Chapter 6

OPEN SOURCES AND OPERATIONAL SECURITY--THE DARK SIDE

6001. Purpose of the Chapter

This chapter is based on work by Mr. Richard Horowitz, a licensed private investigator and security consultant based in New York. Mr. Horowitz has served in the Israel Defense Forces, attaining the rank of Captain, and is a recently graduated law student.

This chapter is grounded on the premise that everything needed for the planning and execution of criminal or terrorist activity can be found in open sources. Indeed, an entire industry exists which is devoted to the publication of such material. In addition, equipment designed for one purpose and legally available can be used in terrorist or criminal activity.

The total cost of the publications and equipment presented in this "dark side" chapter is available for approximately $1,800. The chapter is based on the "seeing is believing" principle. Each of the items discussed in this chapter can be ordered by using the complete ordering information containing in Appendix G.

(NOTE: References to slides have been left in this text to provide a flavor or the complete presentation, but the slides are FOUO and available only from Mr. Horowitz or DIA. Appendix G has also been modified at the request of Mr. Horowitz to eliminate the names of the publishers and their addresses--Mr. Horowitz will provide these on request--his complete contact information is provided in Appendix G.)

From both a military and a law enforcement point of view, it is critical to understand that even our most poorly-funded and least organized opponents can gain access to relatively sophisticated intelligence collection tools as well as tools of destruction.

This chapter--like all other chapters in this handbook--is unclassified. The key point to emphasize is that everything presented is publicly and legally available. Books on intelligence collection, killing methods, offshore money laundering, and any other aspect of criminal operations can be purchased by calling an (800) number and using a credit card. We must all be aware of how such information might be exploited when acquired by persons seeking to harm or take advantage of others, and specifically, to harm members of the MAGTF in garrison or ashore.

6002. General Considerations

It is a fact of life that society contains those who are morally deviant, socially misguided, or worse. It is of similar importance that our society is based on certain freedoms which cannot be taken away. The combination of the two can results in terrorism and crime as we know it today. Underlying the activities of these individuals and groups is a culture

which includes recruitment, indoctrination, education, training, planning, preparation, and execution.

This chapter is not a training manual, though many techniques and methods can be recognized from professional government training. The objective is to create an awareness regarding the availability of open sources for terrorist and criminal activity.

Four general considerations are offered as an introduction to this model:

1) The availability of the open sources to criminals and terrorists, and the extent to which such capabilities exist, does not document a threat *per se*. Each individual command and each individual operation must carry out a threat analysis unique to their circumstances.

2) Everything we discuss in this chapter is available to anybody anywhere. This includes Colombian drug smugglers, Los Angeles gang members, Korean contract employees on a U.S. Army base overseas, and individual "crazies" seeking media attention by causing deaths or damage aboard U.S. military installations.

3) Information that has been available for years in published form is now available through the Internet. Bomb designs are popular in cyberspace. Periodic press reports tell of teenagers injuring themselves trying to construct a bomb they have read about on the Internet. While this problem will arguably increase, it should not obfuscate the reality that the industry which produces the material in hard copy has existed for many years.

4) Although "high-tech" threats attract more media attention, the reality is that low-tech capabilities are often just as effective, cheaper, and easier to develop. A federal officer can be attacked by a doberman with its vocal cords cut out--a low-tech but very effective means of perimeter security. The bomb used to destroy the Federal Building in Oklahoma City was not a complex construction--it was a simple mix in a large amount.

6003. Open Sources and Radio Interception

Intelligence acquisition, or information gathering, is a crucial first step in planning and executing an operation. The books in Appendix G include several devoted to various methods of electronic monitoring, operational activity, and computer databases.

This split slide shows frequencies for Air Force One on the left, taken from a book by a California hobbyist which is devoted to monitoring the President. Entitled "Monitoring Air Force One," the volume discusses and lists frequencies of the Mystic Star, Echo/Foxtrot, and FM-FDM-SSB systems, along with identified Secret Service code names.

