By Scott Stewart

Recently Stratfor's Security Weekly discussed how situational awareness is a mindset that can — and should — be practiced by everyone. We also described the different levels of situational awareness and discussed which level is appropriate for different sorts of situations. And we noted how all criminals and terrorists follow a process when planning their acts and that this process is visible at certain times to people who are watching for such behavior.

When one considers these facts, it inevitably leads to the question: "What in the world am I looking for?" The brief answer is: "warning signs of criminal or terrorist behavior." Since this brief answer is very vague, it becomes necessary to describe the behavior in more detail.

Surveillance

It is important to make one fundamental point clear up front. The operational behavior that most commonly exposes a person planning a criminal or terrorist act to scrutiny by the intended target is surveillance. Other portions of the planning process can be conducted elsewhere, especially in the age of the Internet, when so much information is available online. From an operational standpoint, however, there simply is no substitute for having eyes on the potential target. In military terms, surveillance is often called reconnaissance, and in a criminal context it is often referred to as casing or scoping out. Environmental activist and animal rights groups trained by the Ruckus Society refer to it as "scouting." No matter what terminology is being used for the activity, it is meant to accomplish the same objective: assessing a potential target for value, vulnerabilities and potential security measures. Surveillance is required so that criminals can conduct a cost-benefit analysis.

The amount of time devoted to the criminal surveillance process will vary, depending on the type of crime and the type of criminal involved. A criminal who operates like an ambush predator, such as a purse-snatcher, may lie in wait for a suitable target to come within striking distance. This is akin to a crocodile lying in a watering hole waiting for an animal to come and get a drink. The criminal will have only a few seconds to size up the potential target and conduct the cost-benefit calculation before formulating his plan, getting ready and striking.

On the other extreme are the criminals who behave more like stalking predators. Such a criminal is like a lion on the savannah that carefully looks over the herd and selects a vulnerable animal believed to be the easiest to take down. A criminal who operates like a stalking predator, such as a kidnapper or terrorist, may select a suitable target and then take days or even weeks to follow the target, assess its vulnerabilities and determine if the potential take is worth the risk. Normally, stalking criminals will prey only on targets they feel are vulnerable and can be successfully hit, although they will occasionally take bigger risks on high-value targets.

Of course, there are many other criminals who fall somewhere in the middle, and they may take anywhere from a few minute to several hours to watch a potential target. Regardless of the time spent observing the target, all criminals will conduct this surveillance and they are vulnerable to detection during this time.

Given that surveillance is so widely practiced, it is quite amazing to consider that, in general, criminals and terrorists are terrible at conducting surveillance. There are some exceptions, such as the relatively sophisticated surveillance performed by Greenpeace and some of the other groups trained by the Ruckus Society, or the low-key and highly detailed surveillance performed by some high-end art and jewelry thieves, but such surveillance is the exception rather than the rule.

The term "tradecraft" is an espionage term that refers to techniques and procedures used in the field, but term also implies quite a bit of finesse in the practice of these techniques. Tradecraft, then, is really more of an art rather than a science, and surveillance tradecraft is no exception. Like playing the violin or fencing with a foil, it takes time and practice to become a skilled surveillance practitioner. Most individuals involved in criminal and terrorist activity simply do not devote the time necessary to master this skill. Because of this, they have terrible technique, use sloppy procedures and lack finesse when they are watching people.

Although everybody planning a criminal or terrorist attack conducts preoperational surveillance, that does not necessarily mean they are good at it. The simple truth is that these individuals are able to get by with such a poor level of surveillance tradecraft because most victims simply are not looking for them. And this is where we tie the discussion back into last week's Security Weekly. Most people do not practice situational awareness. For those who do, the poor surveillance tradecraft exhibited by criminals is good news. It gives them time to avoid an immediate threat and contact the authorities.

Demeanor Is the Key

The behavior a person needs to outwardly display in order to master the art of surveillance tradecraft is called good demeanor. Good demeanor is not intuitive. In fact, the things one has to do to maintain good demeanor frequently run counter to human nature. Because of this, intelligence and security professionals who work surveillance operations receive extensive training that includes many hours of heavily critiqued practical exercises, often followed by field training with a team of experienced surveillance professionals. This training teaches and reinforces good demeanor. Criminals and terrorists do not receive this type of training and, as a result, bad surveillance tradecraft has long proved to be an Achilles' heel for terrorist and criminal organizations.

Surveillance is an unnatural activity, and a person doing it must deal with strong feelings of self-consciousness and of being out of place. People conducting surveillance frequently suffer from what is called "burn syndrome," the erroneous belief that the people they are watching have spotted them. Feeling "burned" will cause surveillants to do unnatural things, such as suddenly ducking back into a doorway or turning around abruptly when they unexpectedly come face to face with the target. People inexperienced in the art of surveillance find it difficult

to control this natural reaction. Even experienced surveillance operatives

occasionally have the feeling of being burned; the difference is they have received a lot of training and they are better able to control their reaction and work through it. They are able to maintain a normal looking demeanor while their insides are screaming that the person they are surveilling has seen them.

In addition to doing something unnatural or stupid when feeling burned, another very common mistake made by amateurs when conducting surveillance is the failure to get into proper "character" for the job or, when in character, appearing in places or carrying out activities that are incongruent with the character's "costume." The terms used to describe these role-playing aspects of surveillance are "cover for status" and "cover for action." Cover for status is a person's purported identity — his costume. A person can pretend to be a student, a businessman, a repairman, etc. Cover for action explains why the person is doing what he or she is doing — why that guy has been standing on that street corner for half an hour.

