PROTECTIVE SECURITY OPERATIONS

Borough Events Security Guidance 2019

Protective marking	OFFICIAL
Publication Scheme Y/N	No
Title and Version	Borough Events Security Guidance 2019
Author	PS 221184 Lee BIRD
Summary	Briefing Note
For the Attention of	PSO CTPOs / Frontline Policing BCUs / MO6 Ceremonial Unit
Unit/Directorate	PSO CT SecCo Unit
Date Created	28/08/2019
Review Date	

Contents

1 Aim

This short report aims to raise awareness, encourage a common orientation and contextualise the most common types of terrorist threat and how they might be mitigated during borough events. It draws heavily on research conducted by the Centre for the Protection of National Infrastructure (CPNI).

This report is intended as a guidance document for BCU event planners, BCU SLT, and any non-police personnel who may have an interest in delivering local events throughout London that may not attract a large policing plan.

2 Introduction

The aim of this report is to look will look at initial action when dealing with Vehicle as a Weapon (VAW), Improvised Explosive Devices (IEDs), Marauding Terrorist Attacks (MTA), and Unmanned Aerial Vehicles (UAVs or 'Drones').

When policing a local event on borough BCU officers are asked to consider:

- Will the event attract large crowds and be reported by the media?
- Is it at an iconic location?
- Has the event been published beyond the local area - is it widely known?
- Will the military or police be deployed to or be in close proximity to the event?

In the last few years there have been a large number of significant terrorist attacks across Europe, Israel and the USA. These types of attack are regarded by terrorist groups as attractive attack method because they are relatively low in complexity, cheap, require little skill and are perceived as less likely to be detected in the planning phase. Terrorist groups actively promote the use of these attacks, particularly VAW attacks, within various terrorist publications.

The following areas will be briefly considered:

- The Threat
- Factors Influencing the Likelihood of an Attack
- Factors influencing the Impact of an Attack
- VAW Mitigation
- Initial response to IEDs
- Initial response to a marauding terrorist attack.
- Initial response to a UAV

3 The Threat

The main attack types used by terrorists are IED, MTA and VAW; either singularly or as part of a layered attack. Currently, VAW is an attack method used predominantly, but not exclusively, by Islamist Extremist; but there is intelligence to suggest that various terrorist groups are starting to draw inspiration from each other. Indeed, all of these attack methodologies are encouraged within various terrorist publications, often with the following themes:

• How to plan an attack and undertake reconnaissance of a target. The reader is advised to be mindful of obstacles along any planned attack route, such as street furniture, barriers and vehicles, and that more obstacles may be deployed close to event start time;

• How to choose a target. They suggest and encourage attacks on large outdoor temporary events, pedestrian congested streets, outdoor markets, gatherings and events;

• How to select / build a weapon, i.e. the best knives to buy or how to construct low sophistication IEDs or using fire as a weapon. If selecting VAW then how to choose a vehicle. They recommend the use of large goods vehicles (LGV), especially those capable of accelerating quickly and reaching high speed.

3.1 Attack Analysis

There are notable trends to consider in protective security operational planning.

Attack methodology key observations:

- There is normally evidence of hostile reconnaissance preceding the attack, even on the day of the attack itself;
- Almost all VAW attacks to date have involved a single vehicle;
- Most attacks involve a single attacker who conducts the attack; it is less common for multiple attackers to participate, although the attacks at London Bridge and Barcelona have involved multiple attackers;
- The attack duration is usually very short, typically lasting seconds rather than many minutes;
- Attacks nearly always begin in the public realm, in spaces with little or no security presence;
- It is common for terrorists to carry out layered, starting with a VAW attack followed by another form of attack, such as firearms or bladed weapons. When a secondary form of attack is conducted, they have to date mostly involved bladed weapons;
- Most VAW attacks involved either a car or van (70%). Of these attacks, most use legitimately acquired vehicles (owned or hired by the attacker);
- When LGVs are used they have been demonstrated to be disproportionately lethal. Despite LGVs being used in less than 30% of the 22 attacks, they have accounted for over 70% of deaths. The attack in Nice on a very crowded promenade hosting Bastille Day Celebrations resulted in at least 86 deaths and 450 injured.

