ProtectUK

Purple Guide Chapter on Counter Terrorism - Attack Planning

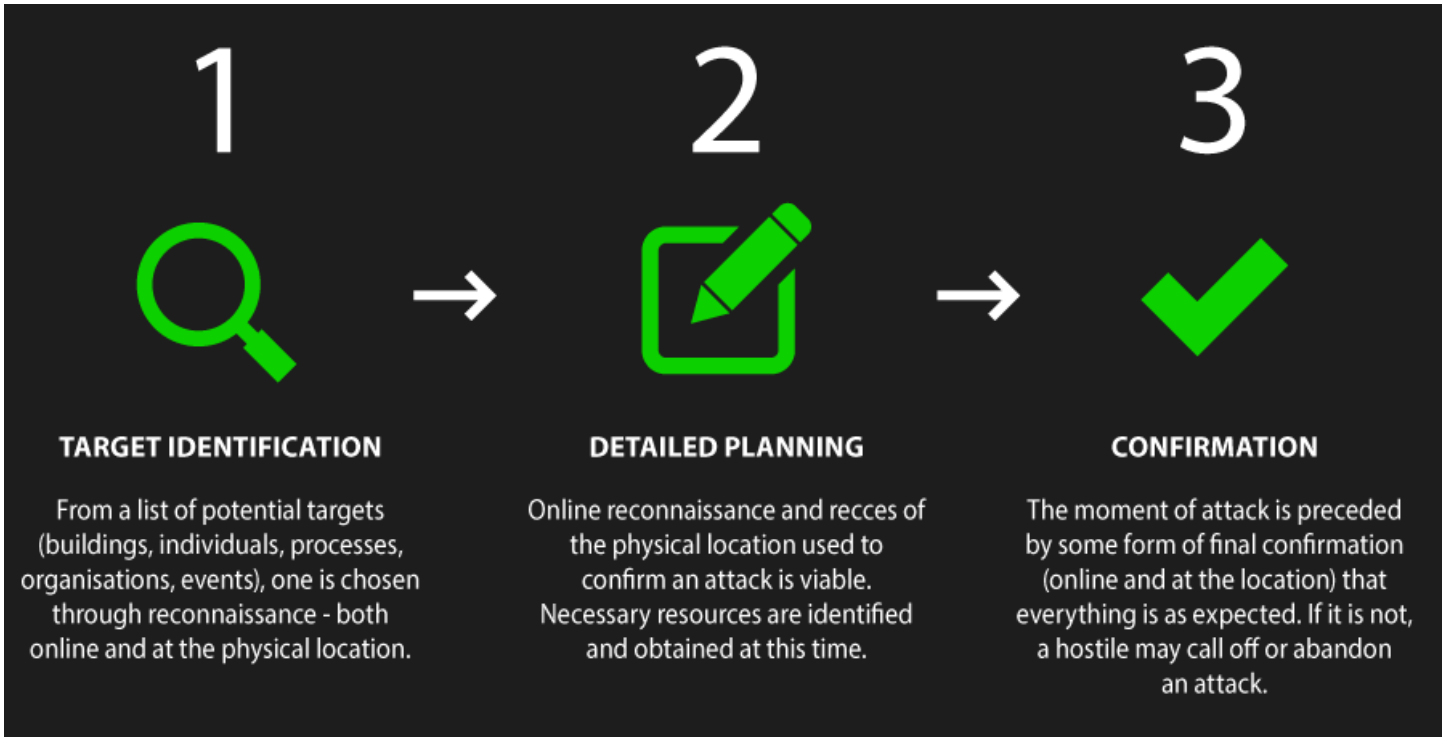
For a terrorist attack to be successful they will need to put considerable energy and resources into the planning. The planning of an attack is broken down into three distinct phases:

- Target Identification
- Detailed Planning
- Confirmation

Some of this planning can be done using online resources. However, at some point the terrorist will need to attend the scene and to complete their planning. They may seek to observe the existing security measures and assess the posture, placement and professionalism of staff to assess the viability of certain attack types. They may want to take photographs and videos of the area or event they are planning to attack.

The ACT and SCaN tools go into much more detail about this reconnaissance activity, but staff engaged at events should be mindful of the following:

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



Methods of attack

Over the years terrorists have used numerous methods to achieve their aims across the globe. When assessing the threat to an event, the risk manager must consider all the different methods of attack that could be utilised at the event as well as any intelligence available to them and any vulnerabilities presented by the event itself. Only when all these things have been considered can a plan be devised and presented to the risk holder to consider appropriate, proportionate mitigation.

The current methods of attack that should be considered are listed below. Alongside these methods of attack are links to guidance on the ProtectUK website where there is useful advice on how to deal with these threats.

