INCIDENT UPDATE

This message contains information about an incident that has occurred within the UK or abroad. Recipients are asked to consider if action may be required in relation to the contents of this message

London Regional Counter Terrorism Protective Security Incident Update — 4th June 2017

UK TERRORISM THREAT LEVELS

INTERNATIONAL in the UK		NORTHERN IRISH RELATED in the Britain
SEVERE AN ATTACK IS HIGHLY LIKELY	For more information please see: http://www.mi5.gov.uk	SUBSTANTIAL AN ATTACK IS A STRONG POSSIBILITY

Bridge Call Summary — Incident — London Bridge, London—3rd June 2017

Detective Chief Inspector Matt Burgess, Office of the National Coordinator Protect and Prepare:

At 10.08 pm on 03 June, calls to police reported that a van had mounted the pavement travelling North to South on London Bridge and hit pedestrians. The vehicle is believed to have continued towards Borough Market. Moments later it was reported that three suspects had begun attacking people with bladed weapons in Borough Market. Armed police attended the scene and shot and killed the suspects by 10.16 pm (within eight minutes of the initial call). Police report at approximately 1.00 am on 04 June that the situation was contained, and are not currently aware of an ongoing threat.

The identities of two of the attackers are confirmed, but not yet published, and the investigation is continuing at pace. The execution of search warrants is likely. The van used in the attack remains in situ. Initial observations are that it contains bottles of flammable liquid and bags of sand.

The suspects were described as wearing suicide vests. Specialist officers have confirmed that these were not viable. Reporting at 1.30 am stated there were controlled explosions in the area, connected to the suspected Improvised Explosive Devices.

An investigation has commenced, led by the Counter Terrorism Command in London. It is focussing on identifying the suspects and any associates.

An Extraordinary Security Review Committee SRC(E) took place at 1100 am, following COBR, to review and set the protective security posture in London and across the country. There will be a heightened uniformed policing presence across London, particularly at transport hubs and other crowded places. Additional armed and unarmed police assets remain on duty.

An emergency number has been established for anyone who is concerned for loved ones who may not have returned home. Please call Casualty Bureau on 0800 0961 233.

Among those injured in the attack are a British Transport Police officer and an off-duty Metropolitan Police officer. Both remain in hospital with serious injuries but neither are believed to be in a life-threatening condition.

Cordons remain in place and we ask the public to stay away from the London Bridge and Borough Market area, SE1.

The MPS urges the public to remain calm but vigilant during this period and if you see anything suspicious, no matter how insignificant you might think it is, please contact the anti-terrorism hotline on 0800 789 321. It may be a vital piece of information.

Before closing I would Like to remind you of the National Stakeholder Menu of Tactical Options, (click HERE) in particular, increased visibility, partnership working and maintenance of CCTV.

Detective Chief Inspector Richard Harding, National Counter Terrorism Security Office:

As you have just been briefed yesterday evening a further terrorist attack was undertaken in London. The threat level remains at Severe, which means that an attack is considered highly likely; I know that you will be very aware of the implications of this situation on the security picture within the UK and for your respective businesses and sectors.

I would remind you that this threat assessment is generic and does not provide any detail as to locations or timings, and whilst it is true that an attack could occur anywhere at any time we know that there are factors that potentially make some locations more attractive or vulnerable to terrorist attack than others, particularly soft targets like crowded places as we saw with the attack last night.

Following the events in Manchester last week we provided advice to you all via bridge calls, and through updated advice and guidance on the NaCTSO Website (www.gov.uk/nactso). This advice and guidance remains valid and applicable to the current and ongoing threat situation. I would therefore recommend that you consider it in undertaking any further business or security planning that you are engaged in. In particular I would draw your attention to three areas of advice:

1) 'Guidance to improve your security stance: Click HERE
2) 'Recognising the terrorist threat': Click HERE
3) Stay Safe—Run Hide Tell: Click HERE

I would also recommend to you the advice contained within the CPNI website and in particular their advice on 'Disrupting Hostile Reconnaissance' (Click HERE); I would further recommend that you consider the advice provided by citizenAID (Click HERE) which provides effective and proven advice on how to treat injuries sustained in IED, and weapon and firearm attacks.

Given the continued relevance and applicability of the advice provided I would want to take this opportunity to remind you of it; again it is not intended to be a comprehensive review of activity but to prompt your thinking.

I would therefore recommend that you consider:

1) Encourage staff to actively monitor news and media sources to ensure they maintain situational awareness.

2) Review your security plans to ensure that they are fit for purpose and ensure that your staff, volunteers and where appropriate visitors or contractors are aware of their contents.

