspicious activity reports, be on the lookout (BOLO) reports, incident reports, and so on.

- **Field officer/agent interviews –** On some occasions, informal interviews may be conducted by field personnel but will not generate reports. This information may be of even greater value due to its timeliness. These contacts should be documented.

- **Internal Document Review –** Reviewing all sources of internal information should not be overlooked or underemphasized. Get to know as many of the various types of data that are maintained in your organization or through regional sharing agreements.

- **Personal Network** – Don't forget any contacts that you may have within the security and law enforcement industry. If you don't have any, then shame on you and go build a network. Network with your peers for information; they will do the same to you and a little cooperation sometimes goes a long way.

- **"Covert Channel" observations –** Covert channels are communication paths that violate communication system security policy, and may be used to provide information deliberately or unintentionally. For instance, the press has reportedly monitored late night food deliveries to The Pentagon as an indicator of current or impending military operations. Another example, effectively used by law enforcement, is the significantly increased electric bills that marijuana growers incur from the use of their indoor lighting systems. Each of these transmit information unintentionally. But, other methods, such as steganography, are used to embed messages within other data streams. If an unintentional covert channel exists for whatever your target is, then it can certainly assist in reducing research time.

These are only a few methods for closed source information collection. The dilemma of closed source collections in arenas other than for national security is the ethicality of the effort. Be certain of the legality and your own standards of ethical behavior before using a particular method. Furthermore, it is exceptionally important to consider where the information will go and who will use it. Information not available to the public should be protected to prevent inappropriate releases. Be certain that all individuals have completed any appropriate documents and agreements, such as Non-disclosure Agreements (NDA) and Third-party Sharing Agreements. Establish who is authorized to receive any interim or completed reports before they are needed. Do not deviate from this authorized distribution list without written approval. If your report is to go to an attorney for additional protections then only send it to the attorney and allow them to distribute it further.

Closed Source Collection Exercises

1. Begin a list of potential information sources within your organization. Begin is the right term because the list will grow and change as your skills get stronger and your collection efforts get more refined.

2. Speak with different departments within your organization, formally or casually, and learn what types of information they obtain, generate or compile. Consider and make notes as to how your efforts may benefit them. Use both information from line employees and managers as their information-generating capabilities will probably differ.

3. Select a few random field activity reports, from different authors if possible, and consider all of the information that it contains. Also consider what information is omitted within the context of the report. Make lists of your findings.

4. Now determine how you can find the omitted information. Where might this be available? Is there more than one way to find this information? Is it an open or closed source?

5. With the approval of your management, call your organization and attempt to obtain information that would not normally be public. Try several approaches and different persons. Make your pretexts or ruses plausible and believable. Report your findings to management. How vulnerable do you consider your organization to such "mild" Social Engineering efforts.

   Try opening a word processing document and copy and pasting the IP address of the search results into the document. Make it a link and you can always return to the current results for that search criteria. But do not forget that as websites change so will the search results. Maintain a copy of all data that you do not wish to lose access to.

Analysis – Getting the most out of the information

Once the information has been collected it must be analyzed. Analysis can be defined as separating something into its various parts for individual study. It is, however for the sake of intelligence, the process of taking the collected information and determining its nature, any correlations, links, similarities, or other relationships. This can be accomplished through several methods and there are a growing number of analytical software tools that provide faster processing of the information. This is not to say that software is needed to be successful. Keep in mind that intelligence operations have been around much longer than the computer. However the amount of data that may be involved in any one collection effort may make manual processing difficult at best. We will look at some of these concepts and tools.

As you may suspect it is not always possible to know that the proper information has been found, so there will be a bit of loop. Some information is collected and an analysis begins. More information is needed, so it collected and the analysis continues. If time permits, it is absolutely acceptable to seek additional data, unfortunately it is often the need for timeliness that forces an analysis to be completed. Just as a protection professional will assume that an adversary possess perfect intelligence on their facility, the analyst may be certain that they will not have perfect data upon which to develop their intelligence. Keep in mind that you have spent considerable effort collecting information the value of which is continually expiring. This is commonly referred to as "paralysis of analysis," and should be avoided. When it is necessary, make a

decision based on the facts at hand, be truthful of the accuracy of your assessment, be prepared to support it, and above all acknowledge that it is imperfect.

