Detecting Terrorist Surveillance

March 7, 2012 | 1936 GMT

By Scott Stewart

As we noted last week, terrorist attacks do not materialize out of thin air. In fact, quite the opposite is true. Those planning terrorist attacks follow a discernable process referred to as the terrorist attack cycle. We also discussed last week how terrorism planners are vulnerable to detection at specific points during their attack cycle and how their poor surveillance tradecraft is one of these vulnerable junctures.

While surveillance is a necessary part of the planning process, the fact that it is a requirement does not necessarily mean that terrorist planners are very good at it. With this in mind, let's take a closer look at surveillance and discuss what bad surveillance looks like.

Eyes on a Potential Target

As noted above, surveillance is an integral part of the terrorist planning process for almost any type of attack, although there are a few exceptions to this rule, like letter-bomb attacks. The primary objective of surveillance is to assess a potential target for value, security measures and vulnerabilities. Some have argued that physical surveillance has been rendered obsolete by the Internet, but from an operational standpoint, there simply is no substitute for having eyes on the potential target -- even more so if a target is mobile. A planner is able to see the location of a building and its general shape on Google Earth, but Google Earth does not provide the planner with the ability to see what the building's access controls are like, the internal layout of the building or where the guards are located and what procedures they follow.

The amount of time devoted to the surveillance process will vary depending on the type of operation. A complex operation involving several targets and multiple teams, such as the 9/11 operation or 2008 Mumbai attacks, will obviously require more planning (and more surveillance) than a rudimentary pipe-bomb attack against a stationary soft target. Such complex operations may require weeks or even months of surveillance, while a very simple operation may require only a few minutes. The amount of surveillance required for most attacks will fall somewhere between these two extremes. Regardless of the amount of time spent observing the target, almost all terrorist planners will conduct surveillance, and they are vulnerable to detection during this time.

Given that surveillance is so widely practiced, it is amazing that, in general, those conducting surveillance as part of a terrorist plot are usually terrible at it. There are some exceptions, of course. Many of the European Marxist terrorist groups trained by the KGB and Stasi practiced very good surveillance tradecraft, but such sophisticated surveillance is the exception rather than the rule.

The term "tradecraft" is often used in describing surveillance technique. Tradecraft is an espionage term that refers to techniques and procedures used in the field, but the term also implies that effectively practicing these techniques and procedures requires a bit of finesse. Tradecraft skills tend to be as much art as they are science, and surveillance tradecraft is no exception. As with any other art, you can be taught the fundamentals, but it takes time and practice to become a skilled surveillance practitioner. Most individuals involved in terrorist planning simply do not devote the time necessary to master the art of surveillance, and because of this, they display terrible technique, use sloppy procedures and generally lack finesse when they are conducting surveillance.

The main reason that people planning terrorist attacks are able to get by with such a poor level of surveillance tradecraft is because most victims simply are not looking for them. Most people do not practice situational awareness, something we are going to discuss in more detail next week. For those who do practice good situational awareness, the poor surveillance tradecraft exhibited by those planning terrorist attacks is good news. It provides them time to avoid an immediate threat and contact the authorities.

Keying on Demeanor

The behavior a person displays to those watching him or her is called demeanor. In order to master the art of surveillance tradecraft, one needs to master the ability to display appropriate demeanor for whatever situation one is in. Practicing good demeanor is not intuitive. In fact, the things one has to do to maintain good demeanor while conducting surveillance frequently run counter to human nature. Because of this, intelligence, law enforcement and security professionals assigned to 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. Terrorist operatives typically do not receive this type of training -- especially those who are grassroots or lone wolf militants.

At its heart, surveillance is watching someone while attempting not to be caught doing so. As such, it 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 belief that the people they are watching have spotted them. Feeling "burned" will cause surveillants to do unnatural things, such as hiding their faces or suddenly ducking back into a doorway or turning around abruptly when they unexpectedly come face to face with the person they are watching.

People inexperienced in the art of surveillance find it difficult to control this natural reaction. A video that recently went viral on the Internet shows the husband of the president of Finland getting caught staring down the blouse of a Danish princess. The man's reaction to being caught by the princess was a textbook example of the burn syndrome. 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 behave normally despite the feeling of being burned. They are able to maintain a normal-looking demeanor while their insides are screaming that the person they are watching 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 proper (if any) 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 after several buses have passed. For the most part, however, inexperienced operatives 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 or 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 is behaving toward them. Innocent bystanders who are not watching someone usually do not exhibit this behavior or trigger these feelings.

Principles of Surveillance Detection

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 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 at a distance, or someone who displays poor surveillance demeanor, then that person can assume he or she is under surveillance.

However, for an individual, TEDD is really only relevant if you are being specifically targeted for an attack. In such an instance, you will likely be exposed to the time, environment and distance elements. However, if the target of the attack is a subway car or a building you work in rather than you as an individual, you likely will not have an opportunity to make environment and distance correlations, and perhaps not even time. You will likely only have the demeanor of the surveillant to key on. Therefore, when we are talking about recognizing surveillance, demeanor is the most critical of the four elements. Demeanor also works in tandem with all the other elements, and poor demeanor will often help the target spot the surveillant at a different time and place or in a different environment.

Time, environment and distance also have little bearing in an instance like the Fort Hood shooting, where the assailant is an insider, works at a facility and has solid cover for action and cover for status. In such instances, demeanor is also critical in identifying bad intent.

The fact that operatives conducting surveillance over an extended period 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. 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 be the difference between a potential attacker being identified and the attacker going unnoticed.

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, or a choke point on a route the potential target frequently travels). It is also important to look for places that provide optimal visibility, or "perches" in surveillance jargon. Elevated perches tend to be especially effective since surveillance targets rarely look up. Perches should be watched for signs of hostile surveillance, such as people who don't belong there, people lurking, or people making more subtle demeanor mistakes.

Paying attention to the details of what is happening around you (what we call practicing good situational awareness) does not mean being paranoid or obsessively concerned about security. Living in a state of paranoia and looking for a terrorist behind every bush not only is dangerous to one's physical and mental health but also results in poor security. We are going to talk more about practicing a healthy and sustainable level of situational awareness next week.

Click here for The Myth of the End of Terrorism.

Click here for Detection Points in the Terrorist Attack Cycle.