



(JEFF J MITCHELL/GETTY IMAGES)

# Understanding the Attack Cycle and Its Vulnerabilities

**T**he evolution of terrorist threats — away from organized and well-structured groups and toward grassroots terrorism under a “leaderless resistance” model — poses a number of risks for corporations and the security personnel charged with protecting them.

But it is possible to protect both people and assets around the world against potentially deadly and costly attacks, with a smart security program that takes into account all the steps of a terrorist attack planning cycle. An attack will never just evolve out of nowhere. People who are planning a strike follow a discernible cycle — and both the cycle and the behaviors associated with it can be observed if you are looking for them.

# The Attack Cycle

Terrorist attacks can come from a wide array of actors — including sophisticated transnational groups like al Qaeda or the Islamic State; regional militant groups like India's Maoist Naxalites; small, independent cells (such as anarchist and animal rights affinity groups); and lone wolves. There can be great variance in attack motives and in the time and process required to radicalize these different actors to the point that they decide to carry out a strike. But once any of these actors decides to take action against a target, there is remarkable similarity in the planning process.

## IDENTIFYING A TARGET

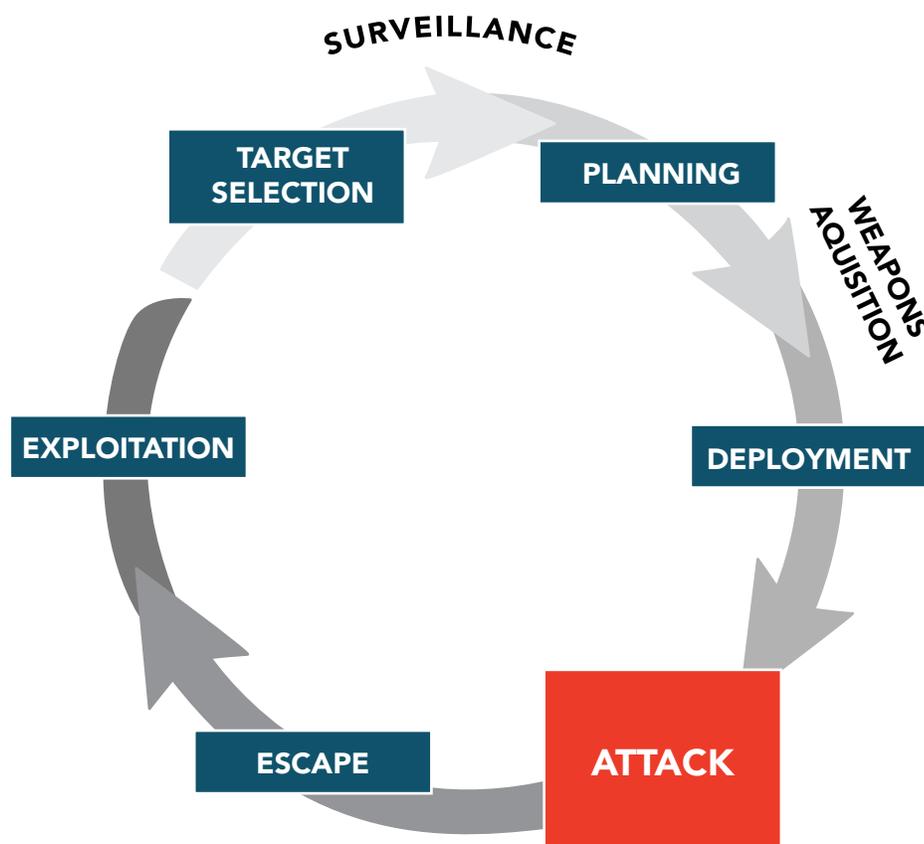
Often an actor will come up with a list of potential targets and then select one on which to focus. In some cases, the actor has pre-selected a method of attack, such as a vehicle-borne improvised explosive device, and looks for targets that would be vulnerable to that specific type of attack. In other cases, the actor will pick a target and then devise a method of attack based on its characteristics and vulnerabilities. The execution of these steps can be somewhat fluid: Some degree of planning or preparation might come before target selection, and sometimes target selection will be altered during the planning process. The time required to execute these steps can also vary considerably, based on the simplicity or complexity of the operation being planned and the capabilities of the actor.

## SURVEILLANCE

Frequently, attack planners will conduct detailed surveillance of potential targets to determine what security measures are in place around the target and to gauge whether they have the ability to get past them. If the target is too difficult to strike (a “hard target”) planners will typically move on to the next one on their list rather than risk failure. We refer to this stage as pre-operational surveillance — surveillance that is conducted before the operation is fully planned.

