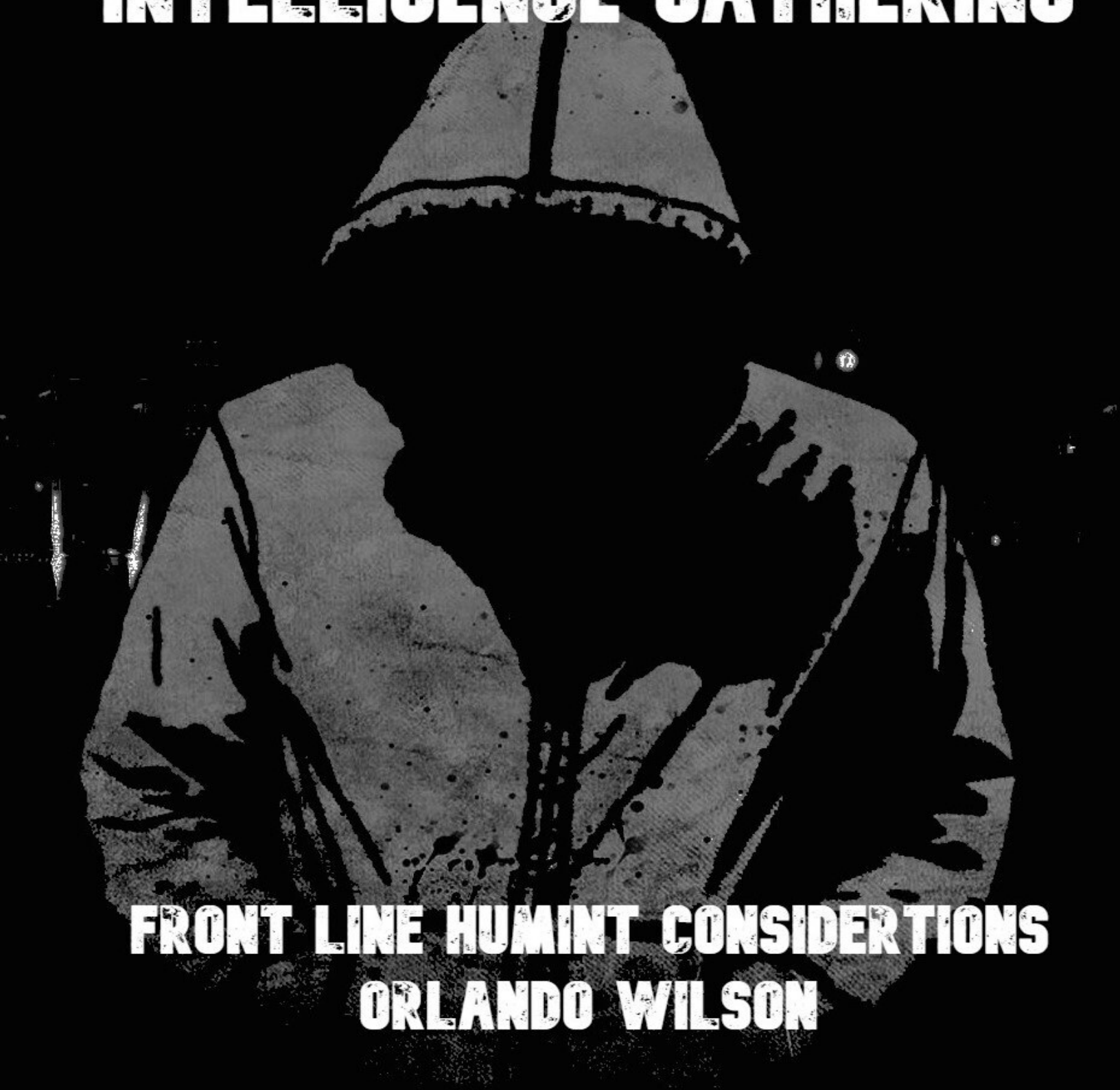
INTELLIGENCE GATHERING



FRONT LINE HUMINT CONSIDERTIONS

ORLANDO WILSON

I N T E L L I G E N C E G A T H E R I N G

Front Line HUMINT Considerations

Orlando “Andy” Wilson

“Nobody can guard your secrets better than you, so do not blame anyone for revealing your secrets because you could not hide them yourself. Your secret is your prisoner, which if let loose it will make you its prisoner.”

Imam Ali (AS)

Cover designed by Orlando Wilson

Orlando “Andy” Wilson
Visit my website at www.tohff.com.com
Social Media @artfulgypzy

Proofread by Ms. Delia Allen

First Printing: April 2020

ISBN- 9798635365069

CONTENTS

THE BASICS

Years ago, a client asked me to do some research on a gentleman in one of the former Soviet Republics. The client had a major issue with this person, who happened to move in very dubious circles. The client, who was very credible and established, said to me he could get this gentleman killed, but this would not worry him as such things were part of the criminal world he existed in.

The client told me he wanted to destroy this gentleman's reputation, ruin his legitimate business, and legally seize his assets. The client knew this gentleman's reputation and assets were worth more to him than his life. To achieve his objective the client needed accurate intelligence on his target. Intelligence is power, it can make someone or break them, literally.

I think since human beings first learned how to talk, they have been spying and telling tails on each other. The only thing that has changed with intelligence gathering from the time Sun Tzu wrote his classic book "The Art of War" in the 5th Century BC and today is the technological advancements that only really started to develop in the 20th century. The basics of tradecraft, personal security, and recruiting informants, etc. are still very similar if not the same as in the times of Sun Tzu and earlier.

Most of the things I talk about in this book are double-sided; you can use the techniques to target others, but they can also be used to target you. If you're involved in serious investigative or intelligence work, you must always be on the watch out for others targeting you in one way or the other.

The information and techniques I talk about in this book are simple, most are just common sense, but they will give you and insight into the skills and mindset required for HUMINT and counterintelligence operations. Operationally you must always keep things as simple as possible, the more complicated things are, the more that can go wrong. Bullshit can baffle brains

and many people seem to think if they over-complicate something it makes them seem intelligent and gives them more content to show a client, etc. That's all good if you're a bullshiter dealing with bullshit clients, but if you're dealing with serious clients and situations always keep things as simple, factual and direct as possible. Believe me, things can get very complicated, very quickly even with the best planned and apparently simple operations, so avoid the bullshit.

In the intelligence and investigations world, people always talk about keeping a low profile, which you should always try to do to the best of your ability. The issue arises when you run a business providing investigations, research or surveillance services. You need to advertise your services and network or else you won't have any clients. Working out how to layer your business, keep a low profile and at the same time market yourself needs to be part of your business plan and protocols.

These days if you're running a legitimate business you have to be on record somewhere, at a basic level, your company registration or your professional licenses at least. In most countries, information on company registration and professional licenses is publicly available which can compromise your personal security to start with. Where legal, always use virtual offices, addresses and phone numbers for your company's registration and licenses.

Below are just some very basic tips I give people who are dealing with debt collectors. I advise everyone who owns a business to think about layering their business and assets if for no other reason than these days it's very easy to get sued. Layering your business and assets will help you understand how such procedures and protocols work. As I said, most of the information in this book is double-sided, and asset locations are very much part of the intelligence business.

- Own Nothing, transfer the ownership of your home, cars and valuable possessions to someone you trust or to a corporation.
- Set up a corporation with other trusted partners so the company bank accounts and assets cannot be seen as your personal bank accounts.
- If your corporation is going under then sell off its assets and transfer the registered corporate office address to a virtual office or mailbox

and the phone numbers to a voice mail.
- If you're going into debt sell your cars and possessions to trusted friends or family and retain rights of use.
- Always research your local laws on company protection of assets, debt and debt collection.

I am regularly asked by people how they can get passports in different names and set up new identities for themselves. The truthful answer is that legally you can't. If you're stupid enough to try to use fake government-issued identification documents, you can end up in a lot of trouble. Making private company or press ID's with fake names on them is not an issue but buying fake driving licenses and passports is illegal.

In many places fake and stolen passports, driving licenses and government papers are for sale if you know the right people or find the right websites and don't get scammed. I know of one idiot who decided to buy a fake passport and attempted to travel on it. He got on the plane without problems, but when his papers were checked by the immigration officers from the country he arrived in, they wanted to know why he had a passport belonging to someone that had been murdered in an EU country about 6 months before.

To make this wannabee James Bond's situation even worse he had mailed his own original passport back to his country, so he was arrested for traveling on fake documents and initially connected to a murder. He ended up serving 6 months in prison and then deported back to his own country, where the cops were waiting to have a chat with him also.

One issue these days for investigators, especially when traveling, is having your computers and phones checked by airport security or the police. In a lot of countries not unlocking your computers or phones to be inspected by the police is a criminal offense. I recommend you always comply with the laws of the countries you are in, just remove anything from your computers and phones you don't want others to see.

There are many ways of sending sensitive investigation notes and reports these days. Keeping such items on your electronic devices while going through airport security or in sensitive locations is very dangerous and stupid.

A simple technique is to upload sensitive information to a cloud app or email server and then take the app off your phone after the upload. When you need to access the information again just reinstall the app and log into your account.

It's easy and affordable to buy smartphones and SIM cards in most places in the world today. For operational phones buy specific phones for that operation and only keep information and apps on them that are relevant. After the operation, the phone can be presented as evidence, stored as part of the case file or disassembled and destroyed.

If you're running a professional business you must keep things legal, every element of an operation needs to be assessed to ensure it is legal in the locations that you're running it. If you're collecting evidence that is going to be used in court, you must ensure it's collected within the guidelines for admissible evidence for that court and legal system.

I have been involved in the security and investigation industry internationally since leaving the British Army in 1993 and things have changed dramatically since then… As I said earlier the basic physical tactics, techniques and procedures have remained more or less the same but, with the development of the internet communications, logistics and networking are in a completely different world. Sadly, though, many are still stuck in the 1990s.

One of the first large investigations I completed when I started working for myself in the mid-90s was to locate a fishing trawler in the far East of Russia. This entailed getting contacts to 1. Locate the vessel 2. Take and develop photos 3. Send to Moscow 4. Fax me the photos and report from Moscow 5. Originals were sent to me via FedEx 6. Forwarded to the client. This job took about 3 weeks if I remember correctly. These days as soon as the vessel was located, we could stream real-time video to the client via a smartphone...

I find it funny how many people seeking work - and quite a few working - in the specialist security or investigations industry have completed many tactical or weapons courses and may be licensed in numerous locations but are still lacking the basic soft skills required to be able to complete the most basic tasks… I class these basic skills as life skills that apply to virtually

everyone, especially those who work for themselves.

These skills include:

- Must be able to use a computer or smartphone
- Must be able to use various messengers
- Must be able to write a report
- Must be able to take viewable photos and video
- Must be able to plan a route and use maps – physical & digital
- Must be able to get from one location to another on time, internationally
- Must be able to book flights, hotels and cars internationally
- Must be able to send and receive money internationally

You might be the best shot or hardest puncher in the world but if you can't communicate or get from point A to B without drama, you're a waste of space. Not being able to send funds internationally can lead to delays in tasks be completed or canceled.

One thing I did not list which is an essential skill is to know how to research and set up companies in various locations. For many operations, it helps if your targets think the people they are talking to are in different countries. You can legally and with minimal cost, set up registered companies, virtual offices, phone numbers in numerous countries that can give credibility to any fake websites or social media accounts you might have set up for the operation.

Many times, I have set up jobs where the fraudsters we were looking into and targeting thought they were dealing with companies and people in different countries, when in fact we were in the same city and we had people standing behind them most mornings when they were buying their coffee and doughnuts.

Personal security is something you must take extremely seriously especially if you start investigating and researching corrupt officials and criminals. You must understand that if you are under an active threat, it will also apply to your family, friends and business partners. You need to ensure that the people in your inner circle understand they need to be vigilant for security threats and suspicious of approaching strangers.