3) It would be easy to concentrate on last night's attack methodology; the use of a vehicle as a weapon and bladed weapons as the threat, however you should ensure that your planning and responses consider the full range of potential terrorist attack methodologies, including these and IED's (person borne, placed or vehicle) following Manchester.

4) Given the generic nature of the threat and that some location are more likely to be more attractive to terrorists and hostile threat actors, you should carefully consider the level of threat and therefore the appropriate responses at your individual sites and, where appropriate, across your portfolios. In undertaking this task you may wish to consider such factors as location, proximity to iconic or high profile crowded places, or other pertinent factors. However, given the methodology that we saw last night you may also wish to consider your operations in or in close proximity to crowded places per-se in your assessments as well.

5) You should ensure that where you decide to instigate additional security or other measures that all your staff at the relevant locations are briefed, know their roles and responsibilities, and have access to the relevant tools, equipment, corporate plans, policies and guidance.

6) You should consider how your resources and capabilities are deployed and configured to deny, detect and deter terrorists and other hostile threat actors, and thus help defeat them. To do this you would want to consider the following:

a. Ensure all your staff are briefed on the threat and what your plan, options and procedures are for responding to it should it present at or near one of your sites.
b. Use your communication channels to reassure legitimate users of your sites and to project a hostile operating environment for threat actors.
c. Proactively deploy your security resources to conduct unpredictable security activities both within and in the footprint around your sites and venues to deny terrorists a safe operating space through deterring hostile reconnaissance and detecting suspicious behaviour.
d. All staff should be encouraged to engage individuals acting suspiciously to determine what the cause is, and then to take the actions appropriate to the circumstances.
e. Ensure that all your staff are briefed on the threat and what constitutes suspicious behaviour. They will know what is normal for their regular places of work and what is not, positively encourage them to investigate or report things which feel out of place to the ordinary and have mechanisms to escalate such reporting.
f. Ensure all staff take responsibility for security, not just security personnel. They should be reminded to be vigilant, and use their customer service skills to proactively engage with customers, visitors and others.

g. Active engagement with customers, visitors and individuals at or in the vicinity of locations in the way described above is both an opportunity to help and reassure legitimate site users and, in context to detect and deter hostile threat actors.
h. Engage with your neighbours to ensure that your plans and activities are mutually supportive. In particular you may wish to ensure that any security activities are coordinated to ensure that gaps and inefficiencies are avoided. Consider how you communicate threat information between yourselves.
i. Ensure that your personnel are aware that ethnicity, religion, colour, clothing, and gender are not reliable indicators for identifying hostile threat actors or terrorists. However, such individuals are likely to display suspicious or nonbaseline behaviours when conducting threat activities. Again it is important to stress that this different behaviour may have many causes both benign and malign, and is not an indicator of terrorism. It is only through identifying, engaged and assessing why someone is behaving differently that a conclusion can be drawn.

7. Consider your action on suspicious activity and object reporting:
   a. What are your 'action on' plans if your security or staff identify a suspicious individual or objects outside or inside your premises?
   b. Are your staff aware of their options for Evacuation/ Invacuation/ Lockdown procedures, and do your plans include provision for vulnerable staff and visitors?
   c. Do your staff know where the emergency assembly points are?
   d. Have you identified any protected spaces within your venues and do staff know where they are?
   e. Are your staff lists up to date and accessible so that you can account for them in the event of an incident?

8. Search and Screening
   a. Given finite resources ensure you should consider focusing it on addressing your highest priority threats.
   b. Configure your search regime to the threat you are looking to mitigate – E.g. prioritise detection of larger threats, accepting smaller items may not be detected *If you are primarily worried about mass-casualty threats, don't look for penknives*
   c. Configure any search and screening regimes to minimise queue.

9. First Aid:
   a. Ensure your first aiders are up to date with their training and that they are appropriately deployed.
   b. Ensure that your first aid kits are stocked and staff know how to access them
   c. Consider what level of skills and equipment your first aiders require within your plans
   d. Consider the skills highlighted by citizenAID and whether they would support your organisational response plans and personnel in managing the effects of a terrorist attack.

10. Stadia and venues specific considerations. In addition stadia and venues may additionally wish to consider the following:
    a. Review event schedules and associated safety & security plans for the next 20 days and then on a rolling basis as long as the heightened alert state persists. This time period should not be taken as an indicator the anticipated duration of the heighted threat , but rather prudent planning advice.

b. Consider staged or managed dispersal through multiple exit points to minimise crowd densities at the end of an event.
c. Consider security and perimeter surveillance at of all stages of event. In particular consider how you manage the dispersal phase of an event and how. you use your personnel and security resources to continue to recognise and react to suspicious behaviour and objects.
d. Ensure activity deployed to identify and act on suspicious behaviour is maintained for the dispersal phase of an event and that known entry and exit points are considered within any plan.
e. Consider your extended footprint as part of any security and safety planning/activity
f. Consider maintaining the same perimeter control measures at the end of an event as you would at the start.
g. Ensure that the public are aware of enhanced security measures before arrival to enhance compliance and ensure that they do not bring items that would slow down any search regime you have in place.
h. Consider your ability to actively message staff and visitors within your venue to pass on instructions or information in the event of an incident or response to a threat.