It is rare for attackers to die or seriously injure themselves during the initial attack phase; in most cases they have either:

- Continued the attack until they have been incapacitated by police or overpowered by a third party;
- Left a vehicle to conduct a second attack phase e.g. bladed weapon attack or fled the scene;
- If using a vehicle it is rare for attackers to attempt to impact/crash through obstacles, such as robust looking street furniture. However, in cases where obstacles have intentionally been impacted, the attackers have used LGVs;

- It is rare for VAW attacks to take place against well protected targets with good HVM, although, as seen with the attack in Westminster, a VAW attack may target a crowded place adjacent to a well-protected site;
- There have been several cases of attacks on specific types of people, such as military/police personnel. In these situations, the target type is often more important than the location;
- Normal rules of the road do not apply to attackers if using a vehicle to access or attack an event. Terrorists have and will speed, ignore traffic signals, drive on the wrong side of the road, cross central reservations and mount footways.

3.2 Further Observations

Based on a limited number of attacks where incidents have good CCTV coverage, the following has been observed:

- People are more likely to be harmed if not alerted to imminent danger;
- Individuals with their backs to an attack are unlikely to be aware of the attack and therefore cannot take avoiding action. Conversely, those walking toward the direction of the attack are able to see and get themselves out of the path of a vehicle;
- Vehicle impacts with obstacles/street furniture can help raise people's awareness of the attack, increasing their chances of survival. The attack in Stockholm is particularly notable in this regard – the number of casualties could have been much higher had people not quickly become aware of the attack;
- Loud music (e.g. sound systems) and other distractions can decrease people's awareness of what is going on around them. There are examples of people being only a few metres from a VAW attack involving a large commercial vehicle and were unable to recognise or react quickly enough to the threat;
- The use of personal headphones and mobile phones distracts people and hinders their response to danger;
- Traffic and ambient noise of a busy streetscape can also impair situational awareness;
- The earlier that individuals are visually alerted to an incident the more time they have to react and escape, obscuration limits this capability. Conversely, obscuring the view of an attacker may influence whether an attack actually takes place as the lack of vision may cast doubts in their minds as to the success of the attack;
- It is common for people to immediately assume and report the incident as a road traffic accident rather than an attack. People may seek to assist the driver (attacker), but in doing so become involved in a second stage of an attack. In high risk areas, security personnel should approach an apparent traffic accident with caution.

4 Factors Influencing the Likelihood of an Attack

Assessing the likelihood of an attack is difficult, particularly in relation to low sophistication attacks that may be conducted by lone individuals operating independently or impulsively. However, factors that can influence likelihood include:

- The location – is it a major part of the city?
- What is the nature and profile of the event/site/public space or local area? Is it iconic?

- What is the demographic of people attending the event or area? Are there people attending who might be considered to be attractive targets (e.g. military/police personnel or other groups)?
- What is the predicted size of the crowd – is there always a crowd or only sometimes?
- What is the vulnerability of the site/event or area – is it easy, or perceived to be easy, to attack?

5 Factors Influencing the Impact of an Attack

The impact of an attack is usually quantified in terms of fatalities/casualties, economic loss, disruption of services and reputational damage. However, it is useful to consider those factors that influence the scale of fatalities/casualties as there may be mitigation options that can lessen the severity. Influencing factors include:

- Type of attack method(s) used;
- Size of crowd;
- Crowd density / dispersal of crowd;
- Formation or shape of crowd (i.e. for a VAW attack on a long snaking crowd - think march or market - is potentially much more severe than a mass gathering in a square);
- The ability of people to recognise that an attack is taking place (can they see it, can they hear it, can they be warned?);
- The ability of people to immediately move away from the attack path (do they have somewhere to run? Are they confined or constrained by barriers, locked buildings etc.?);
- The presence and effectiveness of protection measures, such as vehicle security barriers or operational mitigations;
- The police response to tackle the perpetrator(s);
- The speed of medical assistance provided to injured persons.

5.1 Simple Protection Measures

Along with the usual high visibility patrols that a BCU may put in place for a borough based event there are a number of other simple measures that event organisers or borough based officers can adopt that will increase the effectiveness of any protection around such an event. These can be implemented using the resources that you have in place. These measures include:

- Adopt a non-police led search of the venue and access control by SIA accredited personnel
- The venue owner to conduct own security checks
- Use of a guard force such as SIA security officers and stewards to manage sites and venues
- The use of volunteers and way finders in any grey spaces – control the ground
- Security Minded Communications (See section 6.3 for more details)
- Proactive use of existing, permanent CCTV
- Parking suspensions/Traffic Management Orders

- Instigation of good housekeeping measures i.e. rubbish clearance, staff ID worn, demarcation of private/public areas, culture of challenging suspicious persons/behaviour

If you require any advice about the most suitable use of these simple then please contact the CT SecCo unit.

