News • Reviews • Opinions • Intel • Exclusives

The Circuit

For Security And Protection Specialists

ISSUE 61

PENETRATING A CP TEAM

DEMYSTIFYING COMBATIVES

The Protector Mindset: WARRIORGUARDIAN

TACTICAL MEDICINE

LEARNING CYBERSECURITY | HUMAN INTELLIGENCE | TACTICAL CONSIDERATIONS

By Orlando Wilson

INTELLIGENCE GATHERING: PART 2
HUMAN INTELLIGENCE

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.

> “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.

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.

> “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.

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 to 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 an 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. 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. would lead to the program losing its credibility very quickly.

Orlando Wilson has worked in the security industry internationally for over 25 years. He has become accustomed to the types of complications that can occur, when dealing with international law enforcement agencies, organized criminal and Mafia groups. He is the chief consultant for Risks Inc. and based in Miami but spends much of his time traveling and providing a wide range of kidnapping prevention and tactical training services to private and government clients.