In conclusion; as stated this is not intended to be a comprehensive list, and supporting guidance is on our website to complement this briefing. NaCTSO will continue to provide advice and I would recommend that if you have specific issues that you engage with your relevant force CTSA's.

Again this attack highlights the challenge of mitigating the attack methodologies used. However, there are things that can be done, and the challenge highlights the importance of creating defence in depth and organisational resilience through delivering effective layered security and response plans aligned to the threat and the needs of your businesses. This approach will allow us collectively to deny terrorists and other hostile threat actors safe operating spaces, and to have a chance of detecting and deterring them before they can act. Your organisations ability to engender vigilance, preparedness and awareness amongst your personnel will underpin the delivery of this effect which is vital to meeting this challenge.

***Spokesperson for Centre for the Protection of National Infrastructure* (*CPNI*):**

CPNI provides a range of guidance on how a site's vulnerability to vehicle borne threats can be assessed and the appropriate mitigations to such threats https://www.cpni.gov.uk/hostile-vehicle-mitigation

Links at the end of this document provide some of the relevant documents. A 150 page list of successfully tested vehicle security barriers (VSBs) is available from CPNI on request.

Extract Information:

Vehicle-borne threats range from vandalism to sophisticated or aggressive attack by determined criminals or terrorists. The payload capacity and mobility of a vehicle can offer a convenient delivery mechanism for a large explosive device, known as a vehicle borne improvised explosive device (VBIED) or a vehicle by itself can also be used with hostile intent to ram and damage infrastructure, or as a weapon to injure and kill people (Vehicle as a weapon - VAW).

There are five main methods of deploying a VBIED:

- **Parked:** A Vehicle-Borne Improvised Explosive Device (VBIED) may be parked close to a vulnerable location.
- **Encroachment:** A hostile vehicle may be able to exploit gaps in perimeter protection, or tailgate a legitimate vehicle through a single layer Vehicle Access Control Point (VACP).
- **Penetrative:** A vehicle may be used as a weapon to weaken and/or breach a building or physical perimeter. Note: The worst place for a device to detonate is inside a building structure. Blast effects reduce appreciably with distance from an asset and thus a penetrative attack can be the most impactive as it can result in a large payload device detonating inside a weakened structure.
- **Deception:** A hostile vehicle may be modified to replicate a legitimate vehicle (i.e. "Trojan" vehicle), or the occupants of a vehicle may use pretence to gain access through a VACP.
- **Duress:** A guard could be forced to grant hostile vehicle access, or a legitimate driver could be forced to take an Improvised Explosive Device (IED) within their vehicle in to a vulnerable location.

Other VBIED attack methods may employ a combination of the above (by way of a layered attack) to get a VBIED closer to a terrorist's target or may include tampering with equipment to damage or control an active barrier (eg. Retractable bollard or gate) in preparation for an encroachment attack.

Other VBIED attack methods may employ a combination of the above (by way of a layered attack) to get a VBIED closer to a terrorist's target or may include tampering with equipment to damage or control an active barrier (eg. Retractable bollard or gate) in preparation for an encroachment attack.

Vehicle Security Barriers (preferably with a maximum air gaps of 1.2m) can be:

◊ Permanent measures at fixed locations (this is the most preferable option as the measures benefit from a foundation and can then be more aesthetically pleasing above the ground). HVM can be blended in to the public realm and there are examples of how this can be done in CPNI's Integrated Security Guide for HVM;

◊ Semi-permanent (socketed/ground anchors) – measures which are deployed to specific locations for regular events and which may be removed to storage when not required. These benefit from a foundation which improves their impact resistance and pedestrian permeability;

◊ Temporary barrier systems (such as, but not limited to, the UK National Barrier Asset). Temporary barriers are modular wall, portal and gate units that can be interlinked to provide a surface mounted (gravity) or pinned solution. Some are effective if impacted, others purely act as a deterrent to drivers of hostile vehicles. Some will have residual risks and some will not lend themselves to the ground conditions or pedestrian flows of a public area hence why permanent or semi-permanent measures are preferable.

Document Links: Integrated Security vehicle-security-barriers-within-the-streetscape

tal-1-16-influence-of-bollards TAL-2-13 Bollards and Pedestrian Movement