SOFT TARGETS

Lina Kolesnikova *examines the increasing challenges being faced by soft targets and what can be done to keep them safe*

Soft targets are understood as being those that have no state, military, security or political affiliation. They are often symbolic and can include public, commercial and business targets, such as shopping centres, stock exchanges, trade centres, religious sites and utility companies. They might be any other mass gatherings too, eg sport or cultural events. But high risks are not linked to the 'mass' aspect exclusively.

Analysing some of the recent soft-target attacks, we see that the phenomenon of attacks on soft targets is becoming even more dangerous as barriers are being lowered for new terrorists to be more destructive. In the past, terrorists were still seeking some sort of understanding and support from society. In some way we had a phenomena of Stockholm syndrome, when people tried to understand the motivation behind the attack and look for justification of terrorists' deeds. That has changed, and terrorists do not seem to care about this any more. Rather the opposite, the deadlier the impact is, the better it is for them. There has been a growth in attacks targeting large groups of people – suicide bombing, commando-street and/or active shooter (so-called 'Mumbai' scenario) attacks. Meanwhile arson, attacks by vehicle or knifing are also tools for modern terrorists. We have an increasing number of attacks against individuals – symbolic attacks such as a soldier in the UK, a Catholic priest in France, police officers in Belgium, *etc*.

SOME VENUES HAVE HIGH EMPLOYEE TURNOVER, MAKING BACKGROUND CHECKS VERY DIFFICULT

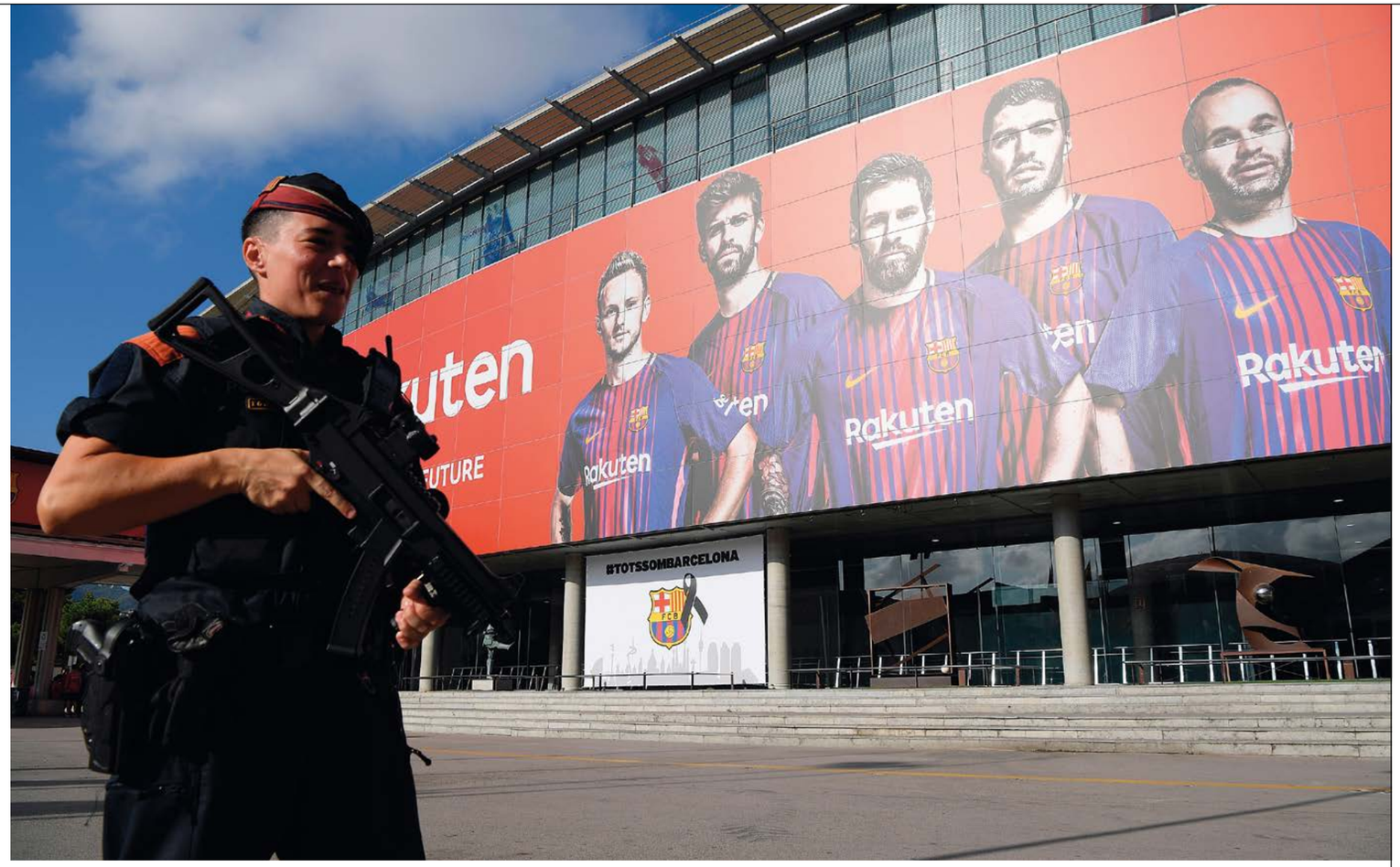
The traditional approach to physical security "guards, guns, and gates" (3G) comes from the military. The idea is simple: to place obstacles in the way of intruders and to use guards (with or without guns, according to perceived threat) to control access through fixed entrances (gates), checking entrants to ensure they should be allowed in. This approach is based on hardening of perimeters to ensure that only invited guests come in, by making it difficult for all but the most highly motivated intruders to enter. Hard targets employ concentric rings of security or Concentric Circles of Protection sometimes also called 'Security in Depth'. This concept involves the use of multiple 'rings' or layers of security. The first layer is located at the boundary of the site and additional layers are provided as you move inward through the building toward the high-value assets. We, therefore, stipulate that when certain installation has the presence of all three elements, it is a hard target. When we have presence of all three, we may say we deal with hard targets.