On the right is the cover of a book published in 1986, entitled *Guide to Embassy and Espionage Communications*, which listed thousands of frequencies transmitted from 55 countries, the International Red Cross, Interpol, and the United Nations.

The extent to which frequencies of federal and state agencies that are intercepted and published presents a security problem is not within the scope of this chapter. The range of equipment and information commercially available indicates a problematic potential or at the very least, can be an incentive for subversive groups to attempt to intercept government transmissions.

Commercially available radio scanners can intercept UHF, VHF, and military bands; some have uninterrupted frequency ranges from 30 MHz to 1.2 GHz and are available in desk top or portable versions. Current law requires manufacturers to block cellular telephone frequencies.

Frequency counters-devices that intercept radio transmissions and display their frequencies on a read-out-are also commercially available.

Monitoring Times runs a column which publishes frequencies used by federal agencies that were intercepted by hobbyists. These agencies include the F.B.I., Secret Service, U.S. Customs, and numerous military agencies. After the World Trade Center bombing, the magazine carried an article listing frequencies used by various Port Authority units, the FAA, and local "press disaster" frequencies. Guides to U.S. and allied official frequencies are readily available worldwide--if a hobbyist can track you, so can a criminal!

6004. Open Sources and Telephone Interception

It is illegal to monitor cellular phone conversations (868-896 MHz). Prior to April 1994 however, radio scanners capable of intercepting these frequencies were legally manufactured and sold. Scanners that blocked cellular frequencies were constructed such that they could be easily modified to intercept cellular transmissions.

Scanners manufactured before April 1994 can still be legally owned or sold. Hence, many scanners capable of intercepting cellular calls are accessible and in use.

Some methods of scanner modification:

-- A Massachusetts company advertises that for $40, they will "unlock" your scanner

-- Journals print schematic diagrams showing how to modify the scanner's circuitry;

-- While the new law prohibits the manufacture of frequency converters- a device that will convert 400 MHz interceptions to 800 Mhz interceptions, many are accessible.

-- For those with technical skills- a cellular phone, which needless to say operates on cellular frequencies, can be modified to intercept other cellular calls.

A book entitled *Tune In On Telephone Calls*, listed in your second hand-out,

enumerates frequencies and channels used in various types of telephonic transmissions. Its various chapters cover such operational relevant areas as military aircraft VIP phone calls, satellite phone calls, coastal maritime calls, and cellular calls.

In addition to voice and data interception, there is a commercially available device called a tone decoder which converts the frequencies of a touch-tone dialing system to numbers and displays them on a read-out, in effect allowing easy identification of those being called by the intercepted telephone, as well as read-out of any other information being transmitted through the touch-tone signals, such as codes and account numbers.

Internationally, for instance from Switzerland, more sophisticated equipment is available, and we should assume that surplus or illicitly obtained military equipment is also available to individuals to whom good intercepts are critically important.

6005. Open Sources and Eavesdropping

Numerous books are in print detailing how to tap a phone or bug a room. Some are quite technical. A manual originally published by the U.S. Department of Justice entitled *Electronic Eavesdropping Techniques and Equipment* has been republished under a different title by a commercial publisher, and is listed in your second hand-out. Please note that "old" techniques can be very effective, especially if there is very little emphasis on operational security against civilian opponents!

In April, 1995, U.S. customs officials raided 40 spy shops in 24 cities that were illegally selling eavesdropping equipment smuggled into the United States from two Japanese companies; 11 people were charged with crimes a result. Termed "electronic surreptitious interception device," among the equipment smuggled into the United States and sold by these shops:

-- telephone transmitters with a range of 400 meters

-- bugging transmitters with a range of 1,000 meters

-- ball-point pen transmitters with a range of 200 meters

-- A/C line transmitters-attached to the line, behind the wall outlet and permanently operates on its current-with a range of 200 meters.

