Lina Kolesnikova argues that soft targets are becoming more attractive to would-be terrorists, and calls for greater guidance for the public on how to respond in the event of an attack

TOUGHENING

The attacks of 11 September 2001 marked a change in terrorist attitudes, in that the aim is no longer merely to threaten and attract public attention, but also to kill as many people as possible. To paraphrase famous terrorism studies researcher J R White, killing was once an outcome of an operation – now killing is a terrorist operation itself. Terrorist groups of the 1960s and 70s tried to avoid mass casualties among the population; they fought with political elites, while simultaneously seeking public support. If we look at the sad list of attacks over the last 20 years, we observe attacks on so-called "soft" targets such as schools, youth camp, universities, hotels, restaurants and hospitals.

Analysing some of the recent soft target attacks, we see that this phenomenon is becoming even more dangerous, as the barriers are being lowered for new terrorists to become more destructive. For example, there has been a growth in "commando-street", or so-called "Mumbai" scenario attacks. Following the devastating attack in India in 2008, we have seen attempts to repeat its results in several other countries (with different numbers of perpetrators, in the name of varying causes and with different consequences). Lone-wolf execution-style attacks have also occurred in Norway (Breivik), France (Merah), Belgium (Amrani), Italy (Casseri) and in the UK (Adebolajo and Adebowale). There have been attacks on large groups in Nigeria and Kenya.

Some of these potential targets have become less soft for a number of reasons, making them more complex for would-be attackers. Attacks on soft targets give terrorists an obvious tactical advantage: for law enforcement it is easier to identify and disrupt plans to attack hard targets because the plotters need considerable financial and technical preparation, and more people involved. Soft targets attacks, however, may be performed by lone-wolves or small cells.

Such attacks can also been performed with the use of conventional weapons and explosives, which could be acquired relatively easily on the black market. Unfortunately, we can not hope for non-skilled local terrorists anymore either; the high number of training camps and hot spots supply and will continue to supply militants trained in a variety of weapons, combat and explosive skills. We may assume terrorists will continue to use conventional weapons but will look for unconventional way of carrying out their attacks. We also can expect attacks on sites at which children are present.

The traditional "3G" approach to physical security of "guards, guns, and gates" comes from the military. The idea is simple: to place obstacle in the way of intruders and to use guards (with or without guns, according to the perceived threat) to control access through fixed entrances (gates), checking entrants to ensure they should be allowed in. This approach is based on the concept of "hardening" a perimeter to ensure that – hopefully – only invited guests come in, by making it difficult for all but the most highly-motivated intruders to enter.

©Getty Images

Crowded, low security facilities such as shopping centres present an attractive "soft" target to potential terrorists

Many soft targets have no or only one or two elements of physical protection, however – usually guards (in Europe mostly without guns) and/or gates. Some soft targets are patrolled by mobile police units with few or no guns as well. While soft targets are generally buildings, places and/or gatherings, we can also see that human individuals (disregarding their location) become soft targets too (as was seen with the murder of soldier Lee Rigby in London in 2013). They might be random members of the public rather than VIPs and, therefore, cannot justify physical protection of any kind.

SOFT TARGETS

There are several different categories of soft targets that must be distinguished, as it is practically impossible to define a "one size fits all" approach for all of them. Hence, "differentiation and specialisation" of soft targets and their protection is necessary. There is no silver bullet to solve problems of protection of all soft targets – each system has to be addressed and evaluated separately.

An original "guards, guns and gate" approach assumes the existence of a perimeter, and some soft targets might have some sort of perimeter defined. If one can define the perimeter for certain category of soft targets (such as a football stadium), then application of "perimiter-based" security still might make sense. Most soft target installations do not have precise perimeter, however, and members of the public and security personnel must act as guards themselves but without guns. As we assume that population and personnel can not hold guns to protect themselves, we may only add a forth G – guidance. Assuming that, in the event of shooting or an explosion there are only three possible reactions – to run, hide or fight – we must provide correct guidance to people on where to run and where to hide.

First of all, one needs to carry out a risk assessment and to prepare for deterrence and response. Law enforcement agencies should provide basic information such as standard questionnaires listing threats. They may also distribute basic information on the level of threats to the general population, as well as to owners/management of certain installations or event organisers. The owners/management should be responsible themselves for extensive risk assessments, determining specific risks, threats and vulnerabilities of their respective installations or venues. Categories of risk include strategic risks, operational risks, and financial risks. Comprehensive threat and risk assessments involve: identifying potential threats, including terrorism, but also common crimes, fires, vandalism, natural disasters and etc; measuring possible damages from such threats (impact analysis); defining the likelihood that the problems will occur; and developing cost estimates and actions to prevent the threats or minimising the impacts of the threats.