To begin the analysis review the goal of the collection effort. Is it to evaluate the threat to a controversial event or the threat posed by a disgruntled employee or student? Is it an ongoing program to evaluate leaks of organization information into the public domain? Knowing the goal will determine which product is being sought by your customer. Whether the customer is management or a client they have similar needs. Many times the customer is not the end user of the product. When this is the case it becomes worthwhile to learn what type of intelligence each consumer or end user is seeking and in what format. This is synonymous with the usability of the intelligence. If the format is not compatible with the field efforts, in whatever form it takes, then the intelligence will not likely be used. In the private sector this will often guarantee the loss of the client. Losing a client or annoying field teams is unnecessary. Determining how each consumer is likely to use the information creates the opportunity to reformat the intelligence for each consumer. The report may have several separate sections designed for each consumer, or there may be several separate reports. Either way, this is part of getting the right intelligence into the right hands to have a positive impact on operations.

In other instances, it may be necessary to create several versions of a report based on the information that will be disclosed. The simplest example of this is a public and a confidential release. In the private sector the report containing information about the collection and analysis methods as well as information that may reveal sources might be provided only to the security team, and a similar but less detailed report that does not reveal source information may be provided to operations managers or event promoters to keep them informed. In this manner, security is able to use the actionable intelligence and operations managers are aware of what may occur without being exposed to details that they do not need to accomplish their functions. In the public sector, information is often classified on a scale with individuals and departments having access to specific levels and/or compartments of information. This may result in a product for release at each level. By using databases it is possible to automate report creation ensuring each product only contains the information authorized for that consumer.

Analysis Methods

As in many disciplines, intelligence analysis occurs both quantitatively and qualitatively. Quantitative analysis, also referred to as "number crunching," utilizes objective information based on distinctly measurable criteria such as the number of crimes in a census tract, or the number of port scans on a network firewall. Qualitative analysis processes information that is subjective in nature. This may include whether a place is clean or safe. The judgment is ultimately based on an individual's perspective. Quality, being a subjective measurement, will typically differ somewhat between persons and quantity, being finite and measurable, will be replicable between persons. Here are a few types of analytical methods used in law enforcement (LEAS 2004) and protective intelligence.

- **Crime-pattern analysis (CPA)** – A process that looks for links between crimes and other incidents to reveal similarities and differences that could be used to help predict and prevent future criminal activity.

- **Association/Network analysis** – The collection and analysis of information that shows relationships among varied individuals suspected of being involved in activities together. This may provide insight into organizational structure, capability, and which investigative methods could be most effective.

- **Telephone record/ communication analysis** – The review of records reflecting communications (telephone, email, pager, text messaging, etc.) among entities that may be reflective of criminal associations or activity. It may recommend steps to take to continue or expand the investigation or study.

- **Flow analysis** – The review of raw data to determine the sequence of events or interactions that may reflect criminal activity. It can include timelines, event-flow analysis, commodity-flow analysis, and activity-flow analysis. It may show missing actions or events that need further investigation.

- **Spatial/geographical analysis** – A look at the locations of criminal activity or criminals to determine if future criminal activity can be deterred or interdicted through forecasting activity based on historical raw data.

- **Financial analysis** – A review and analysis of financial data to ascertain the presence of criminal activity. It can include band record analysis, net worth analysis, financial profiles, source and application of funds, financial statement analysis, and/or bank secrecy record analysis. It can also show the destinations of proceeds of crime and support prosecutions.

- **Strategic Analysis** – Most often related to the structure and movement of organized criminal elements, patterns of criminal activity, criminal trend projections, or projective planning.

Regardless of the methods used in any situation, always evaluate all the available information. Avoid ignoring information that disagrees with your own hypothesis or beliefs. From this evaluation draw conclusions that are supportable by the information. While intelligence analysis provides greater latitude than an investigation when it comes to including opinions and beliefs, these should be supportable based on historical events, available data, or similar situations.

Analysis Tools

The advent of the modern personal computer delivered considerable processing power to individual users, which has been capitalized on by many software makers offering robust applications. Not so long ago that these applications were often difficult to learn and use, however their routine use today provides a tremendous support network just from one's own peers or from online search engines. Consequently, everyone charged with completing nearly any kind of analysis potentially has at their fingertips unprecedented data manipulation applications such as spreadsheets, databases, specialized analysis software and data mining tools. These tools cannot replace an incompetent analyst but they will enhance a knowledgeable analyst's capabilities for understanding data. Training and education for using applications can typically be found through local colleges, universities, or technical job training centers. In

addition, there are many books available to enhance the analyst's skills. Specialized applications will often have training packages offered by the vendor and some times this is the only means to gain the necessary knowledge of the application.