From documents filed in court by the U.S. Government, from October 1993 through February 1995 a total of 161 shipments of 4,367 eavesdropping devices took place. The devises had an estimated retail value of $2,972,517.

Companies also publish electronic plans enabling an individual to assemble his own equipment. These schematic diagrams include automobile tracking transmitters, bugging

transmitters, telephone transmitters, a transmitter locator, and audio amplifiers.

Bottom line: assume your are "on the air" unless certain the circumstances are secure!

6006. Open Sources and Undercover Operations

Undercover operations is a term used to describe various types of activities designed so that the fact they are taking place is not recognized, or, if recognized, not for what it really is. The general purpose of undercover operations is generally either to affect a change on a target or to gather information about a target.

Manuals for private investigators, as well as training manuals for law enforcement from various countries have made virtually all aspects of undercover operations a matter of public record. There are manuals on undercover operations in general, on developing clandestine human networks, on surveillance, on lockpicking, and even on elicitation and pretext calls, a very common technique for obtaining information.

Books are in print containing prepared scripts for obtaining personal and financial information from people. One book opens with a chapter entitled "Establishing Rapport and Overcoming Objections." Complete citations are in your second hand-out.

This slide shows two illustrations, one from a manual on surveillance techniques, the other from a manual on lockpicking. Complete citations for both are listed in your second hand-out.

Lockpicking tools are legally sold; prices can start from about $25. The law does not criminalize possession of lockpicking tools unless the person possessing the tools "evinces an intent" to use them for burglary. To quote the New York State law:
"A person is guilty of possession of burglar's tools when he possesses any tool, instrument, or other article adapted, designed or commonly used for committing or facilitating offenses involving forcible entry into premises...under circumstances evincing an intent to use or knowledge that some person intends to use the same in the commission of an offense of such character."

It merits comment that with the limited number of known aerial and maritime surveillance platforms that the U.S. Coast Guard has to patrol the drug routes from Latin America to the United States, it would be an easy matter for drug criminals to establish both passive observation posts near airfields and ports, and also active aerial and maritime surveillance capabilities. In brief then, criminals and terrorists who understand the value of intelligence collection, can easily establish significant capabilities which can frustrate official government programs.

6007. Open Sources and Interrogations

Criminals and terrorists have access to professional training and professional interrogators. Even the most reputable firms, such as E2G and Rapport Research in the United Kingdom, both staffed by highly trained former Special Air Service (SAS)

interrogator-translators, will be happy to offer training and perhaps even surveillance and other services to those who come to them with cash and an appropriate cover story.

In the United States, the "Soldier of Fortune" circuit includes many training and exercise schools where useful knowledge can be learned.

This slide listed selected chapter headings from two books readily available on the open market, one on psychological interrogation techniques, the other on physical interrogation techniques.

As transnational crime becomes a greater threat to national security, and the military become more involved in support to law enforcement operations, it merits comment that operational security and "need to know" are just as important in this environment as in any other.

Indeed, one of the distinguishing aspects of transnational criminal operations are their ruthlessness, and the ease with which they can select and coerce civilians to help them on a one-time basis by threatening to kill their loved ones--how many Pacific Coast fisherman do you suppose would refuse to carry one load of drugs if they were assured that it would only be a one-time risk, and that their loved ones were being held under surveillance and would be killed if the fisherman did not cooperate?

6008. Open Sources and Direct Research

Previous chapters have dealt with the rich range of open sources, and how to develop intelligence from open sources, including international sources and the Internet. The point to emphasize is that terrorists and criminals have access to everything in the open source world described by this handbook.

Major criminal and terrorist organizations are fully cognizant of the utility of open sources, and know how to do their homework. They know the power of computerized search & retrieval, and the value of information in support of their operational objectives.

