# Event Guidance

The most vulnerable part of the UK to a terrorist attack is our crowded places, which include major events. In the wake of atrocities across Europe, event organisers need to be increasingly mindful of their security arrangements.

Terrorism can be **prevented**. Use the advice below to help keep your event safe.

## The Threat

Mi5 publish a national threat level to help the public plan for appropriate levels of security. The current threat level to the UK from International terrorism is **SEVERE**. Further information on the threat level to the UK can be found at: https://www.gov.uk/terrorism-national-emergency

| | |
|---|---|
| Critical | **An attack is expected imminently** |
| Severe | **An attack is highly likely** |
| Substantial | **An attack is a strong possibility** |
| Moderate | **An attack is possible, but not likely** |
| Low | **An attack is unlikely** |

| Response Level | Description | Threat Level |
|---|---|---|
| **Normal** | Routine protective security measures appropriate to the your event | **Low and Moderate** |
| **Heightened** | Additional and sustainable protective security measures reflecting the broad nature of the threat with specific business vulnerabilities and judgements on acceptable risk | **Substantial and Severe** |
| **Exceptional** | Maximum protective security measures to meet specific threats and to minimise vulnerability and risk | **Critical** |

A terrorist attack may take one or a combination of the following forms-

**Vehicle Borne Improvised Explosive Device (IED),** either an abandoned vehicle or by using a vehicle to ram into an area either to detonate or to be used as a weapon.
**Person Borne IED,** such as the tactics used by a suicide bomber.
**Placed IED,** an abandoned bag or something disguised as rubbish.
**Marauding Firearms/Weapons Attack** similar to the tactics used in Paris, Tunisia and Mumbai.

If an attack were to occur at your event, use the METHANE mnemonic when informing your event security and the police of a major incident

| | |
|---|---|
| **M** | Major Incident declared |
| **E** | Exact Location |
| **T** | The Type of incident |
| **H** | Any Hazards |
| **A** | Available Access /Egress routes for Emergency Services |
| **N** | The Number and Type of casualties |
| **E** | The Emergency Services required and present |

## Protecting Your Event from a Vehicle used as a Weapon

There are a number of ways vehicles can be used in an attack and the exact mitigation will depend upon the nature of the site and/or event. To assess the strengths and vulnerabilities of your site or event from vehicle-borne threats you may wish to seek specialist advice and guidance from a Police Counter Terrorism Security Adviser (CTSA).

Many threats from vehicles can be mitigated by landscaping or the installation of physical measures which may be static or security controlled. These measures can be installed either on permanent or temporary basis.

At your event, consider:

- The use of large vehicles to create soft road closures into an event footprint. This is a flexible solution, to deploy, and can be redeployed and moved at short notice. They can be easily moved to permit authorised vehicular and/or emergency access. Work in partnership with other agencies such as your Local Authority to identify if they can assist with large vehicles such as refuse trucks. The position of the vehicle should be considered, 90 (ninety) degrees to the direction of travel is optimal.
- The use of pedestrian barriers or Herras fencing to be deployed to act as a slowing mechanism. It will not mitigate a vehicle borne threats. If this is all that is available, then its use should be considered.
- Lawful positioning of machinery or street furniture such as large generators, skips, cherry pickers and forklifts at temporary events will offer limited protection and slow down a vehicle.

There are a range of more permanent Hostile Vehicle Mitigation (HVM) options to supplement the above forms of reduction/mitigation if the threat determines. These include:

- Total traffic exclusion from an area with suitable security arrangements to enforce (ATTRO – Anti Terrorism Regulation Order)

- Traffic exclusion but with screening of all vehicles entering the area (with suitable Vehicle Access Control Point (s) (VACPs)
- Traffic inclusion/free flow within an area but with all critical /vulnerable assets within that area protected with tested and approved traffic calming and barriers (HVM)
- Temporary/supplementary tested and approved barriers deployed at times of heightened threat.

Should you feel the above are necessary, you should contact a Police Counter Terrorism Security Adviser for specific advice.

## Instructions on Finding a Suspicious Package


If you find a suspicious package at your event, follow the 4 C's;

**Confirm** the package is suspicious using HOT, see illustration, Consider who should be **contacted** at your event.

(Radios/mobile phones should only be used behind hard cover and at least 15m away from the package). **Clear** the area of visitors and staff in a calm but assertive manner. **Cordon off** the area to ensure no one is able to return to the area.

Safe cordon distances are shown below, these may need to greater if your event is in open space.