Spreadsheet Applications

The spreadsheet is essentially an accounting tool for displaying financial data in rows and columns; however it has proven very useful outside of the financial arena. It is routinely used by many computer users as a mini-database. The spreadsheet does organize data in columns and rows, and it also provides for the manipulation and presentation of that data. Data may be sorted, compared, and displayed in wide variety of graphs.

Data concerning crime statistics, patrol costs, arrests or apprehensions, and any other relevant data may be included to provide a dizzying number of options for analyzing the data. Is your patrol program cost effective? Maybe your spreadsheet would include costs of gas and maintenance, number of incidents prevented or interdicted, crimes in the chosen area, and possibly even some information from a survey of the affected citizens (call it goodwill). Add in a few mathematical formulas and you can know what the cost of each patrol is when compared to the corresponding crime rates and citizen goodwill. Display the information in dollars for management impact, percentages for comparison, change the colors of the print, or place the information in a graph. Spreadsheets provide a convenient means for manipulating data in relatively small quantities. However, they will become overwhelmed in a short time if used to collate all the information within a collection operation.

Database Applications

Databases are just what they sound like, a place to put data. There are several types of databases including hierarchical and relational databases. These classifications come from how the data is organized, for instance a hierarchical database maintains data in a strict set of verticals with child data falling under parent data, but relational databases, as is found in Microsoft Access®, allow data to be related to each other. The latter allows data to be segmented into smaller groups that can then be related to additional pieces of data, providing greater flexibility in drawing diverse information together.

Again with today's applications, nearly any end user may create a database when necessary. Along with this power comes the opportunity for creating many incompatible databases which further complicates the retrieval process that is so important for intelligence analysis. Be aware of the various storage locations and mediums for data within your organization. Inquire as to how the data may be retrieved and integrated into current operations.

Common today are data warehouses in which all of an organization's data is placed, regardless of format, to make it available to anyone with access. Data warehousing developed as a result of the myriad of databases an organization may have created over time, since the introduction of the computer, but were not compatible. As a result, a separate user interface may be used that is able to retrieve data from anywhere within the warehouse. This, of course, oversimplifies the process and purpose of a data warehouse, but it is an important concept for understanding data mining applications.

Data Mining Software

Much like the idiom, "digging for information," data mining is the process of working through all the data within an organization to develop relationships that may not have been known to exist previously. As mentioned in previously, it was not uncommon within organizations or the government, for various databases to be unable to share data with each other. In some instances this may have been a good thing, but as you can imagine it makes for an inefficient operation. Data that is repeated in multiple locations, in multiple formats, creates confusion. Data mining is intended to work across these barriers to create and correlate as much information about the stored data, or metadata. Metadata is data about or describing source data.

Consider this example; a mail order company maintained marketing records separate from their sales records from the 1970's until the 1990's. They based their understanding of their marketing success on gross sales numbers, but as times changed so did the marketing budget. Top executives expected more efficient marketing efforts. Utilizing data mining tools, the marketing team was able to match sales records, addresses and zip codes, with their media coverage. Credit card sales, shipping addresses, and items purchased were all compared with the marketing information in an automated format. As a result, the company was able to target their marketing to those most likely to be responsive.

Now consider this within your organization for protective intelligence purposes. Consider all the information that is buried within the various data resources such as marketing data, human resources information, research information, guard tour information, visitor logs, badge reissues, loss reports and so on. And consider the same within a law enforcement agency with all of the various calls for service, reports for enforcement activities, intelligence field reports, patrol data, and so on. The amount of data is tremendous and it may just be that two types of data have not yet been correlated. Whenever data warehousing and a data mining program is started within an organization an intelligence analyst should try to get involved. It may not be a high priority to the organization to involve intelligence but getting involved is the only way to get a result.

Specialized Analysis Software

Specialized analysis applications that once were only available to government agencies are now available to the public. These powerful tools provide many of the analysis methods discussed previously such as timelines, link or association analysis, and commodity flow analysis. These packages are designed specifically to correlate diverse data and present it in an easily understood and usable format.