Something as simple as bringing someone into your home can cause problems as they will have access to your computers, phones, records, personal space and security protocols. You need to be very careful with personal and professional relationships and should never discuss investigations, operations or targets with people that don't need to know, especially lovers, spouses and family. They can interpret those conversations as casual chats that they can repeat to their bored friends or other family members.

Remember, loyalty is bought, and no-one owes you anything. People will stab you in the back and betray you if it's worth their while, with little concern for the issues or consequences you or your family will have to deal with. If you think this is a harsh outlook, then remember what I said earlier "Most of the things in this book are double-sided".

Your job, or the job you want, involves you buying the loyalty and gaining the trust of people whom you will betray to achieve your objectives, without concern for the issues and consequences they might have to deal with due to your actions. And that's why you're reading this book!

Orlando Wilson
April 2020

INTELLIGENCE

Intelligence is the information we obtain on a target or threat in order to locate them, gain information on their operations and to predict their future actions. Accurate intelligence is not only essential in all security and counter-insurgency operations but also in the corporate world where companies need to know what their competitors are developing and planning.

An easy way to illustrate the importance of intelligence and counterintelligence is this simple example; randomly pick someone online or someone you know and say to yourself "I'm going to kill this person". They are defenseless as they do not even know you are targeting them, if they even know you exist. You can start profiling the target and making your plans for the assassination while they are completely oblivious.

Intelligence and counterintelligence are two sides of the same coin. You cannot expect to be able to source intelligence unless you are alert for others targeting you. Egos and arrogance get people killed. Those who think they know everything and are untouchable are usually the easiest to bring crashing down. Especially if those targeting them are professional, ruthless and unconventional.

There are various means of gathering intelligence but no matter where the information is coming from it needs to be verified and crosschecked to ensure its accuracy and that it is not disinformation provided intentionally. If information and leads are being provided from reliable sources, then every little detail needs to be taken into consideration. One single fact, however apparently insignificant, can open the doors that lead you to your target.

Intelligence gathering can roughly be divided into three areas

- **Surveillance:** This can include physically following a target, watching the target's home or office, hacking telephones and computers to intercept messages, monitor web traffic and movements, etc.
- **Research and Analysis:** Useful information can be found from online news reports, photos, social media, newspapers, radio and trade magazines, etc.
- **Informants and Espionage:** The placing or recruiting of agents and informants with access to the target and their organization can be difficult, time-consuming and dangerous for all involved, but can give you access to the target's plans, documents, networks and the ability to influence or misdirect their activities and goals.

Some of the basic tasks of intelligence operations are to

- Locate criminal and hostile targets.
- Identify criminal and hostile activities.
- Identify the structure, plans and goals of an organization or corporation
- Identify and penetrate an organization or corporation
- Obtain information about an area and its population.

The Intelligence Cycle

The intelligence Cycle is a set of simple bullet points that are used by intelligence agencies to effectively structure their operations.

- **Direction:** You need to know the objectives and goals for every operation be it short or long term.
- **Collection:** You need to have a plan for how you will collect the required information; open-source, informants, surveillance, hacking, etc.
- **Processing:** Once your collection operation starts to deliver information it needs to be checked for accuracy and relevance.
- **Analysis:** When you have accurate and reliable information or leads you need to assess what it actually identifies and how the information can be used.
- **Dissemination:** How will you use the information and who will be informed of your findings.
- **Feedback:** Once your reports have been distributed you will need to wait to see what feedback is given from your clients or the like. Be prepared to defend your finding especially if they are controversial or go against what the client expected to be discovered.

The type of information that will be of use to you will depend on the type of operations that you are conducting. You need to clearly define why you are running your operation and what the required end-results are. Only then you can collate the relevant information required to achieve your goals and start to dismiss false leads, disinformation and irrelevant information.

SECRECY

Nothing is as important professionally or personally as secrecy. All your security, operational or business plans and preparations will be worthless if the bad guys know them. If you cannot protect yourself there is no way you can protect others or work in any potential hostile environments.

Good personal and operational security begins with a clear understanding of what kind of information the criminals or terrorists will be trying to learn about you, your family, business or operations.

Governments must keep secret their diplomatic alliances, secret treaties and military strategies, etc. Although a government may suffer a great loss because of poor security, it is hard to imagine today a situation where a nation's defenses could be completely overwhelmed by a single security leak. However, that is not the case with a small-scale operation.

A company might be ruined as the result of a single security leak. A family might be ambushed and kidnapped because a single piece of information was found out by the criminals, such as home address, security procedures, routes a child takes to school or their travel itinerary.

Things that should be kept secret and restricted

- Addresses and identity of individual employees, their families or close friends.
- Security plans and methods of operation.
- Transportation capabilities.
- Source's supplies.
- Available backup.
- Location of hideouts, safe houses, etc.
- Codes, signals, passwords, and lines of communications.

Good personal security is a must, good team security begins with good personal security. If a person is living or traveling under their own name, they must keep information about their occupation and activities limited to those

who need to know only. There is no one more completely defenseless than the individual whose personal security has been compromised.

Personal security is a 24/7 job, to some, it comes almost instinctively but others can find it very hard to develop. An individual's habits and personality will have a considerable effect on their attitude towards personal security. Some people will just never get it and it can be a liability. Such people should not be allowed access to sensitive information or taken to high-risk locations.

The Basic Principals of Security

- **Deception:** Deception is essential to the success of all security or investigative operations; always have a cover story and be ready with credible explanations as to who you are, what you're doing and why you are doing it.
- **Avoiding attention:** One way for any individual or organization to seriously compromise their security is to attract attention. Always keep a low profile and remember that if people don't know what you are doing, they cannot counteract you.
- **Self-discipline:** Everyone must abide by the rules. If anyone disregards the rules of the security program, they could jeopardize the personal security of all involved.
- **The program:** A security program must be outlined and made clear to all personnel. Everyone must be briefed, trained and willing to work within the program.
- **Continual inspection:** The biggest thieves are usually those trusted with the largest responsibilities- they have access to assets or information worth stealing. The conscientious person with the flawless record can easily deviate by their own accord or with the pressure of a little blackmail. People change and so does the importance they place on their own security; given time people will relax. This is why there is a need for everyone to be constantly inspected.
- **Fluid change:** This is best illustrated by frequent changes of meeting places, routes and operational procedures to keep the criminals guessing. This principle is necessary because, if given enough time, professional criminals can crack the security of any organization. So, old security measures must be constantly and fluidly replaced and

updated.

- **Action:** If someone is not capable of obeying the security program they will need to be disciplined, they should not be trusted or only trusted with information or tasks that will not jeopardize anyone else.

You will not have a security program by following only one or more of these principles, all must be followed, and you must remain alert 24/7.

Basic Counterintelligence

Basic counterintelligence increases the security of all operations and the chances of surprise in offensive operations. Your security program, even if it is for yourself, should be developed to prevent the leaking of information, or situations where criminals can extract information from you or your business.

You could initially be trying to find criminal sympathizers already within your operation; this could be your locally recruited secretary or attorney. If you detect a sympathizer within your operation what are you going to do, fire them or feed them false information? You should also consider why they sympathize with the criminals: is it for money or are they being threatened. Counterintelligence can be broken down in the two practices, denial and detection operations.

Basic denial operations may include

- Thoroughly brief everyone on how the criminals will try to get information on you, your personnel and your operation.
- Place a high emphasis on the security of information. People must understand the need to keep things on a “need to know” basis and not to talk about confidential topics in public.
- Make sure all papers, old computers and communication devices, etc. are properly disposed of.
- Employees should be briefed on the gyms, cafés, bars, clubs and other venues that are safe to frequent socially and those that are not.

Basic detection operations may include

- Background investigations must be done on all employees, especially locals who have access to confidential information.

- Make maximum use of CCTV, covert cameras for detection and overt cameras for deterrence.
- Monitor your staff's communications including e-mail, web activity and telephone calls, , etc.
- Put any staff members acting suspiciously or who seem to be living beyond their means under investigation and surveillance.

These are just some basic considerations, but they can turn your security program into something that would make it extremely difficult for the bad guys to gain information on you. If they cannot get any information on you it makes their job targeting you a lot harder. Hopefully, so hard they'll go and do what we want them to do, find an easier target of which there are plenty.

INTELLIGENCE GATHERING

I wrote the below notes on intelligence gathering a few years ago for a project I was dealing with in West Africa. These notes highlight basic intelligence gathering techniques that can be used against criminals and terrorists but can also be used against you.

A lot of time those engaged in counter-terrorism and organized crime operations do not take adequate counterintelligence precautions to protect themselves, their assets or the operations they are working on. As you read through this chapter think about how you could be targeted and what you could do to prevent information leaks.

The best way to learn how to defend something is to learn how to attack it. So, from a training perspective try targeting others you know with some of the techniques I have listed here. I think you will be surprised to see how vulnerable the vast majority of people are, just try to ensure you're not one of them!

Human Intelligence Gathering

Good intelligence is the most important element in all counterinsurgency (COIN) operations. Your goal is to build an accurate picture of the terrorists' and criminals' network, their identities, safe houses, capabilities, contacts, sources of supplies and finances, etc. Below are a few considerations on how to gain intelligence on terrorist or criminal organizations.

False Intelligence

You must always verify all the information you intercept or is supplied to you, never take things at face value. Unverified information needs to be treated as unreliable or with great caution even if the source is reliable, as they could have been compromised. Sources need to be rated according to their reliability, which can only be done over time. They might have gotten lucky and provided a solid lead once but everything after that one gem still needs to be verified.

When information is supplied, think what was the reason the source supplied it, what was their incentive to supply the information? Are they looking for payment, are they trying to discredit an opponent or lead you into a trap, etc.? All this needs to be analyzed. Over time a source's reliability and value should become clear and they should be rewarded likewise or no longer used unless it's to spread disinformation.

Disinformation is something that can be used either against you or in your favor. The terrorists and criminals can feed you false information to lead you off their trail or into ambushes, etc. That is why all information needs to be verified. If staging an operation based on a source's information precautions need to be taken at all stages of the operations to avoid compromise or ambush. You can also use disinformation to lure the terrorists into arrest or ambush locations and to spread confusion or conflicts within their organization, etc.

These days with social media it's easy to spread disinformation and to use fake profiles to entrap people. From a defensive perspective, you can tag yourself and post photos from locations you're nowhere near to or locations you have under surveillance to see if anyone comes looking for you. From the offensive perspective, setting up fake social media or dating profiles to approach or attract those you're targeting is a basic and proven tactic and a favorite for scammers and identity thieves.

Always be very cautious when analyzing any intelligence that has been supplied to you. Always use your imagination to the max when looking to spread disinformation and don't be afraid to play dirty. If your target's wife receives a message from her husband's pregnant girlfriend that can instigate conflict and discourse, can possibly get the wife to give up the target's location or bring the target out into the open to smooth things over with his disgruntle wife, etc. Use your imagination…

Media & Social Media

You should monitor all media sources such as printed newspapers, social media and the internet for interviews, stories and photos on your target. These days the emphasis is placed on social media but in many developing countries local printed newspapers and radio are the main sources of news and current affairs and should be monitored.

Any journalists who are writing stories about the terrorist or criminal organizations should be monitored and pseudo media operations offering interview opportunities to the terrorist or criminals and their supporters should be considered.

Communications

Once a terrorist or criminal suspect or supporter has been identified you should target their communications. All terrorist and criminal organizations need to be able to communicate internally within their organization and externally with family members, sources of supplies, etc. Interception of the target's lines of communication is an excellent source of valuable intelligence. Remember, if you cannot target the person you are looking for directly then target those whom you suspect they are dealing with and wait for him or her to communicate with them.