The purpose of using good cover for action and cover for status is to make the presence of the person conducting the surveillance look routine and normal. When done right, the surveillance operative fits in with the mental snapshot subconsciously taken by the target as the target goes about his or her business. Inexperienced people who conduct surveillance frequently do not use good cover for action or cover for status, and they can be easily detected.

An example of bad cover for status would be someone dressed as "a businessman" walking in the woods or at the beach. An example of bad cover for action is someone pretending to be sitting at a bus stop who remains at that bus stop even when several buses have passed. But mostly, malefactors conducting surveillance practice little or no cover for action or cover for status. They just lurk and look totally out of place. There is no apparent reason for them to be where they are and doing what they are doing.

In addition to "plain old lurking," other giveaways include a person moving when the target moves, communicating when the target moves, avoiding eye contact with the target, making sudden turns or stops, or even using hand signals to communicate with other members of a surveillance team or criminal gang.

Surveillants also can tip off the person they are watching by entering or leaving a building immediately after the person they are watching or simply by running in street clothes. Sometimes, people who are experiencing the burn syndrome exhibit almost imperceptible behaviors that the target can sense more than observe. It may not be something that can be articulated, but the target just gets the gut feeling that there is something wrong or odd about the way a certain person behaves. Innocent bystanders who are not watching someone usually do not exhibit this behavior or trigger these feelings.

The U.S. government often uses the acronym "TEDD" to illustrate the principles that can be used to identify surveillance conducted by counterintelligence agencies, but these same principles also can be used to identify criminal and terrorist surveillance. TEDD stands for time,

environment, distance and demeanor. In other words, if a person sees someone repeatedly over time, in different environments and over distance, or someone who displays poor surveillance demeanor, then that person can assume he or she is under surveillance. If a person is being specifically targeted for a planned attack, he or she might be exposed to the time, environment and distance elements of TEDD, but if the subway car the person is riding in or the building where the person works is the target, he or she might only have the demeanor of the attacker to key on because the attacker will not be seen by the observer over time and distance or in different environments.

Time, environment and distance are also not applicable in cases involving criminals who behave like ambush predators. Therefore, when we are talking about criminal surveillance, demeanor is the most critical of the four elements. Demeanor will also often work in tandem with the other elements, and poor demeanor will often help the target spot the surveillant at different times and places.

In a situation where a building or subway car is targeted for an attack rather than a specific person, there are still a number of demeanor indicators that can be observed just prior to the attack. Such indicators include people wearing unseasonable clothing in warm weather (such as trench coats); people with odd bulges under their clothing or wires sticking out from their clothing; people who are sweating profusely, mumbling or fidgeting; people who appear to be attempting to avoid security personnel; and people who simply appear to be out of place. According to many reports, suicide attackers will often exhibit an intense stare as they approach the final stage of their attack plan. While not every person exhibiting such behavior is a suicide bomber or shooter, avoiding such a person rarely has much of a downside.

One technique that can be helpful in looking for people conducting long-term surveillance is to identify places that provide optimal visibility of a critical place the surveillant would want to watch (for example, the front door of a potential target's residence or office). These optimal observation points are often referred to as "perches" in surveillance jargon. Perches can then be watched for signs of hostile surveillance like people who don't belong there, people making demeanor mistakes, etc.

This principle can also be extended to critical points along frequently and predictably traveled routes. Potential targets can conduct simple pattern and route analyses to determine where along the route they are most predictable and vulnerable. Route analysis looks for vulnerabilities, or choke points, on a particular route of travel. Choke points have two main characteristics: They are places where the potential target must travel and where rapid forward motion is difficult (such as sharp, blind curves). When a choke point provides a place where hostiles can wait with impunity for their victims and have access to a rapid escape route, the choke point becomes a potential attack site. These characteristics are found in attack sites used by highly professional kidnap/assassination teams and by criminal "ambush predators" such as carjackers. While the ideal tactic is to vary routes and times to avoid predictable locations, this is also difficult and disruptive and is warranted only when the threat is high. A more practical alternative is for potential targets to raise their situational awareness a notch as they travel through such areas at predictable times in order to be on the alert for potential hostile surveillance or signs of an impending attack.

The fact that operatives conducting surveillance over an extended period of time can change their clothing and wear hats, wigs or other light disguises — and use different vehicles or license plates — also demonstrates why watching for mistakes in demeanor is critical. Of course, the use of disguises is also an indicator that the surveillants are more advanced and therefore potentially more dangerous. Because of a surveillant's ability to make superficial changes in appearance, it is important to focus on the things that cannot be changed as easily as clothing or hair, such as a person's facial features, build, mannerisms and gait. Additionally, while a surveillant can change the license plate on a car, it is not as easy to alter other aspects of the vehicle such as body damage (scratches and dents). Paying attention to small details can produce significant results over time.

As we noted last week — and it is worth repeating here — paying attention to details and practicing situational awareness does not mean being paranoid or obsessively concerned about security. When people live in a state of paranoia, looking for a criminal behind every bush, they become mentally and physically exhausted. Not only is this dangerous to one's physical and mental health, but security also suffers because it is very hard to be aware of your surroundings when you are exhausted. Therefore, while it is important to watch for the watchers, watching should not involve feelings of fear or paranoia. Knowing what is occurring in the world around them empowers people and gives them a sense of security and well-being, allowing them to spot the good things in life as well as the potential dangers.