Some examples include (however this should not be considered an endorsement by either the authors or the IFPO):

- I2 Analysts Notebook –http://www.i2inc.com
- Visual Analytics - http://www.visualanalytics.com
- Pen-Link - http://www.penlink.com

The value of these packages can only be truly realized after they are populated with actual data sets. Before purchasing any product, be certain it meets the needs of the organization by requesting demonstrations and a trial use period from the application provider. Utilize the same data sets in each package to evaluate any advantages or disadvantages without skewing the results. In addition, try several different forms of data sets to get a feel for the various ways the application can present an analysis. It may even be worthwhile to request data from you organization's IT security department concerning the latest network attacks. Since this will truly be in the form of difficult to associate data (IP addresses, packet characteristics, and the like) it provides an excellent testing platform for determining how the data can be presented once processed by the analysis software. One additional note to this is the consideration that if the IT security team is given access to the software there may be a cost sharing opportunity if the intelligence budget can not independently provide for the chosen analytical package.

Intelligence Reporting

The value of any intelligence effort cannot be realized unless the intelligence product is disseminated to the right people at the right time. Late information or information delivered to persons unable to utilize it, not to mention if the information fell into the hands of an adversary, not only does no good but could result in injury or loss of life. Quality intelligence reports should be known for their timeliness, accuracy and clarity. As mentioned previously, the value of information decreases over time and that becomes most evident in the reporting process. At this point the competing needs of timeliness and completeness can create considerable stress. Make sure that whatever information you possess is available to those that must make the decision, whatever decision that may be. Waiting to add just a little more information may make the entire report useless. The published report must be clear and *based on current information*. Which means that it may be necessary to produce follow-up reports as additional information is analyzed. It is unreasonable to believe that any analyst will have "perfect intelligence" concerning an adversary or event. So present the analysis in an accurate, clear and timely report without embellishment, conjecture or extraneous information.

Depending on the needs of the organization, intelligence products may look and feel different that any other organization, however the basic intelligence product is a report presented in the form of an assessment. After all the collection, collation, and analysis, the analyst, or team of analysts, must assess something. This may be the validity of a threat, the level of vulnerability, or some similar concern. An assessment may be focused on a particular suspect or person, organization, venue, event, or it may forecast the possibility of a future event. Forecasts based on intelligence are essentially the best possible guess of what a person, organization, movement, or other human entity may do in the future based on current information. Although someday machines may act autonomously, today at the root of every threat, excluding accidents and natural disasters, is human intention. It is the role of intelligence to accurately report what that intent is, will be, how it may react in different environments, and why. It is this combination of assessments and forecasting that ultimately define the value of the intelligence product.

Report Types

General Assessments are commonly used to evaluate the here and now. Where are we and where is our adversary in relation to where we want to be within a specific timeframe. It may be

used to identify any potential adversaries, their capabilities, and your own organization's capabilities in relation to the adversaries. General Assessments may be done on a smaller scale with greater focus than other report types. For instance, the assessment may be concentrated on a particular group rather than an entire movement or criminal subculture. When several adversaries are being monitored it is often helpful to periodically produce updated general assessments of each adversary. Doing so often highlights any changes in their actions or intent. A General Assessment may also be developed for a specific location to determine what historical activity has occurred there, what activity is likely to occur in the future and why, as well as specific vulnerabilities, and causal factors for any activity. Site assessments can be of great help when developing a security program or for determining situational crime prevention options.

Threat Assessments define threats along with their capabilities and their intentions. Threat Assessments may be for a specific person, group, event, or location, among other topics. The report may include historical events to demonstrate capabilities and techniques, as well as a catalog of groups and personalities that may pose a threat. In addition, the report may or may not include some sort of forecast concerning the likelihood that the threat will manifest into an attack. These reports can be a potent force in justifying the allocation of protective or enforcement resources.

Evaluating the protection and weaknesses surrounding a person, group, location, event, or similar target is commonly referred to as a Vulnerability Assessment. This is typically done as a tool for improving security and to ensure that known vulnerabilities are countered. It should also be noted that a determined attacker may also conduct a vulnerability assessment for use in their attack planning process. It differs from the Threat Assessment in that the purpose is not to identify articulated or potential threats but instead to focus on what opportunities a potential threat may find for attacking the target. A vulnerability assessment often begins by identifying assets at the target and potential motivations of different attackers. This provides insight into the likely paths an attacker will choose to successfully complete their attack. It is important to understand that a vulnerability is an exploitable weakness. The focus of the vulnerability assessment is on determining which weaknesses are, in fact, vulnerabilities and offering countermeasure recommendations as appropriate.