- **Mail:** People still use snail mail and written messages can be intercepted, then read or modified to your needs.
- **Landline Phones:** It may come as a shock to many people these days, but landline phones are still used, and payphones can still be found. Landlines are easy to bug with commercially available equipment. If the terrorists or criminals are using payphones, you want to identify any patterns of use via the numbers they are using, then locate and bug the phones as well as put them under remote camera or physical surveillance if your resources and budget allow.
- **Mobile Phones:** If you can access a target's mobile phone you will have access to their location, network and communications. Access can be gained by sending trojan applications, by having sources close to the target install spyware or by gifting new phones, again through sources close to the target. Where budgets allow IMSI-catchers (stingers) should be acquired and employed. IMSI-catchers are devices that are used for intercepting mobile phone traffic and tracking the location and data of mobile phone users. They are expensive and are officially only available to military and law enforcement agencies but are available on the black market. *Warning: Such devices are in the hands of terrorist and criminal organizations as they are bought from or through corrupt officials*

who have access to the equipment or required end-user certificates.

- **Email & Computers:** Unsecured computers and Wi-Fi connections can give you access to a supply of constant and up to date information. As with mobile phones, access can be gained through trojan applications, having sources install spyware, hacking operations or by getting hold of account passwords.
- **Radios:** Most commercial walkie-talkie and CB radio signals can be intercepted with radio scanners. In remote areas a radio scanner on permanent scan will pick up all the radio communications being sent in the area. In urban areas there can be issues with interference due to the number of signals which can be an advantage for the terrorists and criminals but make it difficult for those targeting them.

Family and Friends

Most people only communicate with a small group of family, friends and associates. If you are targeting someone, their friends and family can generally lead you to them. Usually, if someone is OTR (On The Run) or in hiding, it is only a matter of time before they contact their family or known friends, etc.

- The mail, phones, computers and social media of the target's family and associates can be monitored.
- The family and associates can be placed under physical or remote surveillance to see if they contact the target, their associates or are buying supplies for the target.
- The business and home addresses of the target's family and associates can be put under surveillance, mail and phone lines monitored and listening devices placed within the buildings. Also, monitor the electricity or water bills for the building. If the electricity, water usage or food deliveries, etc. increase suddenly, or are in excess for the known occupants, there could possibly be someone hiding in the building.
- Cars of the target's family and associates can be fitted with tracking and listening devices.

Locals and Neighbors

Locals and neighbors of the target, their family and associates can prove to be good sources of intelligence. Send a socially skilled operative to speak with them paying special attention to anyone who shows a dislike for the target, their family and associates. Local children can also provide information on activity in the area and might not be as guarded and keener to talk than adults.

Documents

Any seized or acquired papers need to be analyzed for forensics as well as the information they contain. Even the smallest pieces of paperwork should not be overlooked, such as shopping receipts that show locations, dates and times, etc. that can be acquired from the target or their family's garbage, etc.

Sources of Supplies

All terrorist and criminal organizations need to be supplied with weapons, ammunition, food, medical equipment, gasoline and cash, etc. For example, mobile phones need SIM cards and the accounts need to be topped up with funds, so where and how are the terrorist or criminals doing this? Once sources are identified they can then be monitored, and the supplies tracked to the target or modified before delivery.

Routes or Areas Frequented

Suspected routes used and locations frequented for social activity, etc. by the target should be monitored or ambushed. If the target is spotted, they can be followed or arrested, etc. as can their known associates.

If you're sending people to hang out in cafés, bars or clubs frequented by your targets ensure they fit in with the other people in that location. A rigid former career soldier in his 40's will not fit in with an under 25 crowd at a pool party, unless he's pretending to be someone's sugar daddy. If you're sending people into bars make sure they have some tolerance for alcohol and won't be drunk, acting stupid and talking too much after a few beers. If you're sending people into brothels or strip bars make sure they have some life experience and won't be acting like terrified virgins or excited

adolescents when they see a naked woman.

Rewards

Rewards can be offered for information on the targets. All information would need to be verified as you can expect a large amount of bogus information, if not outright disinformation, to be called in. Rewards need to be paid if the information supplied proves to be accurate. Not paying rewards would lead to the program losing its credibility very quickly.

Spying Operations

Where possible, a network of informers (sources) should be established. You should seek to recruit people who could have information on the targets or are close to them. Methods of recruitment for sources varies greatly from person to person and depends a lot on their personality and reason for giving up information on the target. Our initial phase is to find people who have a grudge against the target; they could be owed money, be ex-lovers, etc. They could possibly still be in contact with the target or be able to establish communications because they are seeking revenge or compensation in return for cooperating.

The second group of potential recruits would be those who under normal circumstances would not be considered sources of information. These are people who would need to be persuaded to provide information on the targets. If you believe someone could provide you with information and be a semi-reliable source, you will need to compile a lifestyle check on the person and identify anything that could be used against them. Such as debts, vices (sex, drug or alcohol use, gambling, etc.), extramarital affairs, criminal activity, etc. that they would not want to become public knowledge and, would be willing to provide information on the target to prevent this from happening. A little pressure can sometimes work wonders and useful information and actions should always be rewarded.

Sources and informants need to understand that they should not let anyone know they are working for or with you. I know of one situation in the US where a businessman had a falling out with someone who happened to be an auxiliary cop, which means they made donations to a police department to be given a police badge.

The businessman was approached by the local police out of the blue for bullshit reasons on numerous occasions and a few days after every incident the auxiliary cop always tried to contact the businessman, even though he had blocked his known phone numbers and social media accounts.

We take it the auxiliary cop was giving bullshit reports to his cop buddies so they would fuck with the businessman. The reason the auxiliary cop was trying to contact the businessman was part of his egotistical power trip: he wanted to show the businessman he could fuck with him. You need to ensure the people you recruit are not prone to going on power trips or spending sprees with any cash you give them as they can end up compromising whole operations and getting themselves and others killed.

Everyone in your network should be offered some form of compensation. If you identify a potential source has debts, then money could be the only incentive they need to provide information on the target. Any exchanges of cash or assets with sources need to be videoed and could be used in the future if the source becomes uncooperative.

Official records need to be kept on all sources and informants, but in high-risk environments, where your communications devices and records could be compromised you need to be very careful. Code names need to be allocated for sources and informants so they cannot be identified by 3rd parties and in high-risk environments their personal photos and details need to be kept off record. Source records can include:

- Name, photograph, and physical description of the source.
- Home and business addresses
- Details of family
- Details of lovers and extramarital affairs
- Details of business partners
- Source’s motivation for providing information
- How the source was developed
- Area in which the source can obtain information
- Source’s connections with criminal or terrorist organizations
- Method by which the source can be contacted
- Record of payments or other remuneration
- Productivity and reliability of the source.

Source Security

The identities of your sources must be kept on a “need to know” basis, code names need to be allocated and used as soon as a potential source is identified. The personal security of the source and their family needs to be considered always. If a source is compromised, they need to be informed and if possible relocated ASAP.

If a source is killed or kidnapped, it can lead to fear in other sources who may become uncooperative. It would be good operational procedure for a terrorist group to routinely punish or execute suspected informants within their organizations. Even if those executed were innocent it would serve as a severe warning to those considering becoming informants.

If people know they are safe and will be looked after, they will be more productive. All files and evidence on sources need to be kept secure, encrypted and quickly disposable. That being said, security concerns for a source always need to be evaluated and should never inhibit the success of an operation.

The Placing of Undercover Operatives

This is a situation where one of your operatives tries to infiltrate the terrorist or criminal organization. Your operative would need to appear to be a sympathizer to the terrorist cause and have similar interests to those he or she is seeking to become friends with.

When a suitable terrorist or one of their supporters is identified, the operative would try to strike up a relationship with them. The initial approach would not be about the terrorist’s cause but should be about a common interest such as sports, food, dating, etc. You would need to compile a lifestyle check on the target for the operative and identify anything that could assist them in building a relationship with the target.

A suitable time and location for this first approach would need to be determined, this is when things can get off to a good start or no start at all. Over time it would be the operative’s job to win the confidence of their target. The path the relationship takes will determine how the target could be used. If they are loyal to their cause they should hopefully be able to supply

valuable information. If they are disgruntled with their cause they could be turned or guided to cause friction within the terrorist or criminal organization.

How involved the operative will become with the target and the terrorist or criminal organizations will depend on the situation and their safety. If an operative is left in place dealing with the terrorists or criminals for an extended period there is a chance, they themselves could turn to the terrorist or criminal cause. The operative's mental wellbeing needs to be closely monitored and they should be given continuous reassurance and support.

Honey Traps

Honey Traps are a spy and criminal tactic that has been around for as long as humans have, but still people, usually men, end up getting entrapped, extorted, kidnapped or murdered. The trap is simple, usually a woman provides or promises a man sexual favors used to blackmail him or to lure him to a location to be killed or kidnapped, etc… The threat is that prevalent that in May 2018 the British Security Service MI5 distributed the "The Smart Traveler" booklet to help protect UK businessmen from honey traps, substance misuse and other entrapment tactics while doing business abroad.

Now think about it: which of the guys you know would say "NO" to an afternoon of sexual games with two attractive young women if you offered it as a gift? Not many, I expect, well I know for a fact… Such a gift can be easily arranged. You just need two female (or male) prostitutes, a hotel room or better still an apartment or an Airbnb these days. Apartments give more privacy and can be easier to rig cameras in… Then the target's afternoon of sexual ecstasy will quickly turn into a nightmare for their foreseeable future…

Honey traps happen all the time and have since men's dicks controlled their brains, so forever. At the low end of the scale, the hot chick will promise a night of debauchery but will just take her target to a shady hotel room or apartment where they can be beaten, robbed and maybe raped by her waiting accomplices. At a higher level, a more intricate honey trap can go on for an extended period of time until the target believes it's some form of relationship, of course, the sex - the more deviant the better - would be videoed and then used to blackmail them for business favors or hard currency.

A common criminal tactic is to pimp out a girl or boy who looks of the legal consenting age for sex and then claim after the sex has taken place, they are underage. That way they have a lot of leverage on the unfortunate and stupid gent who has, unknowingly, possibly committed a serious criminal act: sex with a minor.

Psychological Operations

In simple terms psychological operations are media campaigns and other such actions to impact the opinions, emotions, attitudes, and behavior of hostile, neutral, or friendly groups to support the achievement of your desired objectives. Within counter-criminal and terrorist operations properly employed psychological operations can help you gain support and promote a favorable image of your organization or your clients and at the same time discredit your opponents.

You need to consider who are the audiences that you need to influence and tailor the information that is given to them to ensure they respond as required. This is where accurate intelligence combined with disinformation can be packaged and distributed to ensure it has the maximum effect. Your audiences can include:

- **Your opponents:** Work out a campaign to discredit and isolate them from their family, friends and supporters.
- **Those supporting your opponents:** Highlight betrayals and failures that can cause infighting and division.
- **Those who are supporting you or your clients:** Promote any injustices you have suffered and how you're working to rectify the wrongs done to you, your associates and the community.
- **Those who are neutral:** You need to convince this group that your actions or those of your clients are justified and that you have been victimized. Also, highlight the negative actions and crimes of your opponents.

Psychological operations when properly planned can have a devastating effect on the public image and reputation of an individual or organization. These days what the public views on social media can prove to be someone's judge, jury and executioner.

Dissemination

Once you have the information, photos or evidence you were after you have to work out and plan how you are going to use it. These days with social media it's easy to promote stories and videos to a vast audience very quickly and affordably. It does not take much time or skill to set up social media accounts to host stories, photos, videos that can then be promoted to the audiences you want.

For non-virtual and real-world applications, understanding people's circumstances and thought processes can help you solve a multitude of problems legally and discreetly. I once helped an overtly happily married client that was being extorted by a ghetto prostitute he invited to his house when his wife and kids were away for the weekend.

To cut a long story short, after making it obvious in the neighborhood where this young lady lived that we were looking for her and wanted a chat, for some reason she did want to talk to me… So, I ended up calling her mobile number that I had from day one. Of course, she knew I was the guy that was looking for her and she offered to meet me and to bring her people with all their guns, which was an expected response.