- Vehicle Based Attacks
- Person Based Attacks
- Public Order
- Improvised explosive Device
- Chemical, Biological, Radiological (CBR)
- Fire as a Weapon (FAW)
- Distance Attack
- Technical

In order to fully understand current attack methodologies, it is strongly recommended that competent advice is sought.

Event organisers and planners are best place to understand the unique context of their events. By establishing the context through an effective ‘event’ and ‘crowd’ profile, the first steps in a threat and vulnerability assessment can be made.

In conducting a threat assessment, information and intelligence should be considered. Where practicable, engagement with law enforcement agencies or other security professionals is recommended. A threat assessment should be bespoke for every event. An assessment of each attack methodology, considered against likelihood, vulnerability and consequence, will assist in prioritising protective security methodology.

Staff, particularly those with experience of a venue that know what normal behaviour looks like there, should be empowered and briefed to report anything out of the ordinary. If something or someone does not look right, then something should be done.

An escalation plan is crucial when dealing with suspicious behaviour. Managers should encourage this, and the staff should be made to feel supported when it comes to reporting anything suspicious.

Improvised Explosive Devices (IED)

These devices can take many forms and can be implemented in different ways.

Instructions are readily available online that go into great detail around how to construct both the device and the explosive necessary to make it viable.

The reading of these websites and consideration of preparing these devices, is an offence and these sights are well monitored. The security services frequently disrupt such plots, however, the use of Improvised Explosive Devices is still very attractive to some terrorists. The costs both financially, physically and reputationally cannot be underestimated. Even the placing of a hoax device can cause untold disruption to an event.

See the following guidance: https://www.protectuk.police.uk/guidance

a. Placed/Delivered

b. Person Borne (Suicide Bomber)

c. Vehicle Borne IED

d. Bomb Threat

e. Suspicious Object

f. Petrol Bombs

Considerations

Event staff should be told to carry out a visual check of their area so that they are aware of what is there at the start of their shift and can verify the nature of anything found. This is also sometimes known as a white level inspection.

Stewards and staff must label their own bags and equipment so that it does not get reported as suspicious.

If the police are involved, they may carry out an in-depth search of the event. This type of search will involve highly trained officers using a range of search methods, equipment and dogs to reassure themselves that no explosives or other contraband items are present in the searched area. This provides assurance around the absence of any IED's.

Certain private sector companies are able to carry out this level of search and provide the same levels of assurance.

It is crucial, however, that if this is carried out, the area is secured to maintain the integrity of the site and ensure that nothing is delivered to site after the search concludes.

When dealing with any unattended bags or suspicious items, it is essential that the 4 C's are considered and where appropriate carried out in order.

The H-O-T principles will assist with this:

> ***Hidden?***
>
> *Has the item been deliberately hidden, or has an attempt been made to conceal it from view?*
>
> ***Obviously Suspicious?***
>
> *Can wires, circuit boards etc be seen? Was the person placing it behaving suspiciously?*
>
> ***Typical of what you would expect to find at this location?***
>
> *Is it simply lost property? Ask questions to see who the innocent owner may be.*

1. **Confirm** whether or not the item exhibits recognisably suspicious characteristics.
2. **Clear** the immediate area. Do not touch the item further. Cordon off as best you can. See recommended distances below.
3. **Communicate** - call 999 or inform the control room. Ensure you understand why you think

the item is suspicious.

4. **Control** access to the area. Do not allow members of the public to go near the item.

UNATTENDED ITEMS:
LOST... or SUSPICIOUS?



H

Hidden?

- Has it been concealed or hidden from view?
- Bombs are unlikely to be left in locations such as this – where any unattended item will be noticed quickly.



O

Obviously suspicious?

- Does it have wires, circuit boards, batteries, tape or putty-like substances?
- Do you think the item poses an immediate threat to life?



T

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.

If after applying the HOT protocols you still believe the item to be suspicious, call 999.

NaCTSO NATIONAL COUNTER TERRORISM SECURITY OFFICE

BRITISH TRANSPORT POLICE

If a suspected device is found, then a cordon must be established at various distances depending on the size of the suspected device;

- Bag/suitcase 100m minimum
- Car 200m minimum
- Large Vehicle 400m minimum

In reality, these distances may not be achievable. During the planning phase it may be worthwhile agreeing in advance some assembly points that can be achieved that are supported by risk assessment. Include these points in any briefing or documentation to duty staff.

People should be instructed to stay behind hard cover, where possible, and out of line of sight of the device.

Staff should be briefed to step away from the device before using any form of radio or telecommunications devices.

Do not evacuate the crowd past any suspicious item. If the item is close to the evacuation route then a dynamic reassessment is required.