6 VAW Mitigation

Protective security mitigations relevant to mitigating VAW attacks at borough events should include if possible and proportionate:

- Physical security measures;
- Operational & Procedural Mitigations
- Deterrence communication;
- Awareness;
- Contingency planning.

These mitigations increase the likelihood of a VAW attack being:

- **Deterred** – at the attack planning / hostile reconnaissance stage;
- **Detected** – as the attack starts, giving people time to take action; or
- **Delayed** – by the hindrance of physical security measures.

6.1 Physical Security Measures

To date, VAW attacks have mainly used cars, 4x4s/SUVs and panel vans as these are readily available and require the least amount of planning. There have been fewer attacks involving LGVs (Nice, Berlin, Jerusalem and Stockholm); these have been used against large and dense crowds.

6.1.1 Levels of Protection

Amongst the levels of protection that can be used to protect an area from vehicular attack:

- Using vehicle security barriers (VSBs);
- Using 'street furniture' and other items found in a typical streetscape that can provide a level of deterrence if arranged in a certain way. They should not be expected to provide any significant level of resistance to vehicle impact. Everyday objects found within streetscapes can provide a visual deterrent to an attacker. These include items such as traffic signals and lighting columns, post boxes and bus shelters.

6.1.2 Reducing the Risk to People behind Barriers

Barriers may not stop a vehicle instantaneously and the attack vehicle may travel a significant distance before stopping, thus still presenting a significant hazard to people. It is important to choose the right type and appropriate location of barrier to ensure that effective protection is achieved. For barriers/obstacles where the penetration distance is large, the risks can be reduced by:

- Keeping an appropriate amount of separation between barrier and crowd/personnel; and/or
- Placing the barrier in a location where the path of the attack vehicle is not aligned to the crowd – i.e. by introducing an offset between the path of the vehicle and the crowd. Greater stand-off

will also provide more time for people to identify and react to an attack and, whilst this may only be a few seconds, there is evidence from incidents that even this is beneficial.

6.2 Operational & Procedural Mitigations

Operational and procedural mitigations should include the following:

• Suspicious activity reporting, particularly in the vicinity of the site or event. Hostile reconnaissance, dry runs and erratic driving around the site/event may occur and these should be communicated and assessed quickly;

• Working with local neighbours to develop mitigations and complementary/compatible responses. This should include identifying and communicating suspicious activity, alerting partners to incidents, securing vulnerable vehicles (such as construction plant) that may be stored adjacent to a major event/site etc.;

• Controlling access to the site to authorised personnel and vehicles. Where possible vehicle movements should be scheduled to avoid peak crowds;

• Securing vehicles whilst within the secure area, making sure that vehicles are locked when not in use. Drivers should keep their keys secure and should not leave keys in vehicles whilst running errands or loading/unloading;

• Traffic accidents at vulnerable locations should initially be treated with caution as it may be the end of a VAW attack and the beginning of a second stage attack (e.g. bladed weapon). Approximately half the attacks to date have involved a second stage attack. In the confusion of the attack, people often initially assume a VAW attack is an accident and go to assist the driver;

• It is very important to warn people of an attack as quickly as possible as this will maximise the opportunity for escape. Major Events involving loud noise (concerts, ceremonies, firework displays etc.) have particular risks as the noise of an attack may be masked and the public may not be able to take evasive action (as was the case in Nice). Consider how the source of noise may be quickly inhibited and how communications to people will be made;

• To assist with early detection and communication of an attack, it is important to monitor vehicular entry points and other vulnerable areas, including approach routes. Security officers undertaking this role should be located at a vantage point, but should avoid highly vulnerable areas which may jeopardise their ability to raise the alarm;

• Command structures and lines of communication/escalation routes should be compatible with the very short timeline of an attack (attacks may be over within seconds or a few minutes). Alerting the police and people to get them out of harm's way should be a priority;

• Procedures should be written in consultation with the emergency services (e.g. firearms) to ensure their needs are accommodated.