I asked her a simple question, "What would the people in your neighborhood do if they found out you just ripped someone off for $50,000?". That one question stopped the client being extorted and the girl, stopped contacting him. She knew what the people in her neighborhood would do and so did I. Everything my associates I had done was legal, and we solved the problem, because we had taken the time to understand the target and their environment.

Conclusion

This is just a short chapter on the basics of gathering human intelligence but can also be used as a guide for counterintelligence if you just place yourselves in the target's place.

Where budgets are available there are plenty of electronic surveillance options available these days but if you do not have the budget then the low-tech traditional methods of gathering human intelligence are still as reliable

today as they were thousands of years ago when people started spying on each other, which I expect was about the same time they learned how to walk and talk…

COUNTER-SURVEILLANCE

If you are engaged in investigating corrupt officials, criminals or terrorists you must understand the basics of counter-surveillance. Be assured, if these people find out you are looking into their businesses and activities, they will target you.

If you are serious about your personal security, basic counter-surveillance procedures should be part of your daily routine. The reason you need to understand counter-surveillance is to identify anyone who has you under surveillance. Take precautions when you leave and enter your home or office and especially when you're meeting with informants or sources.

In nearly all burglaries, muggings, robberies, assassinations, or kidnappings the criminals or terrorists will put their target under surveillance to assess their target's routines and the level of personal security. If you're operating in an area where professional organized criminal groups or narco-terrorists are active you can be assured, they will be employing multi-layered surveillance programs to identify threats to their organizations and to identify potential targets for kidnapping or extortion.

Counter-surveillance is the base skill for all personal security programs. In this short chapter, I am going to highlight some of the main considerations for a counter-surveillance plan and detail some simple but effective street drills that will enable you to identify if you are under surveillance.

Many supposed security professionals put a lot of time, effort and money into firearms and unarmed combat training, but very few spend any time or effort on their surveillance and counter-surveillance skills.

Professional surveillance operatives put their targets into three categories: unaware, aware and professional. Most people, I would say at least 75%, fall into the unaware category: you can follow them around all day, and they won't realize you're there. Give it a try the next time you're out at the mall! About 24% of people would fall into the aware category and

would realize, after a while if someone was watching or following them. The 1% left would fall into the professional category; they take active counter-surveillance measures and would spot people acting suspicious, watching or following them. So, I expect most people reading this chapter are in the unaware category but by the time you finish reading this, there is no reason not to be in the professional category.

The Basics

You can start training while you're reading this chapter. Look around where you are now, if you're in an office look out the window. Are there any people hanging around on the street or sitting in parked cars for no apparent reason? If they are still there in 30 minutes and there is no logical reason, what are they up to, what's their body language saying, are they being over observant? People don't hang around the streets and sit in parked cars for no reason unless they are on surveillance or up to something!

Learning to read people's body language is an extremely important skill. If someone is on surveillance or looking to commit a crime, chances are they will be acting differently than those around them. Most people do not pay attention to their surroundings, so if someone is over observant, what are they up to?

When you are out at the mall or in a restaurant or bar, watch the people around you and try to identify what mood they are in or what type of discussion they are having with others. It should be easy to identify if a man and a woman are on a romantic date or two business people are having a heated discussion. When in a coffee shop try to determine what people are looking at on their laptops; are they concentrating or goofing around. Learning to read body language is of paramount importance because it will help you identify, avoid and if necessary, react to potential threats.

A basic counter-surveillance plan for your home, business or office would be to simply look around the general area and identify the location(s) from which you could be watched, then check it from time to time. If someone is hanging around that area take note; if they are there for an extended time or show up regularly, what are they doing?

These days if you're drawing up a counter-surveillance plan you need to take surveillance cameras into consideration. There is a vast array of affordable surveillance cameras on the market that can be used either defensively, to watch potential surveillance locations you've identified, or offensively, by someone intent to spy on you. For example, at a very basic level, why sit outside someone's house and watch them when you can place a $100 hunting trail camera in their garden? Retrieve it after a few days and you will have photos/video of all their comings and goings. If your budget allows it, why not place a camera connected to a GSM network that will send real-time images to your cell phone or email? Here I am talking about regular commercial hunting cameras available at Wal-Mart, not specialized remote surveillance cameras. But no worries, as I am sure everyone reading this regularly sweeps their gardens and parking lots for surveillance cameras, right?

I am old school and believe that you need to be able to operate with minimum equipment and support but should employ technology when you have access to it, just don't be 100% reliant on it. Nowadays drones are easily available to the public and can be used for surveillance and counter-surveillance. Things that need to be considered when using drones are their camera quality, flight time, weather conditions they will be used in and from the good guy's point of view, what are the laws regarding their use in your area. Even within a small-scale private security operation drones could be employed for estate security, for clearance, perimeter patrols, and route checks, etc.

To dominate the area around a location you would need to patrol it and pay special attention to potential surveillance locations, think like the criminals or terrorists and put yourself in their shoes: how would YOU watch YOURSELF? When I say patrol an area, I do not mean you need to dress up in tactical gear and pretend to be RoboCop. You can patrol an area by going for a casual walk, walking a dog or taking a bicycle ride, etc. While patrolling you want to look for people or cars that are out of place, cameras, and ground signs that people have been waiting in specific locations such as cigarette butts, trash, or trampled vegetation.

Overt patrols only draw attention and will alert your opposition that you

are taking active measures, which will then up their skill level and cause them to retreat to farther out positions. If you identify you are under surveillance without alerting your opposition, there are many ways to exploit the situation. How you do so will depend on the overall circumstances of the operation, your resources, and the laws you are working under. All of this needs to be considered in your operational planning.

In urban areas surveillance operatives use as cover locations where people congregate, such as cafés, bars, bus stops or payphones. If someone is sitting in the coffee shop across the road from your office all day they may just be working there, but if you see them on the subway or at another location, then maybe you have a stalker, private investigator, or criminal on your tail.

If you think you are under surveillance you need to establish why and who the threat is: criminals, government, a lone stalker, private investigators, or a crazy ex. You need to do this, so you can determine their potential skill level and consider what other type of surveillance is being used against you: listening devices, remote cameras, mail being intercepted, computers being hacked or physical surveillance?

These days we must ensure our computers, smartphones and internet connections are secure; if the criminals or terrorists get access to these, for most people it means they will know all personal details. I am still surprised that currently a lot of people still have no security on their phones or computers, post personal information, and photos on public social media accounts. I think these days it’s suspicious if someone does not use social media to some extent, personally I think most platforms are safe enough, just understand whatever you post is or can become public.

Computer and network security are a constantly evolving specialized industry that needs to be left to the experts, but social engineering is something everyone in the security industry needs to understand. In basic terms, social engineering is some form of confidence trick used to gather intelligence, defraud or get access to computer systems, etc. A lot of successful computer hacks are just successful social engineering operations rather than network penetrations. Social engineering operations are disguised

as regular everyday happenings that fit in with the target's lifestyle. For example, the bored middle-aged CEO gets a Facebook friend request from an attractive young lady, he confirms the request and starts chatting and trying to impress her. The young lady's Facebook profile can be a complete fraud made up by those targeting the CEO or other members of his corporation. By just confirming the friend request the CEO has given the criminals or terrorists access to a wealth of information, and will give up more in his ongoing conversations and hopefully emails from his corporate account…

Just think about how many people can access your computer, for example colleagues at your office. If you leave your computer at the office overnight can maintenance, security or cleaning staff get access to it? There have been cases of corporate espionage where private detective agencies have placed agents in the cleaning and security staff working at their target's offices, so they can access the target company's computers and trash after work hours. Most people would not consider as a threat the bumbling night shift security guard or the apparently barely literate office cleaner. Both could be downloading business data from their computer or copying confidential papers, and they should be viewed as a threat!

You cannot carry your computers around with you all the time so, one thing to do is to keep minimum information on it. Keep all your sensitive information on a thumb drive or hard drive, which you can always keep on your person. Then if someone accesses your computer or if it's lost or stolen the criminals won't get anything worthwhile information.

The next time you are in a coffee shop for example, without being obvious, look at what people are doing on their computers, phones and listen in to their conversations. Many people regularly work in public locations where anyone can view their computer screens, with unsecured Wi-Fi connections with the same comfort level they would have at home. When chatting with friends in public, people disclose all the time personal information that could be useful to a criminal. So, remember, if you can view what others are doing on their computers or phones and listen to their conversations, others could do the same to you if given the opportunity.

If you believe your computers or phones are bugged then you need to get

them cleaned, which can be costly and difficult in some locations. Another option is to use misinformation to mislead or entrap those who may be monitoring you. This could be a safer option rather than letting the criminals or terrorists know that their operation is compromised, which could force them into acting.

Street Drills

You must always be on the lookout for criminal surveillance and here I have listed a few simple drills, which are used by professional criminals and intelligence operatives alike. These simple drills will help you identify anyone who is watching or following you. First, let me give you an example from the mid-1990s when I was part of a commercial surveillance team in central London whose task was to watch a target that turned out to be in the professional category.

The people running the job had placed a surveillance vehicle, an old British Telecom van, across the road from the target's hotel. The target, I expect, identified the van quickly; tinted rear windows, parked in one position for an extended period, etc. If I remember correctly on the first day the target left the hotel, jumped into a black cab and we lost him straight away due to traffic. On day two the target took the subway and went for a walk around the West End of London. He used several of the counter-surveillance drills I have listed here and ripped the surveillance team apart! Those running the job resorted to placing a pseudo-married couple in the hotel to try to observe what the target was doing and talking about in the bar and restaurant. Running surveillance on aware and professional targets can be extremely difficult, it's not like the movies. You should always be at the aware level but preferably professional level of awareness and it's not difficult to accomplish that!

Adapt a few of these drills to your situation, they are simple and proven.

- When walking on the street, turn around and walk back the same way you came; remember the people you walk past or anyone that stops. Also, remember to check on the opposite side of the street for anyone stopping, etc. Do this several times and if you see the same

person or couples more than once, they may be following you.

- If you are driving, do a couple of U-turns, watch for anyone doing the same and the cars you pass. If you see the same car a couple of times you may be followed.
- Walk around a corner, stop, and remember the first few people that come after you. Again, do this several times and, if you see the same person more than once, they may be following you. Watch the body language of those that come around the corner after you, any flinch could be an indication you have surprised them. You can also do the same when you're driving. From a personal security standpoint remember to always take corners wide as you never know what's waiting for you on the other side.
- Escalators are good for counter-surveillance because while ascending, you can have a good look around at who is behind you. A simple drill would be to go up an escalator and straight back down again. If anyone is following you, they would have to do the same.
- Take special note of people waiting in parked cars, especially near your residence or office. Be especially suspicious of any unattended vans with blacked-out windows parked close to your residence or office. Vans are the most common surveillance and snatch vehicles. As the saying goes: there are only two reasons for two people to be waiting in a car for no apparent reason: they are either having sex or they are on surveillance.
- Do not board trains or buses until the last minute; anyone boarding after you should be treated as suspect.
- Jump on a bus, tram or metro and jump off one stop later and see if anyone else does the same. People usually don't bother getting on a bus to go only 200 yards.
- Go into a café and covertly watch what goes on in the street. Look out for people waiting around to follow you when you leave or anyone who keeps walking past the café, they could be trying to see what you're doing. Pay special attention to locations where people are congregating for legitimate reasons, such as bus stops, cafés, etc…
- Walk across open spaces such as parks or squares and see if anyone is running around the outside of the open area trying to keep up with

you- they must do this because there is no cover for them in the open space and the distance to go around the open space is greater than walking straight across it.

