

OPERATIONAL STUDIES

www.operationalstudies.com

Copyright © 2007

The following paper was written by Mark Lonsdale while serving as a senior security consultant on a Department of Defense contract at a combined US/Iraqi military base north of Baghdad in early 2004. This is also the period when the four Blackwater contractors, one a close friend of Lonsdale's, were killed in Falluja and the Iraqi insurgency began a significant upward surge.

PHYSICAL SECURITY & VBIED BLAST PROTECTION

**A General Guidance for Military Commanders tasked with
Force Protection and FOB Security Operations**

By

Mark V. Lonsdale

Copyright©2004/2007

PREFACE

The purpose of this paper is to offer some guidance to military commanders and security managers on how to best protect their bases and facilities from insurgent attack. Keep in mind that security is seldom ideal, and even less so when restricted by budget and the limited availability of resources. Security counter measures can be further compromised by the terrain, the physical limitations of the base or work site, or lack of support at the command or appropriations level.

This paper is not intended as a criticism or even critique of any specific command or location, but merely as an academic discussion of the subject from a tactical perspective.

INTRODUCTION

Since the successful terrorist bombing of the US Marine barracks in Beirut (1983) killing over 240 Marines, and then the US Embassy Annex (1984), US military and governmental facilities have come under regular attack by suicide bombers and vehicle-borne improvised explosive devices (VBIEDs). The dramatic destruction of the Oklahoma City Federal Building in 1995 also served to further validate the viability of this form of attack.

In late 2003 and early 2004 these same terrorist tactics and vehicle bombs were used against US and coalition bases in Iraq, along with police stations, recruitment centers, civil defense units and NGO facilities. Particularly hard hit was the CPA and checkpoints around the Green Zone; and although these vehicle bombs had not penetrated the outer defenses, they caused significant casualties, disrupted operations, had an adverse affect on morale, and emboldened the anti-coalition forces (ACF) to attempt even more audacious attacks.

As a direct result of these attacks, US military commanders and base security managers were forced to re-evaluate their base security procedures and perimeter defenses. Unfortunately, neither of these subjects had been widely taught within the military system or disseminated in an easy to understand format. Hopefully this paper will help fill some of that void.

However, it must also be understood, and to quote the old adage, “that the best defense is a strong offense.” For base security this equates to aggressive patrolling outside the wire to deny the enemy access to the perimeter or the opportunity to observe the location and security procedures.

PHYSICAL SECURITY PRINCIPLES

Although actual security counter measures can be quite complex, they generally conform to one or more of the five basic principles of Physical Security.

These are:

- DETER
- DENY
- DETECT
- DELAY
- DESTROY

The first principle is to **deter** an attack by the appearance of a robust security program and substantial physical barriers. Deterrence also comes from an aggressive defensive posture, an alert security force, vehicle checkpoints, vehicles searches, guard towers, lighting, visible weapons positions, and fighting patrols pushing out from the immediate perimeter.

The next principle is to **deny** access through physical barriers and guard forces. The types of physical barriers include trenches, fences, concertina wire, razor ribbon, Hesco baskets, and Jersey and Alaskan concrete barriers. In the absence of construction resources, a professional guard force can be positioned to deny access. There is however a direct but inverse correlation between

physical security and the security guard force. The fewer the physical barriers, the greater the guard force required to secure the same area.

Early **detection** of an attempted intrusion or breach is critical to an effective fighting response. This is achieved through open ground, standoff, cleared areas, and alert perimeter security personnel. This can be augmented with electronic alarm systems, motion detectors, motion sensitive cameras, guard dogs, trip flares and other noise or light generating devices. At night, the guard force will require either perimeter lighting or NODs to detect an intrusion.

To **detect** explosive devices or VBIEDs requires a team of specially trained personnel and K-9s certified in IED / explosive identification and detection

When the physical barriers cannot stop an attack, they should at least be positioned to **delay** the enemy approach. **Delay** is achieved through the use of physical barriers such as trenches, fences, concertina wire, razor ribbon, Hescos, Jersey barriers or any improvised device that will slow or hinder the enemy's movement. The delaying barriers should give the guard force the time and opportunity to engage the enemy with effective fire, and for the QRF to reinforce the breach.

