Soft Targets – Terrorist Methodology and Attack Indicators
By Ali Tehrani, Senior Director FocusPoint International

The recent terrorist attacks that have occurred in countries throughout the world have received extensive international media coverage with reporters, eyewitnesses, subject matter experts and well-known news anchors commenting on each event. We often hear the same new age terror terminology used by those who report and comment in the aftermath of each attack.

One term that is frequently used to describe the location of an attack is ‘soft target’. This expression has a particular connotation for the uneducated listener, who may not have been exposed to terrorist-specific vernacular and most likely thinks that ‘soft’ means structurally soft. This is obviously inaccurate; the term ‘soft’ refers to easily accessible. To understand an attacker’s target selection, we have to understand the various phases of an attack. Most people think that the planning phase of an attack is less involved and relevant than the fast and furious execution phase. This is not the case, if it were, far fewer attacks would be successful.

There are some potential options identified before the selection of the actual target is chosen. The objective is to select a target that will produce the greatest results with the least amount of risk. The highest profiled location or site that has the weakest security measures is ideal in hopes of sending a message to the world for public support, to alter the future actions of a country’s government or leader, or simply to discredit a government’s ability to protect its citizens. All terrorist attacks have included some form of target intelligence before the attack; even the mentally deranged, lone attacker needs to plan. The only time terrorists might reveal their intention prior to an attack is when they are conducting surveillance.

There are illegitimate avenues in obtaining target intelligence, such as the use of an unknown informant. This is mostly applicable for attacks on high profile individuals. However, most target intelligence information gathered by a terrorist or terrorist group is acquired through numerous legitimate resources available to anyone including the Internet, television, radio, newspapers, phone apps, libraries, open source government directories, etc. With the advent of social media, unsuspecting victims often post droves of information valuable to terrorists. Most terrorist groups operate in small, unsophisticated teams when gathering target intelligence; however, ISIS and Al Qaeda have demonstrated exceptional planning and execution of terrorist operations. These more sophisticated groups continually update intelligence reports on target locations such as airports, government buildings, theaters, etc., for the purpose of assessing a location’s vulnerability. The terrorists will then simply update their information, prior to a planned attack. Some groups use personal computers to store their information but do so very carefully, since they are aware of invasive electronic surveillance capabilities of law enforcement and intelligence agencies.

Once sufficient information has been gathered, the process moves on to the operational planning phase. With the more sophisticated terrorist groups, it has been found that some perform rehearsals or dry runs. For example, terrorist groups test security strengths to predetermine their chances of success. During the operational planning phase, the group’s top priority is to assess its tactical advantage points.

Terrorists look for the following elements before every attack and require a sufficient probable number to complete their plan successfully:

- Surprise - a sudden, violent event in an area where no one suspected anything to happen
- High ground (topography) – Good vantage points overlooking the targeted area without being seen or using a crowd situation to avoid being suspected or detected by the target audience or security personnel
- Field of fire - The group or individual needs to be able to reach its target successfully with the assault device it is using
- Field of vision – Decent area coverage to discern anything or anyone that could impede the success of the attack
- Choice of time, place, and conditions – only the terrorist knows when, where and how the attack will unfold, otherwise there will be little chance of success
- Diversions, secondary or follow-up attack – this happens during the larger scale, multi-prong attacks
- Training capability - technical knowledge of sophisticated explosive devices or weaponry
- Sufficient logistics - money, vehicles, fake IDs, disguises, etc.
- Proper planning capability - e.g. a kidnapping involves
hundreds of details, such as; a safe haven, food, and water, 24-hour manpower coverage of the kidnapped individual, an escape route, etc.

- Ability to be at the attack site prior to attack - without arousing suspicion (minimum on site time required is 20 minutes)
- Escape route and plan - not all attackers intend to die themselves; they would rather escape to fight another day

In light of these extensive methods used by terrorists, we have to ask ourselves, what can be done to mitigate terrorist threats, and how do our governments deal with this? There are many distinct, sophisticated methods involving technology that we may never know about, if for no other reason than to safeguard the necessary secrecy protecting official networks and agents from being discovered by our adversaries.

International news media and governments are increasingly encouraging the public to report anything suspicious. This is a very tough task since every individual has a different concept of what is suspicious. Without any common denominators and discriminators, people tend to be misled by their preferences, preconceived notions and end up reporting something innocuous while missing the actual threat indicators.

In today’s world, internet based radicalization of young people puts terrorism and attack planning far closer to private citizens and families than ever before. The parents of the attackers have stated that they felt their sons had been taken away from them by some poisonous influence.

Here are some physical indicators of suspicious activities:

- Terrorists often resort to video or camera usage at non-tourist sites such as security operations or locations
- Asking unusual questions about security procedures
- Taking notes, drawing, using cellular phone, or tape recording
- Pacing off distances (using GPS)
- Vehicles parked for prolonged periods with passengers for no apparent reason
- Unusual encampments
- Ruses (static surveillance, disguised as beggar, demo, shoe shiner, food vendor)

- Deliberate penetration attempts
- Foot surveillance with 2-3 people working together
- Mobile surveillance on bikes, scooters, motorcycles, SUVs, cars, trucks or boats
- Unusual behavior (quickly looking away, etc.)
- Observing timing (bollards, gates, motorcades, security procedures)
- Climbing perimeter fencing (boundary probing)
- Watching the same individual or vehicle
- Suicide bomber key indicators:
  - Loose/bulky clothing inconsistent with weather/ disproportionate to body type
  - Bulges/exposed wires under clothing
  - Strange ‘chemical’ odors
  - Sweating, mumbling (prayers), sometimes loud yelling at the very moment of the attack
  - Unusually calm and detached behavior
  - Nervous - unresponsive (blank stare/trance-like) or preoccupied/focused/vigilant
  - Tightened hands (may hold detonation device)
  - Constantly moving/inability to stay still
  - Luggage or gym bag weighing more than it should
  - Hands in pockets of trousers/refuse to show hands
  - Stiff torso/lack of mobility from wearing explosive vest
- Has concealed communication device, cell or pager

The list goes on and unfortunately, there are never-ending changes in the tactics, techniques, and procedures of the terrorists. As individuals, private citizens and organizations we have to consider ourselves the ‘eyes and ears’ of our National Defense Agencies.

In conclusion, the term ‘soft target’ has a very broad and all-encompassing meaning. Being susceptible to radicalization makes one a ‘soft’ target. Not realizing that our children are being radicalized makes us ‘soft’ as a society. Insufficient information and intelligence on potential terrorists and inadequate security at potential targets make us ‘soft’ (susceptible) to growing terrorism. Unfortunately, there is no single answer to the many questions regarding our safety and security. It will be up to all of us to do everything possible to mitigate the various forms of threat. Education is key; awareness needs to be constant, and preparedness must no longer be interpreted as paranoia.