- Use reflections from windows and other surfaces to see who is behind you or use the selfie camera on your cell phone.
- Watch out for people who look out of place or are waiting in the same spot for a long time, such as waiting at a bus stop without getting on any buses or at a payphone for an extended period.
- Be aware of people waiting in a location by themselves, especially fit, young men with short hair. Chances are they are criminals or police. Professional surveillance teams usually consist of mixed couples in their 30's to 50's. Criminals regularly use children, so be wary!
- If you think someone is following you, do not acknowledge them, just slow down and stop to look in shop windows, or go into a café and have a coffee. If you still see the person waiting around, you are most probably under surveillance.
- When you're driving, drive slowly, and take note of anyone doing the same, occasionally pull over and make note of the cars that go past you, if you see the same car more than once you might have a problem.
- If you do not want to look directly at someone who could be following you, look at their feet and remember their shoes. Very few people wear the same shoes, check this out the next time you are out. If you keep seeing the same pair of shoes at various locations, this person could be following you.
- Criminals following you may change their hair, jackets and pants, etc. to try and disguise themselves but they rarely change their shoes. The same goes for jewelry or watches, it can be difficult to give a description of someone so look for distinctive jewelry, tattoos, type of cell phone or anything that makes them stand out. If the person is completely nondescript, chances are they are pros.
- If you think someone is following you check their dress to see if they could be concealing cameras or weapons. Are they always on their cell phone possibly describing your actions or taking photos? What does their body language say, do they look nervous, over observant,

or as if they are concentrating too much, etc.?

- Be suspicious of unknown people who start conversations with you- they could be testing your reactions and personal security level.
- You need to be extra vigilant when attending any meetings. In high-risk situations, these could have been set up by the opposition to photograph you or set you up to be kidnapped or assassinated. Always sweep the area for anything suspicious - people or vehicles - before attending the meeting.
- If you think the opposition is trying to get photos or video of you, meet in places where there is low light, like dark restaurants and stay in the shadows as most cameras will not be able to get decent pictures.
- If you believe someone is trying to get audio recordings of you, meet in a crowded place and keep your voice low. The noise from other people or traffic, etc. would be picked up by any microphones and can cover your conversation.
- To check whether the person with whom you are meeting is under surveillance, turn up 5 minutes late and sweep the area for anyone suspicious. Try to take the person you're meeting with to another location and do a couple of discreet counter-surveillance maneuvers along the way.
- Stop regularly to make telephone calls or look in shop windows as this will allow you to observe your surroundings and identify anyone who may be following you.
- Use underground trains whenever available- radios and mobile phones usually don't work underground. This will cause problems for any surveillance team as they won't be able to communicate with each other.
- You must make plans on what procedures you will carry out if you are under surveillance. These will depend on where you are and the threat you are under. These days if you think you're being watched, chances are the criminals, terrorists or stalker have already tried to hack your phone or computer, so get them cleaned up and secured!

From a personal security point of view if you are on the street and you seriously think you are being followed get to a safe area as soon as possible

and call for someone trusted to come and pick you up. From a close protection operations point of view, there are various tactics you can employ if you want to identify those following you or to warn them off, all depends on where you are and the overall operational plan.

In First World countries, you can inform the police, but I strongly expect they won't take the call seriously unless there is a domestic restraining order in place or there is a case history. If you or your client are being stalked you need to start building up evidence against the stalker, take videos and keep a log of the occurrences. If someone is watching your home or business call the police and report it, if they are not busy, they may respond and question the individual, etc. Depending on the case this could lead to a loitering ticket, an arrest or nothing, but a least you have a record of calling the police for your file.

I've had numerous clients over the years who've had issues with private detectives following and watching them. If you are being stalked and harassed by private detectives call the police on them, they have no special authority, their badges just mean they are licensed, if that. They cannot trespass, go through garbage, or inhibit your lifestyle, etc. If the police can't help, then a written complaint to their licensing authority with evidence of their actions tends to work!

This is a short chapter on a very important and in-depth subject that cannot be learned from a book, I hope it makes you think about your personal security procedures and assists you in your operational planning.

ELECTRONIC SURVEILLANCE

Electronic surveillance is a main intelligence gathering resource for governments, criminals, terrorists and private investigators. You need to understand that you can employ electronic surveillance when you are targeting others but, it can also be used against you!

It is easy to get hold of listening devices (bugs), bugging equipment and covert cameras from commercial outlets and the many shops that specialize in making and supplying this type of equipment. Today, many bugs and covert cameras can be hidden in almost any object like books, computers, mobile phones, rocks, and clothing. You should always take precautions against bugs and covert cameras, especially when you are staying in hotels or moving into a new residence.

There are thousands of devices on the commercial market that claim to be able to detect bugs. However, bugs work on many different frequencies or on GSM networks and many commercially available bugs and bug detectors work on only a small sector of frequencies available. A professional criminal or terrorist will always try to use bugs that are outside of the usual frequencies or on GSM networks, so they stand less chance of detection. In addition, you must take into consideration remote-controlled bugs that can be turned on and off by the listener. With most equipment, you would not pick up this type of bug, because it would usually be turned off until needed, such as during a meeting. In this sector, the most expensive equipment is not always the best. If you consider buying it, make sure it does what the maker claims.

If your threat is from electric surveillance (ES), you should employ the services of a trusted specialist in the electronic counter-surveillance (ECM) field. Always check the credentials of the person you employ for this task and make sure he is trustworthy, also check out that his ECM kit is of a professional standard. An ECM specialist should also have the equipment that is required to find bugs that are not within the usual frequency ranges. If you use the services of a commercial ECM specialist, they must never be left unsupervised. There have been many cases where de-buggers have been

found to be working for the opposition and planting or ignoring devices.

You should also be aware of the threat from “hard-wire” devices. These do not transmit information via the airways and cannot be detected by scanners, etc. A listen through a wall device is a good example of this type of device. The device could be placed on the outside of a meeting/hotel room and pick up all conversation taking place in the room and the device could be attached directly to a recorder. There are government agencies claiming to have a microfiber device that they can stretch for 3 kilometers and receive good quality audio and video footage.

It would be unrealistic for you to always carry around with you ECM equipment. The best defense you have against these devices is to perform a physical search whenever you will be staying for some time in a room or moving into a new residence. You should always carry with you such equipment as a torch and a Swiss Army knife type or tool. These basic items are all you should need to adequately perform a basic room search. If you anticipate that you will have to do an in-depth search always take a full search kit.

How A Bug Could Be Placed

Consider this scenario: a criminal is targeting an executive for kidnapping. He needs to get information on the executive’s movements, routine, etc. A simple tactic would be to place a listening device in the reception area of the target’s office. The criminal would need to buy a simple, small listening device which could be bought over the internet or from a spy shop. The criminal would then task an associate, preferably female, to enter the reception area and ask the receptionists for directions, etc. While talking to the receptionists the female could blow her nose and ask them to let her put her tissue in their trash can. Wrapped in the tissue would be the bug. Who would ever ask to check a tissue someone has just blown their nose in! All going well the bug would now be in place and would pick up everything the receptionists are saying. Think about it, receptionists handle a lot of sensitive information: they make appointments, book taxis and restaurants, etc. A small bug could transmit for about 20 to 75 meters depending on its quality and the environment it’s used in. If someone could not covertly get close enough to listen to it, a receiver attached to a digital voice activated recorder could be placed close by in a flower bed or up a drainpipe, etc. GSM bugs

use SIM cards so they can be listened to globally from any location with a phone connection.

Considerations

- Why might your client be under electronic surveillance?
- Who is the threat? Criminal, government, commercial, personal?
- What is the expected level of skill and equipment of the opposition?
- What information about you does the opposition have?

Counter Procedures

- Change meeting rooms and places at short notice- this will cause problems for anyone who was planning to put you under electronic surveillance.
- Search rooms prior to meetings.
- Clear everyone from the room/area before the search and then secure the area and allow access to authorized personnel only after the search is finished.
- Upgrade the security of all areas and employ your own personnel in a counter-surveillance role.
- Physically search the area for suspect vehicles which could be used as a receiving/relay point for transmissions from a bug.
- Leave enough time to search the area before the meeting starts.
- Meeting rooms should have minimal furniture as this gives the opposition fewer places to plant bugs.
- Search everyone entering meeting rooms for recorders or transmitters and make sure all rubbish is searched and removed.
- Check any vacant-adjoining buildings and physically search the outside of buildings.
- Perform counter-surveillance physical and electronic during meetings.
- Keep a frequency scanner on permanent scan.
- Be aware of remote-controlled bugs.
- Search pictures, sockets, phones, plugs, any gifts. Place tape over screw heads, check any new furnishings, check ceiling panels,

check outside the room.
- Draw curtains or close blinds before those attending the meeting enter the room.

Cell/mobile phones can also be used as listening devices when set to auto-answer. Once they are put in place the threat just calls the phone to hear what is being said in the close vicinity around the phone. The only limitations cell phones have, are their size and battery life. The other issue with cell/mobile is that they can be hacked or have surveillance apps installed. There are many commercially available surveillance apps for cell/mobile phone monitoring. In high-crime areas where the criminals are working with the police and cell phone companies, they can monitor your calls and e-mails via the servers.

Another cover for planting electronic surveillance devices are burglaries. If you came home and found that your house or car had been broken into would you be more worried about what had been stolen or what had been put in place? If your car, house or hotel room has been broken into they need to be searched for electronic surveillance devices and contraband. I mentioned cars here because they are favored areas to plant listening devices as they are generally easier for the criminal or private investigator to get access to and break into than a residence. Also, consider what you discuss in your car; many an extramarital affair has been discovered or confirmed by a voice-activated Dictaphone placed in a straying spouse's car.

Dictaphones on their own can be used by criminals as listening devices. When combined with a miniature microphone (that can be bought from most electronics stores) they make an excellent hardwire device. Dictaphones these days can record more than seventy-two hours and the data transfers easily to a computer. Consider how easy it would be for a criminal to get access to the outside walls or roof of the location you're in right now!!! Drill a small hole through to the inside and then place the microphone in the hole. Outside, the microphone wire could be camouflaged and the Dictaphone waterproofed and concealed, even buried. Then, every few days, the criminal could come by and swap the Dictaphone for one with fresh batteries and memory. The only way to find such a device would be a physical search; the $25K bug locator and the $500.00/ hour specialist would be nothing more than a waste of time and money.

Hopefully, after reading this chapter, you are more aware of the threat from electronic surveillance and how easy it is for even low-level criminals to use this means of gathering intelligence on an intended target.

ATTENDING MEETINGS

Meetings can be extremely dangerous and should always be treated with caution. This is when people will know where you will be at a specific time, exactly what the bad guys want to know. Arranging meetings is an easy way to set someone up for kidnapping, assassination, sexual assault or robbery.

Meetings should be kept as secret as possible and planned well in advance. When under a high- level threat you want to exchange the maximum amount of information with those you are meeting within the shortest possible time.

Firstly, you will need to select a suitable meeting location, be it a coffee shop or a hotel suite, this will depend on how many people you'll be meeting with, what's to be discussed and what is the threat level. You should always have a reason and cover story for being in that area at that time in case the meeting is compromised; for example, maybe you or those you are meeting with have identified they are under active surveillance.

Everyone involved in the meeting will need a covert way of alerting the others that they have been followed or are under active surveillance. This can be done by using codes or signs en-route to the meeting location or quickly posted comments on online chat boards or social media sites. This way if one person is compromised, they should not compromise or endanger the rest of the participants. Cell phones should not be used or taken to sensitive meetings as they can be tracked and used as listening devices; they should also not be used to warn others that you are under surveillance, calls and text messages would lead straight to those you were meeting with. A low-tech method, such as you drinking soda instead of coffee, or putting the "Do not disturb" sign on the hotel suite door could signal the others that things have gone bad.

Whenever you are meeting people for the first time you should always use prearranged signs and countersigns to confirm their identity. The simplest thing is a pre-arranged question and answer, this works better than checking ID cards as the person you're meeting with might be the right person, but you

know them by a pseudonym. In a basic context, you want to make sure the limo driver who is meeting you at the airport is your real driver and will take you to your hotel not into months of captivity or to a garbage dump!