Where the Rules of Engagement allow for aggressive counter force, the intent will be to **destroy** the enemy with whatever weapons are available.

Last "D" is **deceased** – and that is the end result if fundamental security protocols are not followed. Lives may be needlessly lost for lack of command initiative and/or logistical support.

PERIMETER SECURITY

The three essentials for an effective perimeter system are **clear ground**, **physical barriers** and an **alert guard force**.

Without going into too greater detail, a typical external perimeter for a military or governmental facility would consist of the following physical features with security over-watch.

1. Clear terrain outside the perimeter to the maximum range possible
2. Signs outside the perimeter warning the public of the danger of approaching the outer fences and forbidding any form of photography of the installation.
3. Trenches and/or concertina barbed wire to impede and discourage approach to the outer fence
4. An outer fence usually constructed of 3- to 4-meter chain-link fence topped with triple strand barbed wire and razor ribbon.

5. Inner physical barriers such as concrete Jersey Barriers to prevent vehicles crashing through the fence. If a public road passes along the outside of the perimeter fence, then concrete crash barriers should be placed along the shoulder of the road to prevent vehicles veering off the road and into the fence.
6. Perimeter lighting controlled from the guard towers and/or a central location
7. An outer perimeter vehicle patrol road just inside the outer fence
8. Fifty to one hundred meters of clear ground
9. An inner perimeter fence similar to the outer perimeter fence
10. Guard towers positioned every 200 meters with mutually supporting over-watch and intersecting fire. Towers should be at least 4 meters high to the floor of the tower and offer adequate protection to the guard force from incoming fire and the elements. Towers should also be connected with either hard-wire comms or RF (VHF) communications.
11. Running inside the line of towers should be an additional access road and possibly indirect fire / bomb shelters if the threat warrants.

In general, tower guards, sentries, and soldiers manning checkpoints should be rotated or relieved every four hours. After four hours the level of alertness drops off sharply, particularly in hot climates and inclement weather.

The perimeter security towers and positions should be toured and inspected periodically by officers and senior NCOs during each shift. A Quick Reaction Force (QRF) should be on stand-by for an immediate response to any location on the perimeter.

SECURITY GATES & OPERATIONS

Security gates into high threat areas, or sites the terrorists would consider high value targets, are in fact not a single gate but rather a system of physical barriers and man-power. The three essentials for an effective security gate system are **early observation of approaching traffic, approach distance, physical barriers and alert guards.**

The guard force must be able to observe the approach of an enemy or vehicle at some distance, in excess of 300 meters, to be able to track and evaluate the vehicles approach and intent. This requires that the gate be sited with consideration to terrain, clear fields of observation, and unobstructed fields of fire.

If a vehicle(s) demonstrates its hostile intent by ignoring warnings or accelerating, then the guard force will have time to take appropriate counter measures. These counter measures will range from securing gates, activating

caltrops, to engaging the vehicle and driver with heavy weapons fire (.50 cal, MK 19, M240B, or Sniper).

If the vehicle(s) explodes, it should be at sufficient distance to cause minimal injury or loss of life.

There are a number of physical barriers that can be incorporated into a security gate beginning with some form of obstacle to slow approaching vehicles. The entire security gate operation should also be encircled by some form of security fence, usually 2-3 meter chain-link topped with barbed wire and/or razor ribbon.

Substantial heavy obstacles such as concrete Jersey barriers, sections of large-diameter concrete pipe, or earth filled drums should be used to slow the flow of traffic by being placed in zigzag patterns or chicanes. The spacing on these obstacles will vary depending on the size of vehicles processed through the gate, but in general, a vehicle should be forced to slow to no more than 5 mph (7 kph).

Various forms of tire-shredding devices or caltrops can also be used to deter fast approaching vehicles, and all areas designed to slow vehicles should be covered by at least one and preferably two machinegun (MG) weapons stations.