To help reduce crowd densities and maximise 'throughput' via pedestrian and vehicle entrances / access control points it is recommended that a review of procedures and processes takes place. Core principles should where possible include:

- Separation of pedestrian and vehicle entry/access control points;
- Manage the number of access points, reducing their number to a minimum but without creating crowded choke points or having adverse impact on escape routes;

- Consider the closing of route(s) and/or the redirection of pedestrians via alternative / secure routes;
- Efficient and effective search/screening of persons/vehicles to meet anticipated throughput;
- Procedures for pre-notification pass/ticket collection and person/pass/ticket verification;
- Orientation of access points, queues and approach routes to maximise spatial and situational awareness of the public;
- Stagger exit times, maximise exit routes and de-conflict peak periods with neighbouring events/sites;
- Remove/relocate crowd generators such as taxi ranks, burger vans, street entertainers etc. to less vulnerable areas.

6.3 Deterrence Communications

Terrorists do and are encouraged to undertake hostile reconnaissance prior to an attack. The information gathered is used in three main ways:

- To assess the state of security and likelihood of detection during reconnaissance and the attack itself;
- To assess vulnerabilities and how these could be exploited to achieve the desired effects; and
- To inform the modus operandi and assess the likelihood of success. Hostiles want to succeed in their attack, they need reliable and detailed information to be assured of a positive outcome. They will be actively looking for and obtaining essential information about security measures and their effectiveness both online and on the ground. This presents an opportunity to deter them via the type and content of communications that a site, event or organisation puts out about security measures, as this is the information that they're interested in. The objective is to create uncertainty and raise doubt in their minds and as a result, generate an assessment of likely failure or an unacceptable risk of failure of their potential attack. Using existing public and internal facing communications capabilities an event can provide key messages over a range of channels that not only help deter potential attackers but also help inform, reassure and potentially recruit those coming to the event into the security effort.

6.4 Awareness

Event managers should ensure vigilance/awareness training (NaCTSO's – Act Awareness, SCaN products etc.) is provided to all supervisors and staff. The event should consider security awareness campaigns for visitors (DFT/BTP/CTPNI's - See it, Say it, Sorted – NaCTSO's - Run/Hide/Tell). Training should also include information about any additionally installed security measures and why they have been introduced (i.e. for staff/public safety and encourage staff/public to use it). An awareness campaign should be designed to alert not alarm. The event should also publicise that staff are trained and prepared to respond as this can be a deterrent to hostiles – the desired end effect, the impact of the attack, may be mitigated by good preparation by a site to minimise casualties and damage.

6.5 Contingency Planning

Contingency plans should cater for an increased threat, be exercised or, at the very least, 'table topped', and reviewed on a regular basis with key event stakeholders. Any contingency plans involving additional physical security measures should address potentially consequential impact on evacuation, ability of emergency services to respond etc.

7 Initial Response to Improvised Explosive Devices (IEDs)

7.1 What is an Improvised Explosive Device?

An IED is a 'home made' bomb. The main explosive charge in an IED may be made from Home Made Explosive (HME), they may still be as powerful as commercial or military explosives. Although an IED is 'home made', they can be highly sophisticated and very effective.

The effects of an IED can be highly destructive. It is not just the primary blast that can be lethal but debris, such as broken glass and metal in the form of secondary fragmentation, can present a hazard a considerable distance away from the seat of the explosion.

7.2 Suspicious Items

When dealing with suspicious items apply the **4 C's protocol**:-

CONFIRM whether or not the item exhibits recognisably suspicious characteristics. The HOT protocol may be used to inform your judgement:-

- **Is it HIDDEN?**
    - Has the item been deliberately concealed or is it obviously hidden from view?
- **OBVIOUSLY suspicious?**
    - Does it have wires, circuit boards, batteries, tape, liquids or putty-like substances visible?
    - Do you think the item poses an immediate threat to life?
- **TYPICAL - Is the item typical of what you would expect to find in this location?**
    - Most lost property is found in locations where people congregate. Ask if anyone has left the item

  If the item is assessed to be unattended rather than suspicious, examine further before applying lost property procedures. If H-O-T leads you to believe the item is suspicious, apply the 4Cs

CLEAR the immediate area

- Do not touch it
- Take charge and move people away to a safe distance. Even for a small item such as a briefcase move at least 100m away from the item starting from the centre and moving out
- Keep yourself and other people out of line of sight of the item. It is a broad rule, but generally if you cannot see the item then you are better protected from it
- Think about what you can hide behind. Pick something substantial and keep away from glass such as windows and skylights
- Cordon off the area

COMMUNICATE - Call 999

- Inform your event organiser
- Do not use radios within 15 metres

CONTROL access to the cordoned area

- Members of the public should not be able to approach the area until it is deemed safe
- Try and keep eyewitnesses on hand so they can tell police what they saw

