

POLICE ARMORED RESCUE VEHICLES (ARVS) • TERRORISM FOR DUMMIES • MH1 REFLEX OPTIC

Journal for Law Enforcement, Intelligence & Special Operations Professionals

The Counter Terrorist

VOLUME 10 • NUMBER 3

COUNTER
SURVEILLANCE
CONSIDERATIONS



JUNE/JULY 2017
USA/CANADA \$5.99

INTERNATIONAL
EDITION

An SSI® Publication
thecounterterroristmag.com

COUNTER SURVEILLANCE CONSIDERATIONS

If you are serious about your personal security, basic counter surveillance procedures should be part of your daily routine.

by Orlando Wilson

The reason you need to understand counter surveillance is to identify anyone who has you under surveillance. 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 that identify threats to their organizations and potential targets for kidnapping or extortion.

Counter surveillance is the base skill for all personal security and close protection programs. In this short article, 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 whether you are under surveillance.

Many supposed security, tactical, close protection 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.

To put things in perspective on a basic level: what weapon do you think has killed the most people? I would say the rock. Since beginning of time, humans have been smashing each other's heads with rocks! So, Mr. Executive Protection Specialist can be looking cool wearing a \$500 suit and 3A vest and packing a

Most people do not pay attention to their surroundings. So if someone is over-observant, what are they up to?

.40 Glock. But if he is too busy looking cool to realize he is being watched and followed, it will take little skill to come up and smash him in the back of the head with a rock. Game over. Please note, unlike the movies, if you're dealing with professional criminals, they will go after their target's security personnel before the actual target to remove or make an example of the security personnel. The target will be defenseless and most likely very compliant. If you can't look after yourself on a basic level, how can you expect to be able to look after others?

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. Try it 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 someone acting suspicious, watching, or following them. So, I

expect most people reading this article are in the unaware category, but by the time you finish reading this there is no reason not be in the professional category.

THE BASICS

You can start training while you're reading this article. 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 being they 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!



Photo: Pixabay



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? You must learn to read body language, because this 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 where someone could watch you from, and then keep an eye on that location from time to time. If someone is hanging around that area, take note. If they are there for an extended time or 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 are 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 with 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 or 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 realtime images to your cell phone or email? Here I am talking about regular commercial hunting cameras available at Walmart, 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. These days' 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 is their camera quality, flight time, weather conditions they will be used in, and from the good guys' point of view, what the laws are on their use in your area. Even within a small-scale private security operation, drones could be employed for



Photo: U.S. National Archives and Records Administration

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. Whilst patrolling, you want to be looking 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 retreat to further-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 that you are working under. All of this needs to be considered in your operational planning.

In urban areas, surveillance operatives use as cover locations places where people congregate, such as cafés, bars, bus stops, or pay phones. 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 are being used against you: listening devices, remote cameras, mail being intercepted, computers being hacked, or physical surveillance.

These days, we must ensure our computers, smart phones and Internet connections are secure. If the criminals or terrorist get access to these, they will know all personal details for most people. I am still surprised today that a lot of people 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 is constantly evolving specialist 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



Photo: Pixabay

trick used to gather intelligence, defraud, or get access to computer systems, etc. A lot of successful computer hacks are 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 you leave your computer at the office overnight, maintenance, security, or cleaning staff can 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 targets offices, so they can access the target company’s computers and trash after work hours. Most people would not consider the threat of a bumbling night shift security guard or the apparently, barely literate office cleaner downloading business data from their computer or copying confidential papers, but they should!

You cannot carry your computers around with you all the time, so one

thing to do is to keep minimum information on them. 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 any 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 and phones and listen in to their conversations. Many people regularly work in public locations with unsecure Wi-Fi connections where anyone can view their computer screens, with the same comfort level they would have at home. When chatting with friends in public, people disclose personal information all the time

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 you or your clients’ computers or phones are bugged, then you would 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 than letting the criminals or terrorists know that their operation is compromised, which could force them into acting.

STREET DRILLS

So, you must always be on the lookout



Photo: Pixabay



Photo: Pixabay

for criminal surveillance, and here I have listed a few simple drills that are used by professional criminals and intelligence operatives alike. These simple drills will help you identify anyone who is watching or following you. But 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 who 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 for its suspicious qualities: tinted rear windows, parked in one position for an extended period, etc. If I remember right, 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 who 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 point, 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 whilst ascending, you can have a good look around at who is behind you. A simple drill would be to go up and 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 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



Photo: Pixabay

trying to see what you're doing. Pay special attention to locations where people are congregating for legitimate reasons: 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.

- Look for people who look out of place or are waiting in the same place 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 30s to 50s. 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, or 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 meetings. In high-risk situations, these could have been set up by the opposition to photograph



Photo: Pixabay

you or set you up to be kidnapped or assassinated. Always sweep the area for any 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., will 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 five 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 those devices cleaned

up and secured!

Now, 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. It 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 log 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. Which depending on the case, could lead to a loitering ticket, an arrest, or nothing, but at least you have a record of calling the police for your file.

I've had numerous clients over the years that have had issues with private detectives following them 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 article on what is a very important and in-depth subject, and I hope it makes you think about

your personal security procedures and assists you in your operational planning. Remember: if you can't look after yourself on a basic level, how can you expect to be able to look after others? •

ABOUT THE AUTHOR

Orlando Wilson has over twenty-five years experience within the international security industry. His experience in the risk management business began in 1988 at the age of 17, when he enlisted in the British army and volunteered for a 22-month front-line, operational tour in Northern Ireland in an infantry unit. This tour of duty gave him an excellent grounding in personal security and anti-terrorist operations. He then joined his unit's Reconnaissance Platoon, with which he undertook intensive training in small-unit tactics and asymmetrical warfare. Since leaving the British army in 1993, he has worked and coordinated projects in the U.K., South & West Africa, Western and Eastern Europe, the U.S., Latin America, the Middle East, and the Caribbean. His experience has included providing close protection for Middle Eastern royal families and varied corporate clients, asset protection, embassy security, crisis management, corporate intelligence, asset recovery, and paramilitary training for private corporations and government agencies. He has become accustomed to working with minimal support, the problems of organized crime, and the types of complications that can occur when dealing with international law enforcement agencies.

The Counter Terrorist

Asia Pacific Edition

The Counter Terrorist Magazine Asia Pacific Edition is finally available for the Asia Pacific region counter-terrorism and homeland security practitioners. The Asia Pacific Edition not only gives the readers a worldwide counter-terrorism perspective but also in-depth information about counter terrorism activities in Asia. The Asia Pacific Edition provides an excellent platform for counter-terrorism and homeland solutions providers to access and penetrate the Asia Pacific market.

For media kit or enquiry:

Counter Terrorism Practitioner Pte Ltd

Tel: (65) 67342237 • Email: sales@thecounterterroristmag.com

Circle 255 on Reader Service Card