A second round of surveillance comes after the target has been selected. This round will be far more detailed and is intended to provide all the details necessary for planning the attack. For example, if the target is a static facility, planners now will generally try to obtain a detailed description of physical security features and

## The Terrorist Attack Cycle



Copyright Stratfor 2016 [www.stratfor.com](http://www.stratfor.com)

security force procedures. They also will focus on establishing a baseline understanding of the activity that can be expected around the facility at the time of day the attack is anticipated.

If the target is a person, his or her residence, office and other frequented haunts will be surveilled. Additionally, the surveillance team will look for patterns and routines that the target follows between these known locations. Planners often will analyze the person's usual routes, looking for choke points (places that must be passed to get from one point to another). If the surveillance team identifies a choke point that the person passes through predictably, they will then try to determine whether attackers can deploy to that point in secret, whether they will be able to spot and control the target from that location, and whether good escape routes are available. If the location meets those criteria, this point frequently will be chosen as the attack site.

It should be noted that in some types of attacks — such as a suicide attack or acts carried out by a mentally disturbed person — escape is not necessarily a factor considered during the planning process.

## FURTHER PREPARATION

During the planning phase, the personnel who will actually carry out the attack are identified and trained in any special skills they may require for the mission — including languages, marksmanship, hand-to-hand combat, small-boat handling or land navigation. To protect operational security, the operatives may not be briefed in any great detail about the target of their operation until they are very close to being deployed.

Often, the planning phase will end with a dry run — for example, some of the 9/11 hijackers took their assigned flights for the attack in August 2001. While conducting a dry run, the attackers will generally be unarmed to ensure they do not needlessly attract attention from law enforcement. The dry run may result in final adjustments to the plan.

Sometimes an attacker will have acquired weapons for the attack before the planning phase; in other cases, the concept of the operation will be constrained by the weapons and money available. But frequently, the weapons for the attack will be acquired during the planning phase, after the target has been selected and the means of attack established.

## DEPLOYMENT

Once planning, training and weapons acquisition are complete, the attack team can be deployed. The team frequently will conduct surveillance of the target one last time, especially if the target is mobile and the attack team is waiting at a predetermined site.

If it was properly planned, an attack is very likely to succeed once it has moved to the operational phase. Sometimes attacks fail because of mistakes, bad luck, or excellent attack recognition and reaction, but by and large there is no way to stop an attack once it has been set in motion.

Unless the operation has been planned as a suicide mission — or, as a final step in the cycle, the attackers plan to be captured as part of the media exploitation phase — they will seek to escape the scene after the attack is carried out.

These rules of attack planning vary little from group to group or target to target. Therefore, a thoughtful observer can use the attack cycle model to understand how an attack was planned and executed.

## Vulnerabilities

While plots are occasionally thwarted at the last second, security personnel for the most part must detect and interdict the plot before it gets to the attack phase if they are to have any chance of stopping it. Once the bullets fly or the explosive device is detonated, there is little security forces can do but initiate their immediate action drills in efforts to mitigate the impact of

the attack and reduce casualty counts. Emphasis must be placed on identifying attackers early in the process, well before they are in a position to strike.

Unless security forces have a source inside the group that is planning the attack or manage to intercept the group's communications, the only way to identify attack planners is by noting their actions. This is especially true of a lone wolf attack, where there are no co-conspirators and no external communication occurs. The earliest point in the attack cycle that the attackers can be identified by their actions is during the pre-operational surveillance period.

Viewed with hindsight, it is frequently found that people who conduct terrorist surveillance tend to be quite sloppy — even amateurish — in their surveillance tradecraft. This creates a significant vulnerability in the terrorist attack cycle.

As noted, additional surveillance is often conducted at later stages of the attack cycle, such as in the planning stage and even sometimes in the attack stage. Each window of surveillance, to include the dry run if conducted, provides an additional opportunity for the assailants to be identified and an attack prevented.

During the planning phase and as the operatives prepare to deploy, communication between and movement of group members often increases. Additionally, members may engage in outside training that can attract attention — such as playing paintball, visiting the firing range or, as with the 9/11 pilots, attending flight schools. Money transfers might also take place at this stage. All of these scenarios can leave signs that tip off authorities.

Another significant vulnerability during the attack cycle comes with weapons acquisition. This is especially pronounced when dealing with inexperienced grassroots operatives, who tend to aspire to conduct spectacular attacks that are far beyond their capabilities. For example, a grassroots operative or cell might

decide they want to carry out a bombing, even if they don't know how to make improvised explosive devices. Some grassroots offenders have also tried to acquire Stinger anti-aircraft missiles, automatic firearms or hand grenades. When confronting the gap between their goals and capabilities, grassroots operatives often reach out to someone for help with their attack instead of settling on a more modest plan within their realm of ability. In many cases, these types of grassroots plots have been disrupted by police or domestic security agency informants.