If drop-bar or swing-bar type security gates are to be used, then a steel cable should be run through the pipe. This can then be secured to a large concrete block of steel pipe set in concrete to make the gate more impenetrable. In the absence of a drop-bar gate, the cable alone can be used as long as it can be securely anchored at both ends.

At the beginning of the approach lane, and at regular intervals down the road, there should be signage in both English and the local language warning drivers and pedestrians of the speed limit and consequences of violating the posted rules. WARNING! SLOW! "Lethal Force is Authorized!"

The most critical component of any security gate operation is the guard force. These need to be alert professional soldiers, MPs or contractors with specialized training in gate operations and security procedures. They also need to be seasoned NCOs with the ability to be polite but assertive when necessary.

Guard posts and guard towers need to be sited so that they can identify approaching vehicles and have early recognition of a threat. This early recognition is critical if they are to have the time to activate counter measures, secure barriers or engage with effective fire.

A running man can cover 50 meters in six or seven seconds, and a vehicle traveling at 30 mph (44 feet per second / 15 meters per second) will cover 100 meters in 6 – 7 seconds. This is very little time for a guard to identify the threat

and react to it. This also illustrates the importance of having several hundred meters of visible run-up to any guard gate.

Guard towers should be sited so they have a clear view of the surrounding area and unobstructed fields of fire. Crew-served weapons should also be positioned to over-watch all guard posts, approaches, vehicle check-points (VCP) and search areas. Optimally, two weapons systems should be placed at right-angles with intersecting and supporting fire on areas of high threat such as initial check-points and inspection areas. Approaching drivers should feel intimidated by the firepower that can be brought into play if required.

In addition to suitable weapons systems, the guards in the guard towers and fixed positions should be issued range cards that give pre-measured distances to all visible landmarks. They should also be given the opportunity to test fire and zero their weapons under realistic range conditions that replicate the security towers.

At night the guard towers should be equipped with night observation devices (NODs) and weapons should have night weapons sights. As with iron sights and day-optics, it is essential that the night sights have also been zeroed to the weapons system.

VEHICLE BORNE IMPROVISED EXPLOSIVE DEVICES – VBIEDs

Car and Truck bombs (VBIEDs) have posed a significant threat to the US military since the bombing of the Marine Barracks in Beirut. They have also been successfully employed against targets such as the Oklahoma City Federal Building, the World Trade Center (1993), and more recently Kobar Towers.

Since deploying to Iraq in support of Operations Iraqi Freedom, VBIEDs have been successfully used against the entrances to the Green Zone, various police and military installations, government buildings, and most US military bases.

The obvious danger with VBIEDs is that they carry significant amounts of explosive ranging from 100 to 2,000 pounds, and that stopping a fast moving vehicle before it penetrates the security cordon is no easy matter.

The two primary types of explosive devices built into vehicles are military munitions and homemade explosives. The military munitions often consist of assorted 155mm artillery shells or mortar bombs primed with some form of C-4 or Semtex-type plastic explosive. This type of device may create a smaller blast since the over all explosive weight is smaller, but the high velocity fragmentation from the shell casings is deadly.

The non-military ordnance and home-made devices are often composed of some form of “fertilizer bomb” utilizing ammonium nitrate and fuel oil (AMFO). These are cheap to make and have already been found in Iraq in 300 to 500 pound devices. These large devices derive their devastating power from the fact that AMFO is a slower velocity explosive but generates incredible pushing power. Unlike military explosives which have high brisance and dissipate energy quickly, fertilizer bombs are similar to those used in quarrying and designed to move large amounts of earth. The shockwave will travel further and cause significant structural damage, so counter measures and blast barriers must be proportionately more robust.

There are a number of forces at play with a VBIED, most of which are quite deadly. The first is the initial blast and resulting shock wave that can knock down structures and cause massive overpressure injuries. Accompanying the blast wave is the high velocity primary fragmentation either from the device itself or shrapnel packed around the device.