This concept in itself is constrained with the further development of various transportation techniques – as, for example, various unmanned or manned solutions for moving over the air and under the water (and, on the surface as well). Typical implementation of the 3G model, as we may think of it, for the usual soft targets, is rather two dimensional and might provide reasonable protection when the attack vectors develop on the surface (on land, should we say). With the advent and wide commercial availability of solutions for air, water and surface transportation, the model needs to become three, four or even five dimensional.

EYES TO THE SKIES

Third dimension is still geometrical. While fences with guards are good, there is no particular difficulty to overcome this barrier via the air using some sort of drone. Think of drones for commercial packages delivery – they will be able to carry quite considerable weight. Even current kids' toys can often carry a weight of a grenade. This type of activity is regularly be observed in prisons, where drones bring mobile phones and SIM cards to those beyond the fence. So, controlling 'front, back, left and right' should be enhanced with control 'up and down'. Here you may think of some kind of under-surface and over the air protection – roofs (like in the stadiums) or the like.

The fourth dimension is time. Multi-dimensional threat and attack identification should be on all the time and cannot be 'switched on' in the event of an approach, as preparation of the attack does not take much time, and cannot be assumed to be visible to or detectable by any number of circles (or, rather, spheres) of protection. Needless to say, maintaining such four-dimensional protection is usually very costly. Therefore, protection should go as far as beyond the fence/gate as possible and be on alert all the time. It is not at all obvious. Think of a football stadium: security measures can be reinforced on the day of a match (sniffing canine teams for explosives, strong police presence and stringent access control), and then the stadium can be on low profile for a week or a month until the next big event.



Security barriers were put up at the entrances of soft targets like Barcelona's Camp Nou, following the attack on Las Ramblas

The fifth dimension is a tricky one. It is not feasible to have a hard fence (or a roof) over each mass gathering or every street. Technically, this might be imaginable for the surface, but it will be quasi-impossible in the air or in the water. Understanding that any fence can be penetrated brings us to the understanding that on top of the usual does-not-matter-how-many-layers of the fence-like perimeter defences, we need to have ones that will render attacking capability identifiable as early as possible, vulnerable to the guards' countermeasures. Think of signal jamming techniques that may effectively render communication impossible for mobile phones, drones with remote control and the like. Such dimension brings us to the understanding that physical barriers alone (former 3G model) cannot serve as solid protection any more when all these modern technologies are readily available to practically everyone at very low cost.