Other intelligence products should be developed and refined to meet the needs of your consumer. In addition, all products should take into account the consumer's timetable and use of the intelligence. If the intelligence is to be used for implementing additional countermeasures then it should be made available early enough that those countermeasures can be enacted. In other situations it may be appropriate to temporarily maintain an "open channel" of communication and forward raw data to the consumer. While this may be worthwhile for short periods of time, such during some types of operations, it moves the responsibility of analysis onto the field personnel who may not be as well informed on a specific topic. While products should be created to meet the needs of the consumer, they should also be eliminated once their useful life has expired. This avoids unnecessary work effort that may be better applied to another product. Furthermore, being responsive to your consumer prevents the common grievance that intelligence is out of touch with operations.[10]

Training and Certifications

Development of the skills discussed here are often done "in-house" as the need arises. Many security departments may use some of these techniques without creating a dedicated intelligence function. Law enforcement agencies also typically separate the functions of Crime Analysts and Criminal Intelligence Analyst. There are, however, a number training and education opportunities within this growing field as well as professional organizations offering guidance and direction.

Undergraduate and graduate programs for intelligence analysis can be found at a growing number of colleges and universities. A few examples in the United States include the Research and Intelligence Analysis Program (RIAP) offered at Mercyhurst College (www.mercyhurst.edu), several intelligence concentrations offered by the American Military University (American Public University) (http://www.apus.edu), a graduate concentration in Law Enforcement Intelligence and Crime Analysis through St. Joseph's University (www.sju.edu), and others available through online searches. Moreover, a larger number of schools offer specific coursework in intelligence analysis within their other degree programs.

Throughout the world there are a considerable number of professional associations servicing the intelligence field with many specializing in criminal intelligence or crime analysis. As discussed in her article in the IALEIA Journal, Lisa Shultz (2003) compares some that offer certifications or designations in recognition of training, experience and evaluated skills. Here are a few examples:

- International Association of Law Enforcement Intelligence Analysts (IALEIA) and the Society of Certified Crime Analysts (SCCA) – www.ialeia.com and www.certifiedanalysts.net

- International Association of Crime Analysts (IACA) – www.iaca.net

- California Department of Justice and The Alpha Group Center (AGC, 2005) for Intelligence Analysis – www.alphagroupcenter.com

- Florida Crime and Intelligence Analyst Association (FCIAA) - www.fciaa.org as well as other state sponsored programs.

Students completing programs with The Alpha Group can receive credit for their work towards the Certified Crime and Intelligence Analyst credential sponsored by the California Department of Justice and the California State Universities (AGC, 2005). There are currently other certifications available within the industry, however the field is evolving and so are the professional designations. To obtain additional information on education, training and certification take the time to conduct some research. These organizations must attract students and members to sustain themselves and therefore should not be too difficult to locate using the various search methods discussed earlier.[11]

Conclusion

Criminal intelligence is a rapidly developing field of endeavor and many of the techniques used within it are worthwhile tools available to the protection profession in the context of protective intelligence. There are, however, some basic differences in the available research tools with the same goal of preventing future crime and loss. Law enforcement typically has the capability of court action collection methods such as electronic collections, but must legally base all collection efforts on a predication of criminal action. Private security teams, on the other hand, are not necessarily limited by this criminal predication requirement, but should remain focused on real threats to the client, or client organization. Above all, collections must be done in an ethically and legally appropriate manner to avoid exposure to criminal and civil legal actions. A well planned, organized, directed and continually refined intelligence analysis program can be of considerable assistance to the successful accomplishment of both the law enforcement and private security missions.

Additional Exercises

1. If you do not already know, determine whether your local police department publishes crime information on the web. How are you able to manipulate this data? Consider possible uses for it. If your local department does not offer such a service visit the San Francisco PD website and review the data they offer. Consider the value this may have when planning a protection detail, targeting enforcement resources, or simply buying a new home.

2. Select an issue of controversy that you are interested in. Conduct searches via the web using the same search criteria on several different search engines (www.google.com, www.msn.com, www.teoma.com, www.yahoo.com, www.dogpile.com) and any others that draw your attention. Notice the difference in the search results.

3. Now select advanced search tools and utilize different search criteria to obtain more data.

4. Now search for images associated with your search criteria. Try searching images associated with the name of someone involved in your research topic.

5. On the search engines of your preference, review the advanced search features and commands. Learn how to identify all websites that link to a specific URL. Learn how to search just a specific web site. Work with each advanced command.

Sample Threat Assessment [12]

Information

John is a prominent member of a local environmental group.
John was recently seen purchasing several cans of spray paint.
John was recently quoted in the newspaper that a new shopping mall should not be build.
John is 17 years old.