Proactive counter-measures can be grouped around three main areas: deterrence, prevention and detection of sources of incidents. Within the context of soft targets there is not much that can be done in terms of deterrence or protection (costs and effects of elaborated protection might become prohibitive for the to-be-protected target). Owners must be aware that they risk a terrorist attack if they are perceived to become a soft target. The most effective way to avoid identification as a soft target is to remain at a high level of situational awareness. Deterrence can be very helpful in discouraging attacks, though it is less useful against an adversary who chooses to attack regardless.

The protection of any soft target is not an easy task. Due to the high number of people (or in cases of public transportation, massive number), it seems hard for regular security personnel to observe, screen and control every single threat and person. In such circumstances, the attitude of members of the public themselves might be a decisive factor in securing the place. Setting up and leveraging public-private co-operation could result in members of the public assisting security personnel to identify possible suspicious people or activities. One of the key components here is awareness among the population and personnel of possible signals.

©Getty Images

We the people: by offering the public guidance on how to respond to major incidents, the effects can be mitigated

Protecting soft targets from potential terrorist attacks without compromising the accessibility and/or efficiency is the critical challenge. Clearly, if one wishes to enhance the level of public security, the best course of action is to develop and implement a customised security concept and system, based on a site survey and risk assessment. Such a system would meet the specific operator's needs, and taking into account its particular operational profile and the characteristics of the soft target. As part of this process, the actual threats and risks faced by the security provider are to be analysed carefully, to ensure the solution developed provides optimal security coverage for the resources invested. A comprehensive system, which may be implemented in a modular manner, will provide the most cost-effective security response to the variety of threats faced by people, employees and facilities, while ensuring the undisrupted operation of the public system and/or the related commercial activities.

In many countries authorities have adopted some measures to help prevent attacks on soft targets, including random searches of people and baggage, increased presence of security officers and bomb-sniffing canine teams, CCTV and anti-intrusion means (virtual barriers), the removal or hardening of trash cans, enforcement of restricted-access zones at public transportation facilities and infrastructures. In addition to conventional methods, in each particular situation one needs to consider feasibility of the unconventional methods. Security officials should build up a layered security system, implementing a variety of security controls and applying them differentially in such a way as to disturb the mass-throughput operation to a least possible degree.

Risk assessments feed response plans for worst-case scenarios such as terrorism, but can also be thoroughly prepared to deal with ordinary crimes and incidents such as fights, drunkenness, etc). Every plan should start with prompt identification of the fact of an incident, whether a disaster or attack. Simple measures that may help are proper use and monitoring of use of the access control systems, CCTV and on-site monitoring by guards or trained personnel. Both people and traffic should be monitored. Fire, heat and smoke sensors are already basic equipment of most installations. Movement detectors for protected areas might also be employed. Overall, awareness training of the on-site personnel (shop assistants, etc) is the key of getting information from the field quickly to the co-ordination centre for prompt identification of the event. As soon as the type of the event is identified, the specific plan can be activated.

Remember that the initial minutes of the attack may lead either to huge numbers of casualties or to minimum casualties. Prompt reaction of the on-site personnel guiding (to a possible extent) the rest of people is the best chance for positive outcome. Therefore, response teams and on-site personnel should be trained for active shooter situations and basic crowd control management. One has to remember that panic is a prime concern to be dealt with.

Infrastructure can also be better prepared, for example by increasing the number of escape routes and employing segmentation. While not a preventive measure as such, this might permit the creation of safe segments inside and outside the installation, thus securing most of people. The increase of escape routes would also demand an increase in the number of terrorists participating in an attack. Such an increase would lead to a higher probability of intelligence identifying the threat beforehand, as well as identifying the build-up on-site prior to the event. This, in turn, might become a deterrent measure.

The 3G approach should therefore be considered and might make some sense if and only when some sort of perimeter can be defined for the identified soft target. Hence, only some segments (types) of soft targets might benefit from the "guns, guards and gates" approach. A 4G (3G+Guidance) approach is therefore needed to protect most soft targets. We understand that, outside military bases, security guards are not normally trained or authorised to use deadly force as a response. If we have guards they should be trained for active shooters situations. The time for untrained "mall cops" is over. For some particular situations mobile security assets should also be deployed where they are most needed (based on continuous threat and risk assessments). Finally, where standoff is limited, physical barriers provide a key line of defence. Visible security in the form of gates, planters, trees and urban architecture will serve as a deterrent, encouraging the search for a softer target.

Lina Kolesnikova is a Russian-born, Brussels-based Fellow of ICPEM. Lina provides consultancy in the area of security, risk and crisis management to number of organisations within both the private and public sectors. She is a member of the advisory board for Crisis Response Journal and CBRNE-Terrorism Newsletter.