Considerations for Attending Meetings

- Do you know in detail the meeting location? If not, then check it or get someone trusted to check it.
- Things to take into consideration include the facilities (bathrooms, cafés, taxis, payphones, etc.), potential surveillance positions, location of surveillance cameras, escape routes.
- Will it be daylight or dark?
- What is the condition of pedestrian and vehicle traffic, what are people wearing, age and type of people in the area?
- Make plans and procedures for all possible emergencies identified in your threat assessment.
- Consider where along your route to the meeting location you would put surveillance personnel to watch you if you were the opposition and identify where on your approach to the meeting location you would be channeled.
- How will you get to the meeting location: walking, using public transport or driving?
- If driving, where will you park your car, will it be secure or hidden, how long would it take you to get back to it in an emergency and what are you going to do if it’s compromised?
- What will you wear for the meeting and will you need a change of clothes; remember it’s always easier to dress down than up. You can always take off a sports coat and shirt and put them in a plastic bag.
- Will you be carrying any weapons and is there any risk of being searched?
- Always be aware of what’s going on in the environment around you; watch for warning signs posted by the those you’re meeting with that could indicate they have been compromised, any unusual activity, people waiting in cars or vans with blacked out windows, fit young men with short hair hanging around for no reason, read the body language of those waiting in possible surveillance

positions, etc.

- When you reach the meeting location, sweep the area for anything suspicious, you might not be under surveillance but the person you're meeting with could be.
- If you can, select a good position at the meeting location from where you can view as many entrances as possible, be close to escape routes and view what's going on the street outside without being in clear view from outside.
- Locate those you are meeting with and exchange passwords, consider walking them to another location to identify if they are under surveillance.
- If you are going to eat and drink, consider the method of payment; credit cards leave a paper trail.
- Also, do not leave your food or drink unattended or let anyone fetch you a drink from the bar, etc. as this is an opportunity to drug it.
- Under a high threat make sure you do not leave anything behind from which fingerprints or DNA samples could be taken.
- During the meeting constantly watch for physical, video and audio surveillance, if you have the manpower get a trusted associate to do this for you and to watch your back.
- Keep the meeting as short as possible and when it's is over, leave the area as quickly as possible and conduct several counter-surveillance drills, consider changing your appearance if necessary.
- If further meetings are required, they would have to be varied for different times of day and days of the week.

COVERT COMMUNICATIONS

The basis for good communications security these days is understanding that all electronic communications and devices are not secure. All hardware such phones and computers as well as software and applications are hackable or have a backdoor that are provided to governments as part of the licensing agreements. Remember no communications are 100% secure from eavesdropping or interception.

In many countries corrupt government officials and employees of intelligence agencies work hand in hand with criminal groups and sell intercepted communications or will work directly for the criminals. Also, many employees of phone and internet companies have access to the users of their networks data, locations, phone call and messaging records, all of which can be given to government agencies or sold to those with sufficient cash. All communications that go through mobile phone towers and communication companies' servers leaves a history.

Also, there is the threat from devices that can intercept mobile communications such as IMSI-Catchers. An international mobile subscriber identity-catcher, or IMSI-catcher, is a mobile eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users. The IMSI-catchers are essentially a "fake" mobile communications tower that acts in between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle attack.

IMSI-Catchers are restricted items that require government documentation to buy, just the same as weapons systems. But they are available for purchase on the black market from corrupt government officials or manufacturers that are based in locations or sell in or through locations that have weak communications laws and restrictions. For example, IMSI catchers are used in many African countries, in one country it was reported that the foreign operators of the IMSI-catchers were selling the retrieved data and communications to both sides involved in a contested and heated

election.

All smartphone applications have backdoors and are monitored. Such applications as WhatsApp etc. would not be given operating license if they did not cooperate with the authorities in the countries where their apps are used. In numerous countries messaging apps and voice calling apps are blocked for national security issues.

There have also been some messaging applications that have been set up by government agencies specifically for catching and intercepting criminals', journalists, and activists communications. The ANOM messaging app was jointly invented by the Australian Police and the US FBI. Smartphones and computers with the ANOM app installed on them were distributed to known criminals, allowing police to monitor their chats about drug smuggling, money laundering and even murder plots. Another example is the EncroChat encrypted messaging app that was penetrated by French intelligence agencies and lead to the arrest of over 700 suspected criminals in the UK and Europe.

Also, some supposedly private encrypted email servers have given over their users' data to law enforcement agencies. In 2021 the encrypted-email company ProtonMail publicly admitted it handed over the details of its users to authorities even though this Swiss company sells itself on its complete privacy of their users' personal data. Protonmail said it had been legally obliged to collect data from an account said to be linked to a "climate activist" who was arrested by French police.

Spyware is also a major threat and can easily be installed and downloaded onto a target's device. If you lose control of your phone or computer for even a limited time and if falls into the hands of those seeking to target you, spyware can be installed which will turn your personal device into an enemy controlled device that will be spying on you 24/7.

Spyware can also be installed by opening unknown links and downloading unknown applications from 3rd part servers. So, you must keep your communication devices physically secure, do not talk with strangers online or open any unknown links or attachments. A well published spyware infection was that of the Israeli made Pegasus spyware that was used by

governments to spy on activists, journalists, political opponents, and even foreign government official, one of whom was reported to be the former British prime minister “Liz Truss”!

So, these days it’s essential for Investigative Journalists, political activists, or private investigators to be very careful how they communicate and store data and content, especially in potentially hostile environments and situations. What I will do here is give you some guidance on how by using simple techniques you can minimize the risk of your electronic communications being compromised.

- Always try to keep the devices you use for work and personal use separate. If you are working on a specific case or story that requires secure communications buy a device specifically for that job and use it only for communications to do with that job. By doing this if you are ever at risk of being compromised or arrested you can always destroy that phone or reset to factory settings to wipe clean its memory.
- Consider if the source of your phone could have been compromised? Did you buy the device randomly or was it pre-ordered or pre-owned? Could those that gave or sold you the device had placed spyware on it knowing you would be using it? Likewise, if you are using a sim, was its source possibly compromised? It’s better to buy devices, sims and memory cards etc. from random dealers. Be very suspicious of people who want to give you phones or computers, if you accept at lease reset them to the factory settings to try to delete and hidden spyware but I would not use them for sensitive cases.
- Always use a decent VPN service and regularly scan the phone or computer for any unusual applications or programs.
- Most smartphones will operate with Wi-Fi without a sim card, you do not need a phone number or data and can use the phone on Wi-Fi for communications via selected apps or via email. Always ensure that the Bluetooth is turned off and the phone is set to airplane mode.
- You need to select various Wi-Fi locations such as cafes or businesses where you can log on to the internet for free. Vary these locations as much as possible, never use the same location on the

same days at the same times etc.

- When using a café or restaurants Wi-Fi always ensure that you are a good customer, buy drinks and food etc. that way they will be happy for you to sit there and be online. Have a cover story prepared if they ask why, you are there for a long time. Taking a friend with you can help you to blend in better, as two friends talking for a few hours is normal, whereas a lone man drinking one cup of coffee for a few hours can be suspicious!
- When you have access to the internet you can download applications that don't need phone numbers to operate. For example, fake Instagram and Facebook accounts can be set up with just an email address and have good messenger services.
- There is a wide array of free email service where temporary email accounts can be set up for specific jobs and contacts. To login to most email services, you only need access to a web browser like Google or better still Firefox.
- Once you have set up your accounts memorize the usernames and passwords and always log out of the accounts. This way you can always access these accounts wherever you are on any device.
- Try to also remember the social media handles and online names of contacts you may need to contact in case of emergency or if you lose or need to throw away your device.
- In high-risk situations you can download and install the applications you are using for communications or photo and data storage onto your device each time you need to use them. When the messages have been sent or photos or data uploaded the application can be deleted. Your messages would have been sent and your photos etc. stored until the next time you download and login to the applications. Ensure the devices history is always cleaned out as that way if your phone is searched by anyone targeting you it will be clean.
- Setting up email accounts or cloud storage etc. and sharing the login details with the people you are talking to or working with is another way of communicating. That way no messages or data is being sent and information and photos can be uploaded and downloaded as required in draft messages etc.
- Micro-SD memory cards are excellent for data and photo storage and

most smartphone use them for extra internal storage. They are small, easy to hide and can, depending on the model hold a lot of data. A basic 32GB card can hold thousands of photos, documents and hours of video. When traveling all sensitive data can be removed from your devices and placed on a micro-SD card and concealed in the lining of a jacket, inside a shore or among other regular items.

- Where available pay phones, mobile phones that are being rented for calls or call shops can be used for voice calls. But remember call shops can record conversations and will be storing all phone numbers called. Vary the use of pay phones and public calling services as much as possible, do not set any patterns in your activities.
- Today, it is generally assumed that telephone communications are not secure. It is usually safe, however, when previous arrangements have been made, for two people to go to different public telephone booths at the same time and then carry on their conversation without the use of any suspicious words or phrases. Simple codes can be used.
- Internet cafés and business suites can be used for online communications but remember that the computers can monitored and remember to always clear the history and cookies of any public computer you use. If you do not clear the history and cookies others can see the sites, you visited and even possibly your passwords and login details. Be careful and understand how to wipe the history and cookies on any public computers you use or even borrow from friends.

An example of how what I have written about here could be applied could go like the following: An investigative journalist is going to a country to interview a source for an serious story on human rights violations and corruption. He flies to the country with his personal phone that has nothing to do with story or his contacts within that country on it.

When he arrives in the country, after ensuring he is not being followed, he goes to a random phone shop and buys a smartphone. He then proceeds to a café where he logs onto their free internet and with his new phone logs into

the email service that he has previously set up to communicate with his contacts. A meeting is arranged.

At the meeting his contacts give him a micro-SD card containing documents and photos to do with the story. The following day the journalist goes to another café, downloads a cloud storage application onto his new phone and uploads the documents and photos from the micro-SD card that he has placed in his new phone. When the upload is complete, he uninstalls the cloud storage application from the phone. He has the option now to destroy the micro-SD card or to conceal it to take with him when he leaves the country.

If the journalist needs to interview anyone then the interviews could be recorded onto his new phone, uploaded, from a different café to the cloud application or an email account, or stored on the micro SD card.

As this is a high-risk situation the journalist has a trusted associate outside of the country downloading everything that he is uploading in case the journalist is arrested or the online accounts are compromised. When the trusted contact signals that they have downloaded and stored all the uploaded documents and photos the journalist destroys the micro-SD card.

As the journalist leaves the country, he resets the phone he bought to factory settings, takes it apart and throws it in various garbage cans. All evidence of his activities has now been erased. He will leave the country with his personal phone which will just have tourist photos etc. on it. If search they is nothing that could compromise the journalist or his contacts. Remember traveling with a phone that has been wiped clean and is set on the factory settings is suspicious for police or airport authorities.

As another example, this time from a real task I undertook for a client who was having problems in let's say an emerging market. The client was caught up in a legal dispute over several maritime vessels which had been sized by the authorities of the country they were in. The client needed to confirm the vessels were in good order and not being dismantled. They had just given a large amount of money to a very high-profile investigation agency to go and do this task for them but were not happy with the results.

This investigations company had sent two of its specialist operatives to the country to check things out; they took with them the latest encrypted satellite phone for secure communications which initially impressed the client when they showed it to them and gave them a story of how they planned to complete the operation.

The country they were going to had very suspicious and alert government security agencies. Even though the county is supposedly poor as far as the media portrays it, the city they were traveling to was very modern. However, if these wannabe James Bonds had been stopped at customs, the expensive encrypted satellite phone would immediately draw attention to them… Why does someone need an encrypted satellite phone in a modern city?

The client was contacted by the operatives when they were in the county, but they contacted him by a regular landline phone, because they could not get a signal on the encrypted satellite phone. Satellite phones operate on specific networks that are monitored and can be blocked in some locations as was the case here.

