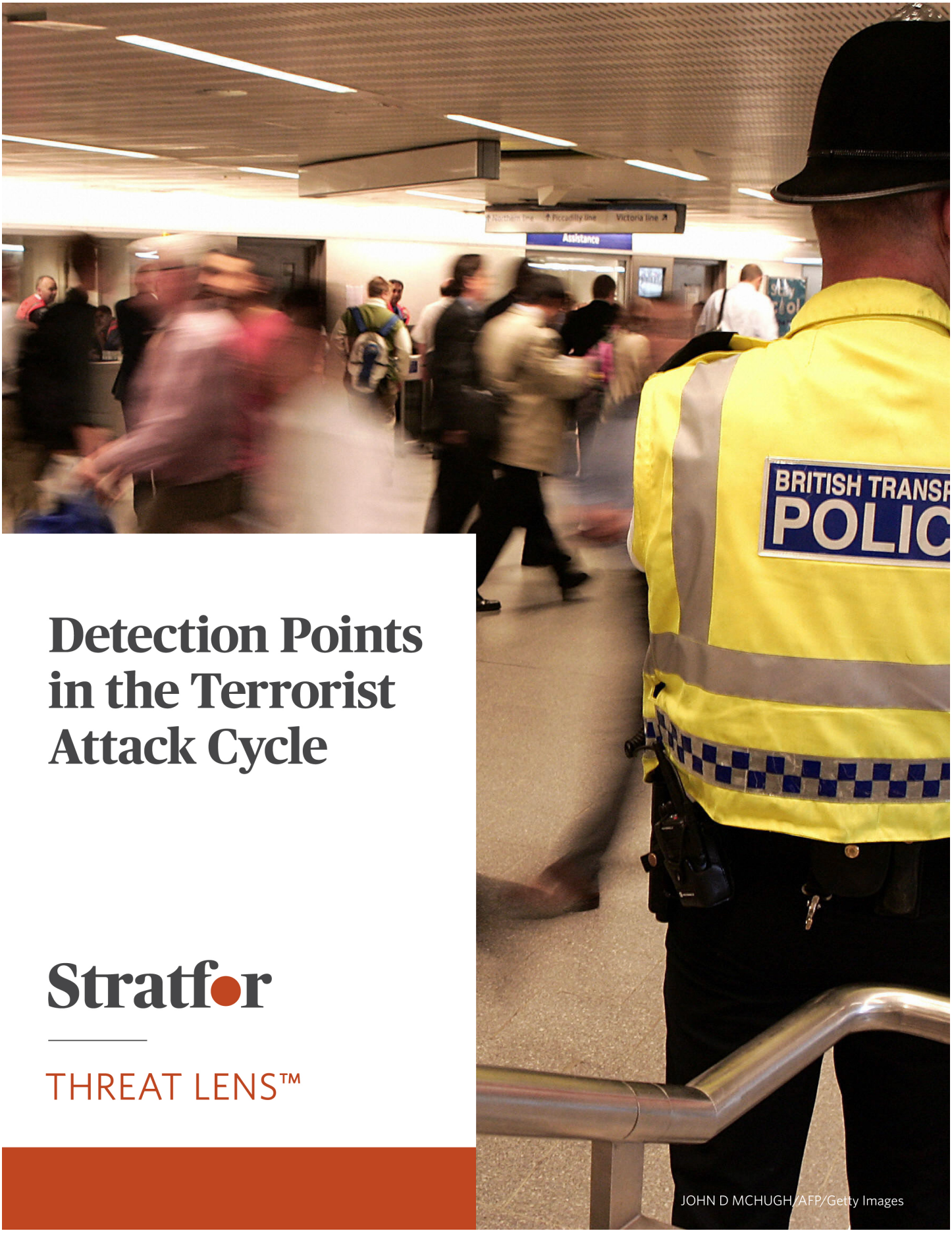
Detection Points in the Terrorist Attack Cycle