For the purposes we are discussing, the computerized databases which can be accessed by anyone in the public, including criminals and terrorists, can be divided into the following three broad categories:

-- Media: available are not only *The New York Times*, *Washington Post*, and *Wall*

Street Journal, but numerous local newspapers such as *The Rocky Mountain News* (Denver, CO), *The Commercial Appeal* (Memphis, TN), and *The Times-Picayune* (New Orleans, LA), and foreign newspapers such as *Le Monde*, *The Irish Times*, and *The Prague Post*. Wire services- UPI, AP, Reuters, and the Xinhua News Agency (China), are also accessible.

-- Business and public records: corporate and bankruptcy filings, SEC filings, property ownership, criminal background checks, driver's licenses. Financial news. Companies combine mailing lists of hundreds of marketing companies, resulting in a database which can identify the address of a person or family, or their neighbors. Reverse phone directory-enter name, retrieve a person's phone number, or enter a phone number and retrieve the name of the person.

-- Specialized trade and industry information: databases exist that specialize in information unique to a particular industry or country, generally in the form of periodic newsletters, and are a valuable source of information. This slide lists some of the sources of possible use to criminals planning electronic thefts or money laundering operations, and terrorists planning specific acts.

A classic example of the basic utility of research: on 3 May 1993 a news report was carried online about the meeting of the Nuclear Regulatory Commission, entitled: "Commission Hears Options for Dealing with Vehicle Bomb Threats". Discussed online: the four options regarding physical barriers surrounding nuclear power plants.

6009. Open Sources and Executions

This slide is a combination of extracts from two books, one on killing and one on creating silencers.

Literature on killings and executions are graphic and the methods described are real. A six volume work entitled "How To Kill" is representative. Volume One begins with "Chapter One: The Target," complete with an anatomy chart highlighting sensitive parts of the body. Subsequent chapters are devoted to various types of killings. Appendices entitled "The Signs of Death," "Your First," and "A List of Poisons" follow the chapters.

A separate body of literature exists on the use of knives. One book has the topical heading of "anatomical considerations" followed by diagrams entitled bleeders, immobilizers, quick kill, showing the respective spots on the body. The book ends with an appendix entitled "Suggestions for Further Study."

Books describing how to construct silencers from household material exist. Attaching a slightly filled plastic soda bottle or a container of three tennis balls to the barrel of a gun are crude methods. More technical methods requiring metals are detailed. In a chapter entitled "Your Last Chance To Be Legal," one book discusses the various federal forms that need be filed in order to request to manufacture a silencer.

Manuals on improvised weapons show how to install a gun or firing mechanism in, for example, an umbrella, belt buckle, flashlight, briefcase, cigarette lighter, or tobacco pipe.

The same publisher selling books on how to kill supplies a book on how to dispose of dead bodies, including a technique on removing a bullet from a body without leaving evidence.

Full citations to all the books cited in this chapter are contained in Appendix G.

6010. Open Sources and Explosives

This slide is also a combination of several diagrams to illustrate the nature of the information that is available in open sources about creating and using explosives.

Improvised explosives, and bomb design, are topics with the most published literature. Numerous books in a "cook book" form describe how to mix readily available chemicals into explosives. Mixing soap flakes with gasoline so as to allow the gasoline to stick to its target instead of dripping off before igniting is discussed in a book and in a video on making explosives.

Separate books exist on how to make C4 and Semtex.

While these books generally have a disclaimer that the information contained therein is for educational purposes only, a book entitled "Professional Standards for Preparing, Handling, and Using Explosives" is available from the publisher.

From a catalogue:

DEATHTRAP! The Video: There is no better way to learn about improvised explosive booby traps used by international terrorists than to watch live, on-camera demonstrations of their construction, deployment and detonation. DEATHTRAP! The Video is a chilling seminar in just that - how terrorists modify innocent everyday items to conceal insidious explosive booby traps designed for maximum shock and lethality. You'll see ingeniously disguised devices made out of books, music cassettes, mugs, portable tape players, foot powder cans, alarm clocks, videocassettes, mousetraps, and more, all triggered by simple electrical, chemical, or mechanical means.