100 Metres Minimum

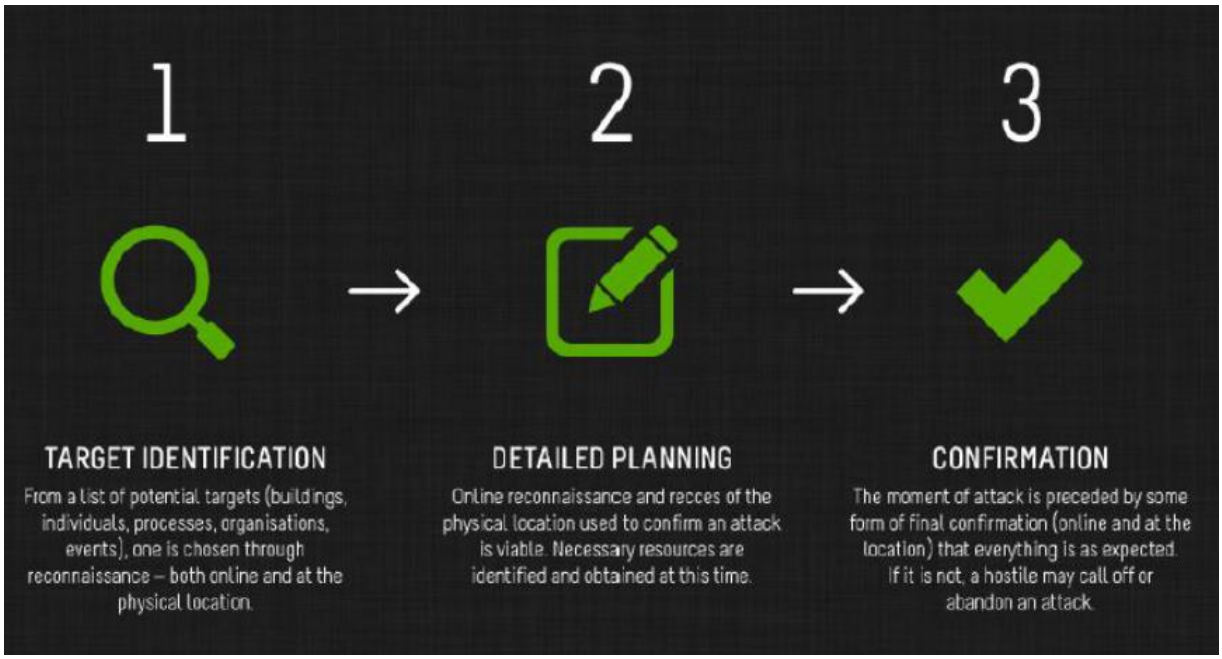
200 Metres Minimum

400 Metres Minimum

**Reporting suspicious activity to police that does not require an immediate response, contact the CONFIDENTIAL ANTI-TERRORIST HOTLINE - 0800 789 321**

## Points to consider in an Event Plan

Hostile Reconnaissance is the term given to the information gathering phase by those individuals or groups with malicious intent. Remain vigilant! Make sure your team know how to identify suspicious activity and where to report it. Benefits of being vigilant to Hostile Reconnaissance will not only reduce vulnerability to a terrorist attack but to general criminality.




Be vigilant to:

- People asking unusual questions about security arrangements
- Filming, taking notes or photographs, or watching for extended periods, focusing on security cameras, hallways, fire exits, access and egress routes.
- People behaving strangely, e.g. nervous, perspiring, wearing overly warm clothing, concealing their face
- People bringing unusual packages into your event
- People found in off limits areas, particularly near plant or server rooms or places of concealment
- Vehicles parked in suspicious circumstances

Generally, the more sophisticated the attack the more complex the attack planning, and consequently the greater the information requirement and reconnaissance needed. The information gathered is used by terrorists in three main ways, to:

- Assess the state of security and likelihood of detection during reconnaissance and the attack itself;
- Assess vulnerabilities in security and how these could be exploited to achieve the desired effects;
- Inform the modus operandi and assess likelihood of success

## Deny, Deter, Detect

Once it is understood what an attacker is looking for and why, event organisers can shape its protective security and other resources, to help disrupt hostile reconnaissance. CPNI research has shown that there are three principle ways that this can be achieved – **DENY, DETECT** and **DETER**

**DENY**

Deny the terrorist reliable information by ensuring that the information is not readily available to them when it doesn't need to be (e.g. site plan on the event website); physically, or via people who work at the site.

**DETECT**

Provide integrated, effective detection capabilities focussed in the right areas (i.e. where hostiles will have to come to obtain information) e.g. functioning well-sited CCTV and proactive control room staff.