Returning to soft targets, there are differing degrees based on the level of access. The most difficult ones are those with open access. These are religious sites (churches, *etc*.), markets, shopping centres, festivals or community festival gatherings on certain holidays.

Hotels are typical examples of so-called soft access soft targets. They are open to guests, but have some restrictions on after hours and have staff-only areas. Meanwhile, screening and verification processes are low profile. Museums, concerts, theme parks and sports venues have ticketed access that has, in general, nothing to do with any protection. Schools, universities and offices of public administration are open to public, but have zones that demand special security screening or have no public access at all. Therefore, these facilities have hybrid access.

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 a specific category of soft targets (eg a football match), then application of 'perimeter-based' security still might make sense. Urban venues often have no setback. Positive identification is difficult for one-time guests and visitors. Security must be provided even for facilities that have limited funds for security as well as staff shortages. Some venues have high turnover rates for employees or have seasonal employment exacerbating training and background checks.

Picture credit: Getty

Any perimeter is not an absolute value and is not always consistent. One may use the airport as an example – one part of a perimeter is there for security of/from travellers, another– for employees and a third for partners or suppliers.

Cyber defence is a buzzword nowadays. But, somehow there is a similar situation with the IT systems – one set of controls (perimeter) exist for clients, another for teams actually managing systems and these controls for clients; where management is often done remotely. So, on one side, the system should have a strong perimeter, while on another side there are intended doors, eg to get service teams on board in case of a need or alert them of such a need.

THE TRADITIONAL 3G GUARDS, GUNS, AND GATES APPROACH COMES FROM THE MILITARY

We all know that there are measures of different nature – preventing, deterring, detecting, mitigating, as well as measures aiming at preparation (think of resilience) and recovery.

Within the context of the perimeter discussion, we may concentrate on first four types: Preventing – someone can see a row of armed soldiers not allowing (preventing) him or her to come through. Deterring – someone can see a row of armed soldiers and would be afraid to risk being shot or detained before, during or after reaching their target. Deterring affects protecting measures particularly in the case of modern terrorist attacks (eg suicide attacks. Detecting – people can see a row of armed soldiers, but still decide to penetrate. Soldiers would notice and raise an alarm or shoot. In case of an attack, the attempt to penetrate the row of soldiers (perimeter) will be evident and can trigger certain countermeasures. Mitigating – someone can see a row of armed soldiers, but still decides to penetrate. However, soldiers resist and do not allow entrance, or pursue the one that manages to penetrate the perimeter.

With that in mind, we arrive at a philosophical consideration. One trend is the globalisation, free exchange, freedom of travel with no borders and other 'jointing, coupling or connecting' developments. Another trend can be observed – more and more walls or landmine fields being constructed to segregate some from others; hence, to introduce segmentation. These two trends should be taken jointly into balanced consideration. We do want segments with assured security at and inside the perimeter. And we want these segments not to be segregated completely, but rather communicating and connected, *etc*.

THE PSYCHOLOGICAL ROLE

Perimeter plays an important psychological role in identifying the border between different sets of rules applicable outside and inside. Such differences might help detection capabilities of the defence model.

We understand now that any perimeter can no longer be considered as impenetrable, even if we make it multi-dimensional. Therefore, multi-layer defence no longer means a multi-layer perimeter; but rather any feasible perimeter combined with detecting and mitigating (and recovering) measures at any single point inside the perimeter. For example, this might include correlation of declared objectives (eg when people crossing each layer of a perimeter) and actual behaviour at any moment when inside (between the layers of a perimeter). Coupled with practical impediments in hardening soft targets, this drives us to the multi-capability "when at rest, standing still, passing through and on the move" defence model as the only one that makes any sense ●

Lina Kolesnikova is a Brussels-based homeland security consultant. She is a member of the Advisory Board for *Crisis Response* Journal.

Events like Wimbledon adopt a 3G approach to security

Picture credit: Getty