8 Initial Response to Marauding Terrorist Attacks: STAY SAFE

Marauding terrorist attacks involving firearms and other weapons are rare in the UK. The 'STAY SAFE' principles tell you some simple actions to consider at an incident and the information that armed officers may need in the event of a weapons or firearm attack:

RUN

- Escape if you can
- Consider the safest options
- Is there a safe route? RUN if not HIDE
- Can you get there without exposing yourself to greater danger?
- Insist others leave with you
- Leave belongings behind

HIDE

- If you cannot RUN, HIDE
- Find cover from gunfire
- If you can see the attacker, they may be able to see you
- Cover from view does not mean you are safe, bullets go through glass, brick, wood and metal
- Find cover from gunfire e.g. substantial brickwork / heavy reinforced walls
- Be aware of your exits
- Try not to get trapped
- Be quiet, silence your phone and turn off vibrate
- Lock / barricade yourself in
- Move away from the door

TELL

Call 999 - What do the police need to know? If you cannot speak or make a noise listen to the instructions given to you by the call taker

- Location - Where are the suspects?
- Direction - Where did you last see the suspects?

- Descriptions – Describe the attacker, numbers, features, clothing, weapons etc.
- Further information – Casualties, type of injury, building information, entrances, exits, hostages etc.
- Stop other people entering the building if it is safe to do so

8.1 Armed Police Response

If you encounter armed officers responding to an incident then:

- Follow officers instructions
- Remain calm
- Can you move to a safer area?
- Avoid sudden movements that may be considered a threat
- Keep your hands in view

Please remind any officers deploying to this event, or any non-police partners that armed officers may:

- Point guns at you
- Treat you firmly
- Question you
- Be unable to distinguish you from the attacker
- Officers will evacuate you when it is safe to do so

You must STAY SAFE

- What are your plans if there were an incident?
- What are the local plans? E.g. personal emergency evacuation plan

9 Initial Response to UAVs

An unmanned aerial vehicle (UAV), often referred to as a drone, is an unmanned system that can be flown autonomously or by a remote human pilot at distance using a control system that communicates flight instructions to the drone.

It is widely accepted that most drones utilised for criminal purposes are the commercial off-the-shelf consumer types that can be easily purchased over the counter or on line and are ready to fly out the box in a matter of minutes.

Most drones of this type are supplied with an on-board camera that transmits high definition and live images back to the control unit and its connected ground control station.

Drones may be used by criminals for the following examples:

- Reconnaissance purposes for planned criminal activity
- Surveillance ranging from voyeurism through to counter surveillance techniques
- Transportation of items – into prisons/ payloads/ drugs

The intention of this guidance is to address the negligent, reckless or malicious use of UAS and to acknowledge that drones also pose a threat as the devices could easily be used by terrorists and criminal groups to carry out attacks.

9.1 Immediate Actions - DALEC

DETECT the drone, identify it and track its flight as best as possible

- What is its location, size, height, speed, payload attached, flying style (smooth/erratic/point to point/aimless/ hovering, etc.) to determine intent. Detail is paramount – take pictures if possible. Ensure to record all information from callers / witnesses try to ascertain as much detail as possible.

ASSESS the situation – identify size, location relevance and intent and decide level of risk

- If a drone appears to have the presence of an object attached/payload immediately consider the presence of an Improvised Explosive Device (IED) and CBRN implication. Whether in flight or grounded/crashed it can still present a risk to those within the direct vicinity and represents a hazard whilst it has a payload attached. Based on your initial assessment evacuate people to a safe distance and call 999.

LOCATE the pilot – consider vulnerability assessments

- Identify the launch point, its last sighting and direction of travel. Most likely to be a site with good vantage point, allowing for control of the drone. Likely be using two hands on a controller (which may be a conventional transmitter, smartphone, tablet, etc.). Their focus will be on controlling their device – they are likely to be looking toward the device and rarely changing their orientation. The pilot may be static or walking slowly. The pilot maybe wearing 'First Person View' (FPV) goggles. If so, they must be accompanied by a competent observer who is able to see the aircraft.

ENGAGE the pilot - control the situation

- What are they doing? What are they filming? Do they have permission to fly?
- Do not attempt to take control of the system.

CONSIDER further action

- Consider if waiting is an option, if the risk allows. The battery life on the UAV will range from 10 to 40 minutes and more advanced systems have a failsafe return to home function when batteries are running low.