Construction equipment will be arriving on-site for the new mall in three days.
The company building the shopping mall has received threatening communications to stop the project.

The new mall will include at least one store selling furs and leather products

John's environmental group has publicly advocated the legitimacy of property destruction in forwarding their goals.

Several local individuals have been convicted of vandalism and criminal mischief with environmental undertones.
Previous vandalisms within 50 miles have included environmental slogans. Construction equipment has been sabotaged and disabled.

Intelligence

Situation

A new shopping mall will be built over the next six months on a recently purchased area of local forest.

Construction equipment will be arriving on-site for the new mall in three days.

Assessment

There is a heightened threat of attack to the new construction site. Particular attention should be paid once equipment and supplies have been placed at the site. Potential attacks to the construction equipment may include sabotage rendering them unusable without significant repair.

Previous local attacks have included ***arson*** in addition to ***vandalism***.

Upon completion of the mall, the fur/leather product stores could be at higher risk for attacks, including vandalism and arson.

Threat Environment

The Threat Environment includes any information gleaned from collected data specifically about the upcoming events or future actions that are being evaluated. This includes articulated threats, or collections that clearly state intent to commit an act, and potential threats, or those threats that the analyst logically believes may occur given the capabilities and intent of the adversary. Potential threats are often expressed as a probability.

Historical Activity

Typically, short summaries of the details of the historical events that were used in developing the assessment should be included here. These events may be entirely local or they could include some that demonstrate adversary MO and capabilities in similar circumstances elsewhere in the world. This is particularly true when there is information showing that individuals from these other areas have moved to your local area for operations.

Sample Practice Scenarios:

Scenario #1

One of your peers, another security professional, has told you a story of an unknown person that was able to have a copier, several computers and networking hardware ordered and shipped, however they are not an employee and no one is sure exactly how it has happened. He mentions that so far, the evidence is pointing to an outsider that utilized Social Engineering techniques. You, being concerned about a similar vulnerability with your employer and unfamiliar with this topic, have decided to collect information and present a report to your manager.

Problem Statement/Search Target:

What is Social Engineering and how is it a threat?

Online Search Tools:

(www.google.com, www.msn.com, www.teoma.com, www.yahoo.com, www.dogpile.com)

Online Search Criteria:

"Social Engineering"
"Social Engineering" "what is"
"Social Engineering" "how to"
"Social Engineering" methods
"Social Engineering" laws violations
"Social Engineering" "consulting OR training OR education"

Off-line Search Tools/Locations:

Top security managers
Other industry peers
Receptionists and other initial call takers
Corporate training staff

Specific Target Information:

Understand what Social Engineering is.
Understand some historical examples of it and who was responsible.
Understand some common examples useful for training.
Cite some countermeasures or sources for countermeasure expertise.

Analysis:

Describe the threat posed by Social Engineering to your organization.
What information or assets are at greatest risk?
Who or what position is most capable of identifying or defeating an attack?
Have you been attacked? How do you know?

Scenario #2

Someone in your organization has leaked information to an adversary (This could be either a law enforcement agency or a private organization). You know this is most likely true because some of your current countermeasure techniques have been appearing, with some detail, in adversary communications. As an analyst, you have been tasked with creating a method for determining how, or from whom, the adversary has been obtaining the information.

Problem Statement/Search Target:

How is the adversary obtaining internally sensitive and protected information from your organization?

Online Search Tools:

(www.google.com, www.msn.com, www.teoma.com, www.yahoo.com, www.dogpile.com)

What other online tools might you use for this?

Online Search Criteria:

You must identify what information has left the organization, what your adversary's capabilities most likely are, and what methods have been used by others in similar situations.
You may also conduct searches on counterintelligence techniques that may be useful in determining who is 'losing' the information.

Off-line Search Tools/Locations:

Who can you talk to about this without tipping them off? What might you peers know? Do you have a source within the adversary's organization that may be able to provide insight into there efforts?

Specific Target Information:

What specifically do you need to know, and who do you need to know it about?

Analysis:

How is the information most likely leaving your organization? What are the easiest and hardest ways? What are the least and most technical methods?
How will you go about identifying the person that is ultimately losing the information?
How could you use this to your advantage in the future?

References

Alpha Group Center for Intelligence Analysis (AGC) (2005). Certification Information. Retrieved January 31, 2005, from http://www.alphagroupcenter.com

California State University, Sacramento (CSUS) - College of Continuing Education. Crime and intelligence analysis certificate program. Retrieved January 31, 2005 from http://www.cce.csus.edu

Carter, D. (November 2004). *Law Enforcement Intelligence*. A guide for state, local, and tribal law enforcement agencies. Retrieved from http://www.cops.usdoj.gov

Cooper, H. (1996). *Business intelligence: A primer*. Berryville, VA: The Executive Protection Institute.