Stratfor

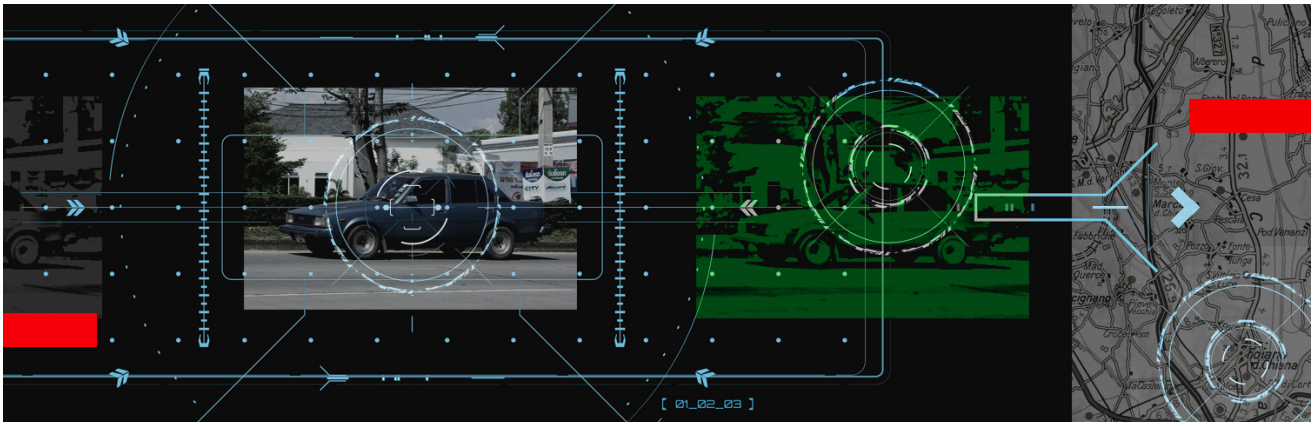
THREAT LENS™



JOHN D MCHUGH/AFP/Getty Images

ANALYSIS

Detection Points in the Terrorist Attack Cycle



Last week's Security Weekly discussed the fact that terrorism is a tactic used by many different classes of actorsand that, while the perpetrators and tactics of terrorism may change in response to shifts in larger geopolitical cycles, these changes will never result in the end of terrorism. Since that analysis was written, there have been jihadist-related attacks in Afghanistan, Nigeria, Yemen and Pakistan, an assassination attempt against the president of Abkhazia, and a failed timed-incendiary attack against the Athens subway. (The latter incident, which militant anarchists claimed, reinforces that jihadists are not the only ones who practice terrorism.)

But while terrorism is a continuing concern, it can be understood, and measures can be taken to thwart terrorist plots and mitigate the effects of attacks. Perhaps the most important and fundamental point to understand about terrorism is that attacks do not appear out of nowhere. Individuals planning a terrorist attack follow a discernible cycle – and that cycle and the behaviors associated with it can be observed if they are being looked for. We refer to these points where terrorism-related behavior can be most readily observed as vulnerabilities in the terrorist attack cycle.

The Attack Cycle

Many different actors can commit terrorist attacks, including sophisticated transnational terrorist groups like al Qaeda; regional militant groups like India's Maoist Naxalites; small, independent cells like the anarchists in Greece; and lone wolves like Oslo attacker Anders Breivik. 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 conduct a terrorist attack. But once any of these actors decides to launch an attack, there is remarkable similarity in the planning process.

First, there is the process of selecting or identifying a target. Often an actor will come up with a list of potential targets and then select one to focus on. In some cases, the actor has preselected a method of attack, such as a vehicle-borne improvised explosive device, and wants to find a target 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 that target's characteristics and vulnerabilities. Simply put, the execution of these steps can be somewhat fluid; some degree of planning or preparation can 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. Some attacks can be planned and executed within hours or days, while more complex plans, such as those used in the 9/11 or Mumbai attacks, may take months or even years to complete.

Frequently, those planning an attack 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 successfully attack it. If the target is too difficult to attack – commonly known as a hard target – the attack planners will typically move on to their next target, which may prove easier to attack. (When they do continue with attacks against targets whose security measures exceed the attackers' capabilities, those attacks fail.) We refer to this stage as preoperational surveillance, which means surveillance that is conducted before the operation is fully planned.