The operatives told the client they could not locate the vessels and asked the client where he thought they might be. He did not know and asked them if they had asked the harbor master in the city's port. They did not, because neither of them could speak the local language.

In the end, they located someone to speak to the harbor master and found the vessels. The operators then drew up plans which detailed how they could steal one of the vessels, which would have been highly illegal. This was when the client’s patience had run out and they contacted me.

Within our network, we had a local contact within the country and had them monitor the vessels. All communications were done using encrypted e-mail; almost everyone has computers and smartphones these days and, as long as you have a internet access, you can send messages globally in a just few seconds.

E-mails are monitored and can be easily intercepted, which is why they should be encrypted. Good encryption software can be downloaded from the

Internet for free or used via secure internet providers such as Tutamail, so there is no excuse not to use this technology. There are millions of e-mails being sent every day, many more than encrypted satellite phone messages. Basic rule: always blend in with your environment!

The following techniques are used by intelligence agencies world-wide, they are simple, effective, low-tech and work in environments where electronic communications are completely compromised or when you need to move large amounts of documents, photos or video evidence. Low-tech non-electronic communications techniques can be divided into two types:

- Personal communications: personal communications include face-to-face discussions, either between two participating parties or with the active assistance of intermediaries.
- Non-personal communications: non-personal communications may involve mail, notices placed in newspapers, magazines or social media sites, messages left in hiding places to be picked up later by another person, etc.

Both personal and non-personal forms of communication have both advantages and disadvantages.

Face-to-face meetings are extremely dangerous in times of an active threat or when sensitive information is being handled. Therefore, they should be well planned in advance, so that the maximum amount of benefit can be guaranteed from a meeting of the shortest possible duration. If subsequent meetings are required, they should be varied as to the location, time of day or the day of the week.

In selecting a time and place for personal meetings, the general character of the area must be taken into consideration. The location will depend heavily on the threat level and what the opposition is trying to uncover. You will need a logical reason for being in that area at the time scheduled. In the event that either party decides they may have been followed, they should have some legitimate activity which they can take care of and then leave again without it compromising the person they were planning to meet. Both parties must have a plausible and convincing cover story which will explain their

activities at that time and place. Alternate times and places for the meeting should have been decided on in advance, in case one or both parties are not able to make the first scheduled meeting.

Both parties involved will also need a covert way of alerting the other person that they are under surveillance. Additionally, along the route that each will travel to the meeting place, certain signal posts should have been selected in advance. These are areas in which a sign of some kind could be left by either party who wished to warn off the other so that they would not approach the meeting spot and fall into a possible trap. A chalk mark on a specific wall or crushed chalk of a specific color or a piece of fruit on a pavement can be used to represent a multitude of signals and messages.

Phones are not recommended ways of warning people off when you are under surveillance, phone calls and messages leave a paper trail. The specific way your car is parked in a certain car park space can be used as a warning sign. Or you reading a certain newspaper or magazine at the meeting spot could be sign to the other person with whom you are meeting with to abort the meeting. Just as you drinking orange juice instead of coffee could send the message that thigs are safe for the meeting, use your imagination and keep it simple.

When you are meeting people for the first time, prearranged signs and counter signs should be used to confirm the identity of each person. Generally, the best sign is a question, and the best counter sign is an answer to that question. Both must contain predetermined words or phrases and each should be both short and simple in content and pronunciation. A simple example would be, question: Is it raining in Mombasa? Reply: No, it is very dusty! You need to always make sure those you are meeting with are the real people, so you don't end up in captivity or found strangled on a garbage dump!

The terms "cut-out" and “live-drop” are used frequently in intelligence networks and espionage organizations. A cut out is a person who carries messages back and forth between two other people that cannot meet personally without arousing suspicion. The cut-out is often an active participant in the conversations and may make plans, us his own means of

persuasion or participate in negotiations himself.

The term live-drop applies to a person that merely accepts a message or item from one person and holds until another party can conveniently pick it up. The live-drop must always be aware they are taking messages from legitimate sources, codes phrases should always be employed when accepting and passing on messengers as the couriers might vary and be unknown to the live-drop.

For the sake of security, the amount of information given to cut-outs is usually no more than is required for their task. At times a message left with a live-drop may be given to them verbally, memorized and passed on verbally to the pickup. One good option is to encrypt or place in a password protected vault any documents, photos etc. and put them on a micro-SD card or thumb drive that can be passed to a live drop for a pickup.

Non-personal communications generally provide greater safety for the participants, but they add an element of chance as far as the security and the accuracy of the transmission of the messages are concerned, and also the possibility of interception. The third party used for a cut-out or live-drop must be 100% trustworthy and are personal security and counter surveillance aware.

The term "dead-drop" refers to a hiding place where someone may leave a message to be picked up later by another person. The advantages and disadvantages in the use of dead-drops are these: dead-drop communications are safer as there is no direct contact between the sender and the recipient of the message. Dead-drops are more secure, because the recipient does not need to know the identity of the person who leaves the message for them. Likewise, the person who leaves the message does not need to know the identity of the person who picks it up. Dead-drops provide a greater flexibility of time in the event it is difficult for both the sender and receiver of the message to be in the same area on the same date.

One disadvantage in the use of dead drops is that the message is out of control for a certain length of time. It may be accidentally found, it may be destroyed or perhaps intercepted by the threat without participants’

immediate knowledge. Dead drops may be stationary or mobile. One example of a stationary dead drop could be a hollow limb of a tree in some public park or an apparently abandoned tin can or old bottle lying in the middle of a weed patch that can contain a message or micro-SD card etc.

Wide use can be made of magnetic containers as they can be attached to anything iron or steel. For example, they can be placed on the bumper of a bus or truck as it leaves one terminal or gas station and can be taken off by a receiving operative in some other city as the bus comes into the terminal or the trucks stops to fill up its gas tanks.

In the use of dead drops, it is customary to leave a signal in some public spot or on a social media post to indicate that a message has been placed in the dead drop. In this way, it is not necessary for the intended recipient of the message to risk themselves unnecessarily by going repeatedly to a dead drop when no message may be waiting for them there. Always check the area around a dead drop location before approaching it to ensure it has not been compromised and is under surveillance or being ambushed by threat personnel.

When you have reason to travel legitimately to another area, you should always use this opportunity to scout out possible meeting places or possible locations where hidden messages might be left to be picked up later.

Codes should be used between group members. For example, a bodyguard may not live with his client but can call them several times a day, if the client mentions a certain word or phrase during the call it could mean there is a problem etc.

Various objects of clothing hanging on a clothesline, certain lights left on in various rooms of a house at a certain time, a parked car left facing either north or south, a certain hat worn askew either to the left or to the right are all typical signals that may be used as a covert warning or to convey information. Use your imagination, there are endless things that can be used and simple but effective warning and messaging systems.

All of these things remind us once again that the requirements of security are in conflict with the requirements for speed and efficiency where

communications are concerned. It is very easy to become so security minded that your efficiency is badly impaired. There will always be times when speed is of the essence and when security precautions must be thrown to the wind. In most cases, however, covert communications techniques should be used which will provide a reasonable balance between speed, efficiency, and security.

The conclusion of this document is that you must remember that no electronic communications or devices are secure, so you need to be extremely careful. By following the guidelines here, you will help to minimize the risk of being compromised by those actively targeting you.

PHOTOGRAPHY

It always amazes me how many people in the investigation, close protection and even the media world can't take decent photographs or videos. Most cell phones come with cameras that can take decent stills photos and video that is more than adequate for operational purposes, so there is no excuse why people can't take photos these days.

I regularly come across people who have completed close protection and firearms courses but have no clue how to take a half decent photo or video. If you ask me what is more relevant, knowing how to use a firearm or knowing how to use a camera, I will say knowing how to use a camera is a priority. Knowing how to use firearms may be a required skill, but it's not a priority for most people and if taught properly, it does not take long to get someone up to an OK operational standard.

These days photography is simple compared to what it used to be say 20 years ago. Back in the day you had to understand such things as shutter speeds, exposures and film speed, these days you can just point and shoot. I still have my old stills camera, a manual SLR with a 300mm lens, a x2 converter to boost it up to 600mm, a 28mm wide angel lens and filters. These days most cell phone cameras are way more effective, versatile, and powerful than my old SLR and its accessories.

The issue with professional SLR cameras for investigations and close protection work is their size, walking around with an SLR camera and a large lens draws attention, especially if you're pointing it at someone. For static or mobile observation posts sure, they have an application, but for everyday street use, I would say their applications are limited. Even back in the day I tended to use zoom compact cameras a lot more than my SLR for no other reason than they were a lot more discreet.

Many times, I have heard experts telling their students etc. to always buy the best equipment they can afford, don't go for the cheap option. This I can understand if you're in a government agency or spending money that's not

yours, but I will always say buy what's adequate to get the job done. The issue with buying equipment that's going to be used for operations is that it's going to be banged around, abused, and ultimately broken. Also, remember if you are looking to lend your cameras to those working for you, they will not look after them, why should they, they didn't pay for them!

Why spend $2500.00 on a fancy camera when you can get a decent refurbished cell phone for $200.00 that can do the job just as well, more money in your pocket right! Of course, you will get better picture quality with a professional camera, but you must ask yourself how high of a definition do you need the photos to be? If you're looking to sell your photos and become a professional photographer a $5000.00 camera may be a good investment. If you spend $5000.00 on a camera hoping to get some surveillance work, then will say you have been given some really bad advice!

Even if you're traveling you can buy smartphones with decent cameras at airports or on the streets virtually everywhere these days. So, if security is an issue, you can buy a smartphone at an airport, use it to take what photos you need, upload the photos or video via a Wi-Fi hotspot, delete the pics/apps, then dump or resell the phone before you leave the county, you don't even need a sim card. These days you must always remember to keep your online accounts and your communication devices secure but that's another issue altogether…

Photography, both stills and video, have a lot of applications in investigation and close protection operations, a picture can speak 1000 words! In the planning phase of close protection operations, photos of locations, facilities, hotels, hospitals, obstacles on routes etc. can be very useful to see. If you need to set up the security for a residence, photos of the perimeter, grounds and buildings will be useful when you are briefing your team or if you are considering putting in CCTV. In protective surveillance operations, the operative should always have access to a camera to help them identify any opposition surveillance, suspicious people, or vehicles among other things.

As I said earlier, photography is an invaluable skill, photos and video are used to collect, confirm, or reinforce other intelligence. At a basic level I

always tell people working for me to get photos if they are visiting or watching a location to verify to the client that they have actually been there. A few years ago, we had a surveillance job on one of the Islands in the Caribbean, the target should have been there for business meetings but stayed in his 5-star hotel suite with his, let say secretary. The client doubted our story, claiming we must have been at the wrong hotel etc. but we had video of the hotel, the suite door, room service trolls in the corridor etc. This client had not thought about the timings for the job and would not listen to our advice so, they got what they asked for.

The best way to learn how to take decent photos and videos is to go and start taking photos and videos. These days with digital photography you don't have to worry about the cost of developing film, if you shoot 100 photos and none are any good, then delete and take another 100, it costs you nothing.

When using a camera think of it as a firearm, to get good photos or video you need to be able to aim and shoot. Always ensure when you're operational that you have enough storage space and battery life on the camera, if you think you need extra make sure you have a spare memory card, battery pack and charging cables etc.

You need to know what to take photos of, but you also need to know what not to take photos of. For example, team members, clients, residences, or safe houses etc. Anything that could compromise an operation or leak sensitive information, always check the backgrounds of your photos, you might have something in there that you did not intend to have.

Types of photography

- **Documentation photography:** This is used to record printed documents, when doing this ensure that the print is in focus and readable.
- **Object photography:** If you need to take a photograph of an object, say a knife, try to get as much detail as possible such as markings and any serial numbers. Also, photograph the object with an object

of a known size such as a pen, lighter or car key, then those viewing it can get an idea of the object's size.