As far back as 2009, jihadist leaders such as Nasir al-Wahayshi of al Qaeda in the Arabian Peninsula recognized this problem and began to encourage grassroots jihadists to focus on conducting simple attacks against soft targets. It has taken several years for evidence that attackers are actually following his advice to emerge as a trend in the jihadist realm, but since 2014 there has been a discernible trend toward simpler attacks. Other types of grassroots militants, such as anarchists, have displayed far greater comfort in conducting simple attacks with readily available items.

## **Detecting Terrorist Surveillance**

Although target surveillance is a necessary part of the planning process, it does not necessarily follow that terrorist planners are very good at it. Here, we'll examine surveillance more closely, with emphasis on what bad surveillance looks like.

### **EYES ON A POTENTIAL TARGET**

Unless the operation being planned involves something like a letter bomb, surveillance is a mandatory part of the planning cycle. 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 can see the location of a building and its general shape on Google



CCTV images of two out of four men wanted in connection with attempted suicide bombings in London, July 21, 2005. Left, a man flees Oval Underground station, right, a man at Warren Street Underground station. (SCOTLAND YARD VIA GETTY IMAGES)

Earth, but not 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 and its complexity (think, for example, of the many attack teams deployed in the November 2008 strikes in Mumbai, vs. the husband-and-wife shooter team in San Bernardino, Calif., in December 2015). Complex operations may require weeks or even months of surveillance, while a very simple operation may require only minutes. The amount of surveillance required for most attacks falls somewhere between these two extremes. Regardless, planners 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, but most people involved in terrorist planning simply do not devote the time nec-

essary to master the art of the tradecraft. And the main reason that so many have been able to get away with sloppy surveillance and demeanor is simply because most victims simply are not looking for them. But for those who do practice good situational awareness, the poor surveillance tradecraft exhibited by those planning attacks is good news. It allows them time to avoid an immediate threat and to contact the authorities.

## KEYING ON Demeanor

To master the art of surveillance tradecraft, one needs to master the ability to display appropriate demeanor for whatever situation he or she is in. Practicing good demeanor is not intuitive. In fact, the things involved in maintaining 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. In a sense, 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 "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. Even experienced surveillance operatives occasionally have the feeling of being burned; the difference is that, due to their training, they are able to control their reaction and behave normally despite the sensation. They are able to maintain a normal-looking demeanor while their insides are screaming that the person they are watching has seen them.

Another very common mistake made by amateurs in surveillance is the failure to get into proper "character" for the job ("cover for status") or, when in character, appearing in places or carrying out activities that are incongruent with the character's "costume" ("cover for action").

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 he or she 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 tend to just lurk and look totally out of place.

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 uses the acronym "TEDD" to illustrate the principles that can be used to identify surveillance conducted by counterintelligence agencies. 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.

For an individual, TEDD is really relevant only 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 — not you personally — you likely won't have an opportunity to make environment and distance correlations, and perhaps not even time. In all probability, you would have only the demeanor of the surveillant to key on. Therefore, demeanor is the most critical of the four elements in recognizing surveillance. Demeanor also works in tandem with all the other elements: 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 insider attacks (such as the 2009 Fort Hood shootings or 2015 San Bernardino attacks). In these instances, the assailant was an insider, worked at a facility and had solid cover for action and cover for status. In these cases, then, demeanor is also critical in identifying bad intent.

The fact that operatives conducting surveillance over an extended period can change their clothes 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. 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.

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. Maintaining a state of relaxed awareness — and understanding the vulnerabilities in the attack planning cycle — are the keys to an effective corporate security plan. ■



## STRATFOR PROVIDES **3** CORE ENTERPRISE PRODUCTS

### ENTERPRISE MEMBERSHIP

Stratfor's Enterprise Membership platform organizes and delivers daily, weekly and monthly analysis to meet the needs of busy executives, investors and fund managers as well as military and academic professionals. Stratfor Enterprise Memberships leverage technology to disseminate content across organizations and can be customized to fit every size organization and budget.

### CUSTOM ADVISORY SERVICES

Our advisory engagements focus on direct contact with a team of analysts, consultants and strategists that supports our clients' business objectives by performing a range of advisory services, including risk assessments, global intelligence monitoring, strategic planning support, and protective intelligence, among others.

### KEYNOTE SPEECHES & METHODOLOGY TRAINING

Stratfor's keynote speakers deliver insightful, thought-provoking presentations on current headlines and future trends for industry events and corporate gatherings. Stratfor can also provide training offering insight into its methodology for developing such analysis and forecasting.

---

CONTACT: **[business@stratfor.com](mailto:business@stratfor.com)**

WEBSITE: **[stratfor.com/enterprise](http://stratfor.com/enterprise)**