After the target has been selected, a second round of surveillance is conducted. This round will be far more detailed and is intended to provide all the details necessary for planning the attack. For example, if the attack is being planned against a static facility, this round of surveillance will generally try to obtain a detailed description of the target's physical security features and security force procedures. It will also 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 of the attack is an individual, the individual's residence, office and other places the individual frequents will be surveilled. Additionally, the surveillance team will look for patterns and routines that the target follows between these known locations. The team will often analyze the target's usual routes looking for choke points, or places the target must pass to get from one point to another. If the surveillance team identifies a choke point that the target passes through predictably, it will then try to determine whether that point will allow the attackers to deploy in secret, permit them to spot and control the target, and provide them with good escape routes. If it does, this point will frequently be chosen as the attack site.

In the case of large organizations, different groups or individuals may conduct different phases of the surveillance. Many organizations use specialized operatives for surveillance, though the operational planner will often attempt to get eyes on the target to help with the planning process. For instance, it is known from court testimony in the Mumbai case that David Headley made five extended trips to Mumbai as those attacks were being planned. The repeated trips were required because the operational commanders in Pakistan considered India a hostile environment and the operational planners could not go there to conduct the surveillance themselves. As a result, Headley was sent to observe and report on specific things as planning for the attacks progressed.

During the planning phase, the personnel to be used in the attacks 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.

Many times the planning phase will end with a dry run, as the preparation did for the 9/11 attacks, when some of the hijackers took their assigned flights in August 2001. While conducting a dry run, the attackers will generally be unarmed to ensure they do not needlessly bring law enforcement attention to themselves.

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

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

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

At the attack's conclusion, the attackers will seek to escape the scene. The exception is suicide attacks or when, like Breivik, the attacker intends to be captured as part of the media exploitation phase, the final step in the cycle.

Regardless of whether the attack is a suicide attack against a church in Nigeria or a timed-incendiary attack against a subway in Athens, the same attack cycle is followed. With an eye toward averting future attacks, 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, for the most part law enforcement and security personnel must detect and interdict the plot before it gets to the attack phase 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 an effort to reduce the body count. This means that an emphasis must be placed on identifying attackers earlier 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 no external communication occurs. The earliest point in the attack cycle that the attackers can be identified by their actions is during the preoperational surveillance required for target identification.

There is a widely held conception that terrorist surveillance is generally sophisticated and almost invisible, but when viewed in hindsight, it is frequently discovered that individuals who conduct terrorist surveillance tend to be quite sloppy and even amateurish in their surveillance tradecraft. We will discuss what bad surveillance looks like, and how to recognize it, in more detail next week, but for now it is sufficient to say that poor surveillance tradecraft is a significant vulnerability in the terrorist attack cycle.

As noted above, 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, as the attackers track the target from a known location to the attack site. Each instance of surveillance provides an additional opportunity for the assailants to be identified and the attack to be prevented.

During the planning phase and as the operatives prepare to deploy, communication between and movement of group members often increases. Additionally, group members may engage in outside training that can attract attention, such as playing paintball, visiting the firing range or, as was the case with the 9/11 pilots, attending flight schools. This increase in activity, which also might include money transfers, leaves signs that could tip off the authorities.

Another significant vulnerability during the attack cycle is weapons acquisition. This vulnerability 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, they may decide they want to conduct a bombing attack even though they do not know how to make improvised explosive devices. It is also not uncommon for such individuals to try to acquire Stinger anti-aircraft missiles, automatic firearms or hand grenades. When confronted by this gap between their capability and their aspirations, grassroots operatives will often reach out to someone for help with their attack instead of settling on an attack that is within their ability. Increasingly, the people such would-be attackers are encountering when they reach out are police or domestic security agency informants.

As far back as 2010, 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. Nevertheless, grassroots jihadists are consistently drawn toward spectacular attacks, as seen in the Feb. 17 arrest near the U.S. Capitol of a Moroccan man who thought his handler, who was in fact an FBI informant, had equipped him for a suicide attack. Unlike most jihadists, other types of grassroots militants, such as anarchists, are far more comfortable conducting simple attacks with readily available items.

Personality traits and psychological profiles aside, anyone desiring to plan a terrorist attack must follow the attack planning cycle, which at certain stages will necessarily open them up to detection.