Dempsey, J. (2003). *Introduction to investigations*. Belmont, CA: Wadsworth/Thompson.

Edmonston, G. Jr. (June 7, 2002). Carry me back. Retrieved April 15, 2005 from http://alumni.oregonstate.edu/eclips/carry/june7_2002.html

International Association of Chiefs of Police (IACP) National Law Enforcement Policy Center (October 1998). Criminal Intelligence: Concepts and issues paper. International Association of Chiefs of Police.

International Association of Crime Analysts (IACA) (2005). *IACA website*. Retrieved January 31, 2005 from http://www.iaca.net

International Association of Law Enforcement Intelligence Analysts (IALEIA) (2004). *IALEIA website*. Retrieved January 31, 2005 from http://www.ialeia.org

Law enforcement analytic standards (LEAS) (November 2004). Global Justice Information Sharing Initiative and International Association of Law Enforcement Intelligence Analysts, Incorporated (IALEIA). Retrieved March 1, 2005 from http://www.iir.com/giwg/pdf/law_enforcement_analytic_standards.pdf

O'Hara, C.E. & O'Hara, G.L. (1994). *Fundamentals of criminal investigation*. Springfield, IL: Charles C. Thomas.

Operations security: Intelligence threat handbook (OSITH) (1996). The Interagency OPSEC Support Staff. Retrieved February 5, 2005 from http://www.fas.org/irp.nsa/ioss/threat96/part02.htm

Shultz, L. (2003). Crime and intelligence analysis certification. *IALEIA Journal*, *15* (2), Pp. 145 – 161.

Steganography (2004). Webopedia website. Jupiter Media Corporation. Retrieved on February 5, 2005 from http://www.webopedia.com/TERM/S/steganography.html

Vellani, K., & Nahoun, J. (2001). *Applied crime analysis*. Boston: Butterworth – Heinemann.

WordNet (2003). Princeton University. Online dictionary definition retrieved on February 10, 2005 from http://dictionary.reference.com/search?q=infiltration

Additional Notes

1. Competitive Intelligence is also a specialized field and is often what is referred to concerning information on intelligence programs within private organizations. Its focus is on obtaining data concerning competitors and the industry environment to assist in guiding business activities. This may be pricing practices, marketing strategies, or research and development data. The decision to not discuss this topic within this paper is more to maintain focus on non-market threats than a statement that competitive intelligence is handled differently.

2. This definition for intelligence was developed after reviewing many different definitions over the years. It is a reflection of the hybrid environment this paper is dealing with concerning intelligence as a function of investigations. It seems that no one definition can be settled on in the various intelligence communities, so one was created to focused on the key components of what happens with the data, why it is obtained and what it is turned in to through the process.

3. More on competitive intelligence. Although its goals are fundamentally different from protective intelligence and can more easily be equated to its defensive counterpart, OPSEC, the methodology and techniques are akin to any collection effort. So anyone interested in learning about protective intelligence is strongly encouraged to do some research and better comprehend competitive intelligence. These programs should not, however, be mingled within an organization. This would create competing interests within the collection and analysis effort and it is highly likely that the protective program would suffer. This is the simple result of the fact that competitive programs more visibly add to the bottom line than does any security effort.

4. OPSEC grew out of the government sector dealing with classified information; however it has just as an important role today within the private sector. Unfortunately it is often overlooked by security professionals until it comes back to haunt them. Those interested in learning about intelligence programs should also study OPSEC concepts and material for several reasons. One being that your adversary may be practicing strong OPSEC which will make your collections difficult at best. Two, it is only a matter of time before your adversary becomes interested in you, so the time to try and limit the information leakage is now. There are several online resources with the Interagency OPSEC Support Staff (http://www.ioss.gov) being a good place to start.

5. The differences between Crime Analysis and Criminal Intelligence Analysis, while significant and important to individual agencies, would not add to this paper and the discussion of the intelligence process in general. For further information on either of these subject areas it is strongly recommended that the International Association of Law Enforcement Intelligence Analysts, the Society for Certified Crime Analysts, and the International Association of Crime Analysts websites be consulted.