- **Identification photography:** This is photographing individuals or groups of people to record their identity. The targets may or may not know that they are being photographed, an example of this would be photographing groups of protesters who may later be a potential threat. If you're taking photos of a specific individual try to focus on faces, tattoos, scars, jewelry or shoes, anything that can be used to identify them at a later date.

- **Location photography**: This is used to provide an overview of a location, security systems, possible surveillance sites, avenues of approach, access and exit points, vehicles on site, perimeter security etc. This may be done covertly or overtly for defensive or offensive purposes. The main issues I have seen with location photography is that people do not take enough photos and tend to have a narrow focus instead including wide angle or panoramic shots, which if anything interesting is identified can always be zoomed in on. A good video sweep can be worth a ton of narrow stills. When taking video footage describe what you're looking at and what direction you are looking at it from; north, east, south, west etc. This is essential as locations can look different when approached or viewed from different angles.

- **Surveillance photography:** Surveillance and counter surveillance photography is used to gather covert intelligence on individuals and locations etc. Surveillance photography usually involves some imaginative practices such taking posed photos of individuals just to get what's going on in the background or using the selfie camera on a smartphone to get photos or video of what's going on behind you. Where there is a sufficient budget remote cameras and drones can be

employed.

Most investigation or security operations will combine the principles from most of the above types of photography. For example, using photography in and advance security detail as part of a close protection operation to check out a restaurant that might be visited by a client could include:

- **Document photography:** Photos of menus and venue evacuation plans.
- **Identification photography:** To record the type of crowd and key members of staff.
- **Location photography:** Approach routes, overall venue, internal layout, bathrooms and exits etc.

Small details can be of great intelligence value, such as what shoes someone is wearing, what's on the screen of a person's smartphone, what the weather is like at a location, road surfaces, the flooring in a building or where the buildings water tanks are. It's always better to have more photos and video footage of the target than to be missing one critical detail. These days for surveillance its best to take video footage as this is easier for most people and if required stills photos can be taken from the video when editing.

When you have your photos and videos you need to save them in a secure location be it online or on a hard drive. Save the originals and edit copies if required. Ensure you save the photos in a file with a description of when and where they were taken. Photos from a route check done on a weekend afternoon may show light traffic on a road but at 0830 on a Monday morning the same road could be congested.

I think we can all agree there is no excuse these days for someone in the private investigation or close protection industry not to have access to a camera that can take respectable photos and video. My friends in Somalia take some brilliant photos and post them online all the time so, why can't you?

This is only a short chapter on an important skill in which I have spoken about some key points, I hope it gives you a few things to think about!

INTERVIEWS & DEBRIEFS

A major part of investigations and intelligence operations is the interviewing of witnesses and debriefing of informants. One of the differences between interviewing of witnesses and debriefing of informants is that a witness might need to go court to give evidence, whereas an informant is supplying confidential information.

Evidence presented in court, must be verified by a witness and their statements must have been taken in a professional environment to a set format. Debriefing an informant might consist of a quick conversation in bar where you record the conversation on your smartphone so you can go over and process it later on.

In this chapter I am going to briefly go over what you need to consider when interviewing or debriefing someone. I am not going to talk about taking formal witness statements as the requirements vary from country to country due to their individual laws. Wherever you are operating if you need to take a formal statement from someone ensure it’s in full compliance with the local laws.

Over the years I have been interviewed and debriefed in numerous settings and for various reasons and I find it funny how many of those doing the questioning follow standard textbook procedures. I have had people play good guy and bad guy, repeatedly ask the same questions trying to catch me out, use sleep deprivation and of course make extreme threats. I have even had people put obscure theories into the conversation that I know could have only come from people that were telling tales on me… So, thank you very much to my “questioners” for the tips on the snitches btw!

If you’re the one being questioned stick to your story, or cover story, but remember: if a story is repeated perfectly word for word, chances are that a professional interrogator will know it’s been rehearsed!

As I have said throughout this book, intelligence and counterintelligence

are two sides of the same coin. You can employ the tactics and techniques against others and can expect others to employ them against you. You must think outside the box, because if you're dealing with professionals, they will already know the textbook tactics and responses.

The Basics

As soon as the witness or informant decides to talk to you, they could be putting your and their lives at risk. You need to consider the all risks to yourself and the person you're intending to talk to and do everything possible to minimize them. Not only is there the risk of physical violence but also the risk of compromising investigations, operations and the destruction of evidence.

When interviewing and debriefing you must remain professional and impartial. To get the best results, the person you're talking with must be comfortable with you and believe that you are not judging them or their actions. Many witnesses and informants will be very afraid, and you will need to reassure them that they are safe, and you are working in their interests.

You need to be very careful when dealing with scared and vulnerable people to ensure that they are not just telling you what they think you want to hear. They need to know that you want them to only tell you the facts and if they don't have the answers to your questions, they will not be punished in anyway. On the other hand, they need to understand that if they lie, give you disinformation or hold back on information they will be squeezed in some way.

The location for the interview or the debrief can also influence how the person you're talking to behaves. If you want to make someone comfortable meet them in an environment they are used to, keep them in their comfort zone. If you want to apply pressure on someone then take them to a location you know will be outside of their comfort zone.

Before the interview or debriefing you need to have a strategy and your

questions pre-planned. If necessary, select trusted others to conduct the interview if you believe they would have a better rapport with the witness or informant than yourself. If you're using multiple interviewers make sure they know who will be taking the lead in the questioning and what topics they need to concentrate on specifically. The interviewers would need to be briefed on the objectives and the background of the operation and debriefed after they have spoken with the witness or informant. Things that you need to consider before you talk with a witness or informant are:

- **Their age:** Knowing the person's age helps to determine the best individual to interview them, an older person might have no rapport or respect for someone half their age for example.
- **Cultural background:** The interviewer must understand the culture of the person they are talking to.
- **Religion:** People's religious beliefs need to be understood and respected.
- **Gender:** Straight, gay, transgender… You don't want a homophobe interviewing a person who is transgender…
- **Personal life:** Are they married, single, gay, have children, cheating on their partners, etc.?
- **Physical and mental health:** This needs to be taken into consideration for their safety and possibly yours.
- **Previous contact:** Is the person known and could they be a security threat? The meeting could be a set up for an assault…

Questioning

The first step to questioning someone is to get them talking, this is where some knowledge of their personal life and interests helps. Where time allows, the initial conversation does not have to be about the investigation or operation, some small talk can help to relax the witness or informant. When you start talking business then make sure the witness or informant knows that you want the facts only, are impartial and are there to help them when you can.

The witness or informant needs to understand why you want to talk to them. The reason, real or not, should have been worked out in the planning

phase and the initial questions need to be about that reason. As the interview develops you can take the conversation in the direction that you require. The witness or informant needs to know you are interested in knowing anything that they feel could be relevant, such as the personal lives, circumstances and opinions of others involved in the investigation or operation. You need to let the witness or informant talk; as they talk, they will relax and will become more comfortable with you. Consider:

- Is your body language giving the right impression?
- Always allowing the person you're talking to pause and think, without interrupting.
- Encouraging the person to talk until they have given the full story.
- Guide the witness or informant in the direction you want and try to emphasize important topics.
- Go back and bring up previously talked about topics to clarify and expand on what's already been said.
- Ensure you covered to the best of your ability the questions and topics you identified in your interview plan.

Your questions should have been pre-planned and must be put across in language that the witness or informant understands. Keep your questions short, simple and to the point. Do not over-complicate the language you use or the questions as this can confuse the person you're talking to. You can expand and clarify what the person is saying by using various pre-planned questions and responses. Types of questions include:

- **Open-ended:** For example, saying 'Tell me', 'Describe' or 'Explain' invites the person to expand on what they have said and talk freely.
- **Specific-closed:** Questions such as 'Who shot him?' 'What did he say?' or 'Where do they stay?' can be used to clarify the specifics of what the person is saying or could be reluctant to say. Such questions are best asked when the conversation is warmed up, since they can come across as too direct if the person you are talking to is scared or nervous.
- **Forced-choice:** 'Were the drugs sold or exchanged?', these types of questions can lead to the person guessing the answer and are best

used when you know the answer but want to see if the person is lying or ill-informed.

- **Multiple:** Asking questions such as ‘Where did they come from, what did they do, where did they go to?’ can confuse the person you’re talking to. Keep questions short, simple and to the point.
- **Leading:** Saying such things as ‘You saw the knife, right?’ can lead the witness or informant to give you an answer they think you are asking for. Leading questions are less credible and should only be used when finally confirming previous statements.

Where time allows you should try to summarize what’s been said before closing up the conversation and ensure the witness or informant has nothing else to say and you have asked all your questions. Once the interview or debrief is over what’s been said needs to be processed and a decision made if further actions or meetings are required.

Types of people and hints for interviewing

- **Talkative:** Let them talk; listen and select what you require.
- **Reluctant:** This is the person who does not want to talk. Either they do not like publicity, they dislike you or he or a friend are the ones you’re after. You need to understand them and gain their confidence and assure them you can work together.
- **Emotional:** This person can easily confuse what they have seen, heard or imagined. Always verify their stories and beware that they are not just seeking attention.
- **Timid:** This type of person can prove to be a valuable and reliable witness; be friendly and encourage them to talk.
- **Hysterical:** Do not question them. Calm them down and get back to them later if necessary.
- **Shy and Nervous:** Dealing with them can take patience and understanding. Be friendly, build a rapport and don’t pressure.
- **Adolescent:** Normally self-centered, worst observers and rarely describe accurately what they see or hear. Always double check their stories.
- **Middle-Aged:** People in this age group generally have fixed

viewpoints and prejudices; this is where knowing their backgrounds helps to build a rapport.

- **Elderly:** Elderly people can be keen observers, but they may need to be kept focused.
- **Lying:** Check and re-check their stories. They can be used for spreading disinformation or exposed and then pressure applied so that they tell the truth.

Recording interviews and debriefs

These days everything should be recorded where possible if the circumstances and threat level allow. Do not record and save anything that could compromise a witness or informant. Remember that recorded statements, especially virtual, when used as evidence can always be deemed as non-credible due to the fact, they have been recorded in a non-professional environment. Witnesses and informants can always claim they were intimidated or blatantly lying. Statements need to always be backed up with facts and evidence.

AUTHOR

Orlando Wilson has worked internationally at all levels of the specialist security and investigation industry for over 30 years. Over the years, he has become accustomed to the types of complications that can occur, when dealing with international law enforcement agencies and the problem of dealing with kidnapping, organized crime and Mafia groups.

His experience in the international security business began in 1988 when he enlisted in the British army at 17 years of age and volunteered for a 22-month frontline, operational tour in Northern Ireland in an Infantry unit, 4 Platoon, 1 WFR. He then joined his unit's Reconnaissance Platoon, with which he undertook intensive training in small-unit warfare.

Since leaving the British army in 1993, his time spent working in Eastern Europe in the 1990s gave him firsthand experience of the operational procedures of organized criminals and Mafia groups from the former Soviet Union. In addition, he had the opportunity to oversee criminal cases that have been the first of their kind in their respective country. His operations in Mexico training tactical police teams put him in a unique position to understand the war on Narco-Terrorism. His continuous and ongoing projects focusing on kidnap and ransom prevention in South American, the Caribbean and West Africa have given him the knowledge to formulate practical programs to counter the kidnapping threat.

Orlando is a published author, writer, photographer and has been interviewed by numerous international TV and media outlets on topics ranging from kidnapping, organized crime to maritime piracy. He had his first article published in 1997 in an association magazine and his first book in 2012. He has been interviewed by media outlets ranging from the Professional Mariner Magazine, Newsweek Serbija, Newsweek en Espanol, GrupoMilenio, MundoFox, The New York Times, Soldier of Fortune Magazine and others.

Orlando's diverse and continuous operational experience enables him to provide no-nonsense professional services and training programs. His

operational investigation and close protection procedures are cutting edge and the most effective commercially available. He is also a founding member and operations manager of Risks Incorporated.