A blast will also create secondary fragmentation from any of the surrounding structures to include concrete, glass, metal and rocks. The next concern is fall-out and fragmentation from the explosion that will be returning to earth at terminal velocity for several seconds after the initial blast. This necessitates overhead protection for the guard force.

Finally there are the risks of sympathetic detonation of surrounding vehicles as their gas tanks ignite; ammunition cooking off in damaged military vehicles; additional flammable substances that may be on trucks in the vicinity; or ammunition storage points or fuel farms that may have been the primary target of the attack.

When dealing with VBIEDs, the first security principal is to get the vehicle slowed down and stopped some distance from the initial US military checkpoint. The aim is to create as much distance as possible between a potential explosion and the US or coalition forces. If the driver becomes nervous and blows his load, then the loss of life should be limited to the two to four soldiers or local police at the initial checkpoint. A brutal but sad reality.

There should be at least three to four vehicle stops or checkpoints within the security system:

1. Initial ID check to make sure the car or truck is supposed to be entering the camp and the driver is who he says he is.
2. Vehicle search by Iraqi soldiers, police or civil defense
3. Vehicle search by US or coalition soldiers or security contractors
4. Detailed inspection of the vehicle’s load if required.

Explosives trained K-9s should be utilized during the first or second phases of the search process, but unfortunately, since the K-9 handlers are usually US

soldiers or contract force protection specialist, the K-9s are not utilized until the vehicle has reached the third or fourth checkpoint within the security zone.

If the suicide driver makes the decision to run the checkpoint with the hope of causing greater destruction, then the physical barriers should be sufficient to stop the vehicle; guards should have the time and appropriate weapons systems to engage the vehicle and driver with effective fire; and the surrounding berms, Hescos, Jersey and Alaskan barriers (T walls) should contain the blast resulting in minimal damage or loss of life.

GUARD FORCE TRAINING

Although alert and professional, US soldiers and Marines do not receive formal training in security gate operations during their basic training.

Programs need to be instituted to give soldiers the basic procedures for security gate operations, vehicle search procedure, ID check procedures, checkpoint interview techniques, IED identification, reaction to suspicious vehicles or individuals, tower operations, rules of engagement, and post-blast reaction drills.

This type of training can be coordinated through the Military Police, S-2 shop, Air Force force-protection instructors, or civilian contractors.

CONCLUSION

There are two factors that continue to create significant weakness in perimeter and gate security operations – flow rate and training. International airports are a good example of these problems that almost everyone has seen and experienced.

First, the airport must process high volumes of passengers and baggage in a timely manner. For example, 400 individuals, 800 pieces of hull baggage, and an equal number of carry-on pieces need to be processed for each international 747 flight in less than two hours.

Similarly, on a military base or FOB, 2,000 – 4,000 visitors and workers must be processed each day, along with several hundred non-military vehicles. The sheer volume that must be processed precludes any expectations of a detailed search of all vehicles, or computer database background review of drivers and visiting individuals.

The second problem is the lack of a professionally trained guard force. The slovenly minimum wage security worker has become an all too familiar sight at US airports, and while our soldiers have a professional appearance, they have

not received intense training in security operations, IED identification, terrorist methodology, smuggling and concealment methods, or individual interview and vetting.

These two issues – flow rate and lack of training – create significant opportunities for terrorists to capitalize on the weakness in base defenses.

Finally, and on a more military level, a base will always be vulnerable to attack if the area around the base is not heavily patrolled. Fighting patrols need to be operating 24/7 out to the maximum range of the enemy's weapons – for example, 3,000 – 5,000 meters for indirect fire weapons such as the mortar.

These patrols need to be augmented with HUMINT collection efforts, covert OPs, sniper operations, night ambushes, and surprise vehicle checkpoints. In this manner, and with this level of aggressive counter measures, the terrorists and insurgents will be forced to move on up the road to softer targets.

Copyright © 2007

END

For contract security and advisory services Operational Studies AND Mark Lonsdale can be contacted directly at OPStudies@aol.com