The video costs $29.95 and runs for 35 minutes.

A wide variety of related books are also available, for instance on bridge demolition.

6011. Open Sources and Radio Detonation of Bombs

Apart from simple explosives, it merits comment that sophisticated devices for

detonating explosives from a distance are readily available to criminals and terrorists.

Bombs can be detonated by remote control, through radio detonation. The chip needed for production of the detonating tone retails under $20.00.

A book entitled *Improvised Radio Detonation Techniques* describes how to modify various types of radio equipment into detonation transmitters. This slide lists devices afforded a chapter in the book, along with relevant information regarding their modification.

In March, 1994, this book was among numerous other books found in a storage locker of a man suspected in the package bomb that killed five people in upstate New York. In a similar incident, on February 10, 1995, the Associated Press released a report of a high school student's locker booby-trapped with a set of firecrackers wired to a circuit board and capable of being detonated by radio control.

Radio detonation, including that of car bombs, is a major problem worldwide:

-- In May 1992, the Mafia killed Judge Giovanni Falcone and three bodyguards with a car bomb detonated by remote control while they were driving along a Sicilian highway.

-- A March 1994 article in the Current Digest of the Soviet Press entitled "Who's Getting Killed In Moscow, and How" cited the problem of remote control detonation.

-- In January 1995, a group that manufactured radio detonated bombs was arrested in St. Petersburg. Constructed for $60 and sold for $1,500, the bombs came with a six month guarantee.

According to the Intelligence Newsletter of March 16, 1995, Egypt spent $18 million in 1994 on equipment to detect car bombs and to jam their detonation frequencies.

6012. Open Sources and Vehicular Enhancements

Evasion is a significant concern after executing an operation. There are a number of enhancements that can be made to vehicles, enhancements which can increase chances of evasion if detected and pursued. Some possible enhancements are listed in this slide.

There is a thriving small industry specializing in the production of armored cars for civilians. Publications such as *The ROBB Report* routinely advertise all manner of armored vehicles for sale--vehicles which to all outward appearances, are simply a normal car.

In addition to enhancements to the individual vehicle, skill at evasive driving is crucial in case operatives are detected. One manual on evasive driving illustrates evasive techniques on city or country roads, and in chase situations, along with automobile security modifications such as an oil slick or smoke screen generator. In case the driver does not

successfully evade the pursuer, techniques for knocking the pursuer off the road are described. The manual has a chapter entitled "Suggested Training Schedule."

This is a good point in the chapter to emphasize that criminals and terrorists are very aware of the fact that they pursue very high-risk, high-gain occupations, and have a great deal to gain from proper preparation. Their preparations are all the more difficult to deal with because by definition they are camouflaged as civilians and do not wear uniforms or follow any recognized rules of engagement. Establishing their technical capabilities and their "order of battle" thus calls for entirely different collection methodologies.

6013. Open Sources and Tactical Communications Jamming

Military forces rely heavily on command & control, and on combined arms operations. Military patrols in support of law enforcement operations are relying on artillery and other forms of reinforcement as they venture out "on point". It therefore becomes important to understand that criminals and terrorists are capable of executing tactical communications jamming operations.

Although radio jamming is illegal, *Improvised Radio Jamming Techniques* is a technical book describing the construction of a jamming station, allowing an operative to jam radio transmissions of government agencies as part of an operation or during the evasion stages.

Chapters in the book include:

-- Intercept Equipment Selection
-- Covert Antenna Systems
-- Intercept Operations
-- Police Radio Operational Procedures
-- High-Risk Frequency Detection Techniques
-- Jamming Equipment Deployment
-- Operational Security

6014. Open Sources and Bank Card Forgery

Central to criminal and terrorist operational security is the creation of a new identity, or a variety of identities that frustrate the efforts of law enforcement officials to track their international and domestic movements. The methods of creating a new identity in various books range from obtaining a new public image to physically disappearing and altering one's identity. Some books on creating a new identity focus on obtaining public records under a new name. Chapters are devoted to social security cards, driver's license, credit cards, and bank statements.