**DETER**

By promoting DENY and DETECT capabilities to the attacker that shape their perception and assessment of likely failure both of the reconnaissance and the attack itself.

## Countering the threat: CPNI advice

Event organisers can help reduce their vulnerability to online and physical hostile reconnaissance by considering the following:

- Secure online presence – As an event, you should think about the information that is put in the public domain?
- Robust entry process – Are your security personnel sufficiently motivated to identify, deter or detect hostile reconnaissance?
- Hostile reconnaissance points understood
- Strong staff security awareness
- Vigilant and professional security

## Security minded communications

This short guidance note provides assistance from the Centre for the Protection of National Infrastructure (CPNI)'s in using Security-Minded Communications; how to utilise professional communications to help deter terrorist attack and wider criminality whilst simultaneously informing, reassuring and potentially recruiting the normal event goer to assist. How an organisation provides its messages and evidence of these capabilities needs to be done carefully and thoughtfully. For example, being considerate of the normal site user and their perceptions of such messages (ideally to be reassuring and informative) and critically, to convey the protective security without giving away detail that could be helpful to hostiles. For example:

*"We have airport style screening at our event and a range of secondary security measures some of which may not be visible"*

Opportunity for Security minded communication should be considered in the lead up to and during the event. The aim for this communication should be;

Discouragement; leveraging communications to relay messages so that criminals will find it difficult to target the event. Proactively communicating the effective security capabilities of the site may result in a potential attacker discounting the site.
Non-encouragement; ensuring communications do not say anything that makes the criminal think security will be a 'doddle' or that provides a criminal with knowledge of particular security measures in place.


## Weapons and Firearms Attack

## Lockdown Guidance

The Governments **RUN, HIDE, TELL** guidance explains how to keep safe during a marauding firearms or weapons attack. This guidance has been devised by analysing how people survived in recent terrorist firearms/weapons attacks.

It advises people to **RUN** away from danger if possible, if that is not an option people should aim to **HIDE** and lockdown the area around them. Find cover from gunfire; cover from view does not mean you are safe, bullets go through glass, brick, wood and metal so move away from doors. Be aware of your exits and try not to get trapped and lock / barricade yourself in. Finally if it is safe to do so, dial 999 and **TELL** the police what is going on and what you have seen.

The sooner the emergency services have a clear picture of what is occurring the sooner they will be able to intervene.

Tell the emergency services your 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.

## In Summary, prior to your event:

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 suicide IED as the threat, however you should ensure that you focus your planned response on the full range of potential terrorist attack methodologies, particularly those from vehicle as a weapon, bladed weapons and IED's (person bourne, placed or vehicle), although other methodologies should be actively considered.

4) Given the generic nature of the threat and that some location are more likely to be more attractive to 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 crowded places, or other pertinent factors. For example you might prioritise your locations in city centres, near sporting or entertainment venues and transport hubs for security uplift and activity.

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 corporate plans, policies and guidance.

6) You should consider how your resources and capabilities are deployed to deter, detect and disrupt and thus defeat hostile threat actors and terrorists:

To do this you would want to consider the following:

a. The use of your communication channels to reassure legitimate users of your sites and to project a hostile operating environment for threat actors.

b. The proactive deployment of security resources to conduct unpredictable security activities both within and in the footprint around your sites and venues to deter hostile reconnaissance and detect suspicious behaviour. They should be encouraged to engage individuals acting anomalously to determine what the cause is.

c. 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.

d. 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, deter or detect hostile threat actors.

e. 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.

f. Ensure that 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.

g. Ensure that your personnel are aware that ethnicity, religion, colour, clothing, and gender are not helpful in identifying hostile threat actors or terrorists. However such individuals are likely to display suspicious or non-baseline behaviours. 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?

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 queues

9) Stadia and venues specific considerations:

In addition stadia and venues may additionally wish to consider the following:

a. Continually review event schedules and associated safety & security plans against the changing threat picture.

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.

Full guidance is contained on the National Counter Terrorism Security Office (NaCTSO) website:

https://www.gov.uk/government/publications/recognising-the-terrorist-threat.
https://www.youtube.com/watch?v=4jxOXbpTmnk

## Contact us

Counter Terrorism Security Advisers (CTSAs) can provide support and guidance to enable you to run a safe successful event, please contact the team on: ctsa.bouverie@kent.pnn.police.uk.

For further information on anything within this guidance, please visit
**National Counter Terrorism Security Office**
www.nactso.gov.uk

**Centre for the Protection of National Infrastructure**
www.cpni.gov.uk

**June 2017**