6. Covert channels are an interesting point of discussion. The author first learned of them while studying for the Certified Information Systems Security Professional examination. The examples provided here were discussed in the review classes by the instructors. As

more attention is given to this concept an individual begins to identify additional covert channel uses and threats.

7. This formula for defining a threat was first presented to the author in a graduate class on asset protection by a Consultant from Booz, Allen, and Hamilton. The focus of the formula, and the arguments it created, is the multiplication of the capability and intent. The logic being that a capable organization that is not interested does not meet the threshold of a real threat. In other words, you can't simply count every "potential" as a real threat. In terms of intelligence, it's good to know everyone with the capability and where their intentions currently lie and how they may be changing.

8. These classifications of information sources are somewhat arbitrary but necessary given the problem that arises when mingling government and private collection efforts. The court-action and non-court-action categories are based on the distinction drawn by Carter concerning open source intelligence, but since there are opportunities in the private sector to collect non-public information without court involvement a new category was needed. There are some instances in the U.S. when a private entity may be given court-ordered permission to conduct collections or seize property, but they are very specific and the most useful are extremely rare. One example can be found in Peter Schweitzer's book Friendly Spies. In the book and instance was presented in which an employee stole information concerning synthetic diamonds from General Electric and, after some considerable effort, GE was allowed to entered the former employee's home and retrieve the materials. This is not a common occurrence by any stretch of the imagination. Furthermore, the classifications developed beyond court-action versus non-court-action were also meant to allow the two realms of business and government to be bridged. By no means were these intended to state that any classifications currently in use by an organization are inappropriate. The original notes used for this paper are based on a continuum with court-action being on the far left, legal non-court action in the middle and illegal non-court action on the right. This coupled with the collection method classifications (electronic, infiltration, and direct) running vertically on the left provided a convenient framework for placing any method of collection regardless of the entity or specific method used.

9. Depending on what books, articles and other media that are reviewed concerning cover identities will determine how many different categories of covers exist. The important part of this is to recognize that covers do not need to be equally "bulletproof" depending on their intended use. Again, these classifications were not intended to question the validity of those that may be used by any organization but simply that their complexity can very significantly.

10. Trying to describe specific report formats in such a broad-based paper as this would be disastrous. The authors have written and created many different report formats for different consumers. Ultimately an organization's managers or clients will dictate, to some extent anyway, the format of any intelligence product. Being flexible goes a long way to insuring that the information is actually used. Should anyone want some assistance in designing a format or in discussing sample formats feel free to contact the authors through Asset Protection Innovations, Inc. found on the web at www.assetprotectioninnovations.com.

11. This is a very partial list of organizations within this field. It is not meant to sleight any organization. However, it is intended to somewhat challenge those interesting in learning more, and with a little luck, the information on developing search criteria will give the reader a method for finding further information.

12. The Sample Threat Assessment is just that, a *sample*. It is not intended to malign the environmental protection movement. It is, however, roughly based on work done by the author and so is representative of real-world analytical work. The report itself is far less than what would normally be provided but creating such a sample is difficult without drawing too heavily from personal experiences.

About the Authors

Robert Metscher, CPP, CISSP, CSS, CPO, MBA

Rob Metscher has held positions at various levels within the security industry since leaving the U.S. Army in 1993. He is the founder of Asset Protection Innovations, a Risk Management Consulting firm (www.assetprotectioninnovations.com) located in Maryland. He is skilled and knowledgeable in retail security, executive security, cash-in-transit/secure storage, protection program development, risk assessments, investigations and protective intelligence. He earned a B.S. concentrating in Asset Protection and a Masters of Business Administration, in addition to numerous certifications including the Certified Protection Professional, Certified Information Systems Security Professional, Certified Protection Officer, Certified Security Supervisor and Personal Protection Specialist. Rob writes periodically for various publications, some of which may be found on the Web.

Brion P. Gilbride, CSS, CPO

Mr. Gilbride is employed by U.S. Customs & Border Protection, under the U.S. Department of Homeland Security, and specializes in Intelligence and Counterterrorism Response. He also spent three years as a first-line supervisor in both the Campus Security and Industrial Security settings. He was previously published twice in Security Supervision: Theory and Practice of Asset Protection and in the ASIS magazine *Security Management.* He holds a Bachelor's degree in Criminal Justice from York College of Pennsylvania and a Graduate Certificate in Terrorism Studies from American Public University. He is currently working toward a Master's degree in Strategic Intelligence through American Public University. He is both a Certified Protection Officer (CPO) and Certified Security Supervisor (CSS).