Other books exist on how to produce counterfeit identification documents. One book

contains chapters such as The Forger's Kit, Forgery Techniques, and Quality Control, and discusses the "False Identification Crime Control Act of 1982" which prohibits selling fake I.D. by mail. The book continues: "It's still possible for the forger to buy the various materials needed to produce fake I.D." and provides names and address and several companies.

A separate book exists devoted to counterfeiting currency. Chapters include "Basic Printing Techniques Used in Counterfeiting," " Purchasing Equipment and Supplies," and "Passing Counterfeit Currency."

Worldwide contacts, and world-wide mail drops, area readily available to criminals and terrorists. Companies publish booklets listing lawyers, bankers, and accountants in numerous countries ready to take a call from someone in need, together with lists of thousands of companies providing voice, fax, and correspondence forwarding services.

These are the traditional methods. Today, "cyber-theft", and direct anonymous access to bank accounts, as well as the complete concealment of international financial transactions through encryption and anonymous remailers, is becoming the major foundation for global criminal activity. One good reference is *Electronic Fund Transfer Systems Fraud*, published by Paladin Press (ISBN 0-87364-490-5).

6015. Open Sources and "Legal" Offshore Passports

Companies will, for a fee, arrange a legal passport and citizenship for their client, from a country not the person's country of birth.

Below is the fee scale from a company based in Amsterdam which specializes in passports and citizenship from Latin American and Caribbean countries--a legal citizenship with can be obtained within 90 days of submitting the company's application.

Dominican Republic	$19,500 for 1-4 individual orders
Venezuela	$21,900 for 1-4 individual orders
Panama	$20,900 for 1-4 individual orders
Ecuador	$23,900 for 1-4 individual orders

The application requests information such as the applicant's name, date and country of birth, height, eye color, visible scars, existing citizenship, profession, and mother's maiden name.

Along with the application, one need submit:

-- the signature and photo page of the applicant's current passport
-- copy of a birth certificate
-- three color negatives in three different sets of clothing

-- affidavit of good conduct from a licensed attorney or local police clearance
-- six thumbprints
-- six signatures on a white sheet of paper
-- a personal character reference or bank reference

The company's material explains that one need not visit his new country but can remain a "citizen living abroad," and contains a chart indicating countries that can be entered without a visa with your new passport.

The company can arrange a diplomatic passports "to some," for a fee of $55,000.

A midwest American company offers "genuine" passports and driver's licenses from countries that no longer exist, such as Burma, Rhodesia, Dutch Guiana, and the Republic of Zanzibar. The company portrays these passports as "emergency passports," in case terrorists hijack a plane and the American traveller would not want to identify himself as such. The application requires only a name and credit card number.

A U.S. Government "Passport Agent's Manual" has been acquired and republished by a commercial publisher. The manual is a useful guide for avoiding obvious mistakes.

6016. Open Sources and Offshore Corporations

In addition to arranging second passports and citizenship, companies exist that will establish shell companies for their client, generally offshore.

One British company specializes in establishing companies in the Bahamas, Belize, the British Virgin Islands, Delaware, Gibraltar, and Panama. The company's promotional material contains a chapter on each country, reviewing the requirements regarding:

-- capital and shares
-- directors and shareholders
-- meetings
-- accounting
-- corporate seals
-- company name
-- registered agent, office, and domicile

The application form requests only the name of the company to be established, the names and nationalities of the shareholders and directors, the objective of the company, and the applicant's name and address.

A Hong Kong company will also form a company in localities around the world, from the Cayman Islands in the Caribbean to the Isle of Man located in the Irish Sea. The company's specialty is Hong Kong "shelf companies"- corporations ready for purchase.

The Hong Kong company provides a list of over one hundred shelf companies incorporated in Hong Kong. Company names were chosen, apparently with the intent of attracting American buyers. These shelf companies were incorporated in 1993-94, allowing the company's purchaser to give the impression that the company had been in business years before the purchaser took control.

The application form requests only the names, business occupations, nationalities, and passport numbers of the company's officers and directors, along with information on the purchaser's bank account. For the client's benefit, the Hong Kong company includes educational material on how to arrange letters of credit through the client's new offshore company.

6017. Open Sources and Choosing a Criminal Specialty

Similar to books on individual methods and techniques, books are available on crime as a profession. For example, a book entitled *Drug Smuggling* contains information on how to find a drug source, what type of airplane is suitable for smuggling, and how to launder money. It closes with a discussion on dealing with law enforcement and a chart detailing federal and state drug laws, shown in this slide.

A book entitled *Successful Armed Robbery* written by an inmate in a federal penitentiary, contains the following chapter headings:

-- The Selection Process
-- Strategic Production-Planning
-- Factors Affecting Your Success
-- Self-Caused Failure

This book contains diagrams of various types of parking lots and illustrations on how to approach and assault the driver of a car.

Hit Man; A Technical Manual for Independent Contractors covers the entire range of activity for the planning and execution of a contract murder. Topics range from surveilling the target to psychological approaches to the job. From a chapter entitled "Finding Employment, What To Charge, Who To Avoid": "Prices vary according to risk involved, social or political prominence of the victim, difficulty of the assignment, and other factors." A federal judge was listed at the suggested price of $250,000, for example. A county sheriff might bring $75,000 to $100,000....

A related book entitled *How To Hide Anything* is available to criminals and terrorists. It contains numerous diagrams illustrating the construction of hiding compartments for objects or people an indoor and outdoor settings, and can be used to create hiding places for contraband, documentation of illegal exchanges, and special illegal technical equipment.

The list goes on. There is a market in information about how to be a criminal or terrorist, and there are established concepts, doctrines, and information about organization, methods, and equipment which is readily available world-wide.

6018. Conclusion: The Dark Side of Open Sources

This chapter has reviewed the open source knowledge available to criminals and terrorists which, when properly utilized, can make the military mission and the mission of law enforcement more difficult.

In particular, this chapter has sought to emphasize that operational security and the "need to know" are important aspects of success against a well-trained and well-equipped criminal or terrorist organization which understands the value of intelligence collection.

Criminals and terrorists can intercept radio and telephone conversations; they can exploit eavesdropping devices and execute tactical signal intelligence collection operations. They know how to conduct undercover operations, how to interrogate captured prisoners, and how to do direct research using open sources.

Individuals can be effective at executions and in the use of explosives. Radio detonation of explosives through a variety of remote devices is easily understood and readily carried out.

In the escape and evasion phase, criminals and terrorists can exploit armored vehicles equipped with oil slick and other devices for delaying pursuit, and can also execute tactical jamming operations which may allow them cut off and surround their military or law enforcement pursuer before back-up forces can be mobilized.

In conducting transnational criminal and terrorist activities, these individuals can avail themselves of false credit cards, new identities including legal passports possibly obtained through false supporting documentation, and related corporate and letter of credit documentation.

Over all, this chapter has sought to communicate the degree to which information about various criminal professions is available in the open source world, allowing for knowledge about how to conduct many different kinds of crimes and illegal activities to pass from one generation of criminals to another.

Criminals and terrorists can think and read--open sources are as useful to them as they are to intelligence professionals and the operational commanders they support.

Open Source Intelligence: HANDBOOK Proceedings, 1997 Volume I, 6th International Conference & Exhibit Global Security & Global Co - Link Page

Previous	OSS '97 HANDBOOK Chapter 5. Open Sources and Military Capabilities,
Next	OSS '97 HANDBOOK Chapter 7. Conclusion: Collection and Processing Open Source,

Return to Electronic Index Page