Beware of secondary devices. If possible, a search of any muster point should occur, using dogs and trained responders.

Explosive Detection Dogs (EDDs)

The deployment of an EDD should be as part of an integrated solution to IED mitigation that considers people, processes and technology. The dog may provide an ‘indication’ this will serve as an impact factor in considering a response. The deployment of an EDD does not negate the consideration of other options.

If using a private provider of explosive detection dogs, then ensure due diligence is exercised in their selection and approval. The government now has a scheme to assist in the selection of capable providers. Guidance on this scheme can be found here.

Bomb threats

Bomb threats can be as impactive as any other incident at an event. They may take the form of direct person to person calls, but could also be transmitted by email, recordings, social media post or any other form of electronic communication. It is essential that the call taker or person receiving the message remains calm and tries to recall everything that is said. A checklist is available at Appendix

A to assist call takers with recording vital information.

Vehicle-based attacks

Vehicle-based attacks have increased significantly in recent years. This is because of the easy accessibility of vehicles and the potential results gained from using even a small vehicle to impact into a crowd of unsuspecting people. It has been highlighted and promoted as a successful method of attack by several terrorist organisations in their propaganda.

a. Hostile Vehicle Mitigation (HVM) is a term that refers to methods of deploying measures that can be used to counter the threat of a hostile vehicle attack.

b. Suicide Vehicle Born Improvised Explosive Device (SVBIED)

c. Vehicle Borne IED

d. Vehicle as a Weapon (VAAW)

It should also be borne in mind that a vehicle-based attack may only be the start of something more complex and multi-layered, such as that seen at London Bridge and Borough Market on 3rd June 2017. Disabling or slowing the vehicle may not be the end of the attack. It is crucial that your plan develops to consider the response to any attack to minimise the effects.

Hostile vehicle mitigation should be a consideration for the overall plan. The most effective HVM is complete separation of vehicles and pedestrians, however, this tends to be impossible at most events. Any plan should strive to underpin this aim.

Considerations

Seek expert advice in the provision of hostile vehicle mitigation. The expert should look to provide a holistic plan not just deploy some products.

Any HVM plan will need to carefully consider its impact on crowd movement, especially in an emergency. This emergency may not be terrorism related. If gates are used, then consideration should be given to enabling them to be opened or measures moved, if necessary to aid crowd movement.

Event staff should be made aware of the threat from hostile vehicles and briefed on what to do in the event of an attack.

Even seemingly legitimate vehicles could pose a threat on a site. For example, emergency services vehicles could be a disguised “Trojan Horse”. It is crucial to consider the management of all vehicles

moving around the site and the potential impact they can have on crowds. In the past vehicles backfiring have been known to cause stampeding and a large vehicle travelling too fast around a site can cause an unwanted reaction from a crowd.

Consider safe systems of movement by vehicles, such as insisting on hazard lights, using banksmen where appropriate, or restricting movement completely when there are crowds present. Consider also the security of vehicles by ensuring their keys are always removed secure so they are not able to be taken and used as a weapon.

Person-based attacks

a. Close Quarter Attack, (e.g. stabbing or use of a blunt force instrument)

b. Person borne IED

c. Marauding Terrorist Attack

The use of bladed weapons as a method of attack has increased over the past few years. It is undoubtedly headline grabbing and is also easy to carry out with little or no planning. This makes it hard to get any notice of an attack prior to it happening, particularly if the attacker is a lone individual and not part of a larger network.

Considerations

Regardless of the terrorism threat, knives should not be allowed into any event. It is not wise to rely purely on metal detectors as a number of non-metallic items could be used to carry out an attack and the extra assurance of a thorough search regime can have other benefits as it can be a significant deterrent to both terrorists and others who may be bringing other items into the event, such as drugs. Advertising the search in advance can be used to both manage expectations on entry as well reassurance that security is a priority.

Equally as important are the “actions on a find”. Any person carrying a knife of any sort should be considered a threat to those around them. The process for dealing with the object and the person should be in the plan.

Consider the use of behavioural detection or disruptive effects teams on the approach to your search lanes and around your event. However, do ensure that these individuals are trained and experienced. Staff, particularly those with experience of a venue that know what normal behaviour looks like there should be empowered and briefed to follow their instincts. If something or someone does not look right, then something should be done. An escalation plan is crucial when dealing with suspicious behaviour.

Encourage the use of RUN-HIDE-TELL. Staff should be briefed on this scheme. Posters are available from the links above. If staff are transient agency staff or unfamiliar with the area in which they are working, encourage them to consider their RUN – HIDE response. The Stay Safe video is available here and should be viewed by all those involved in the event.

Public order

a. Protest/Single Issue

b. Fixated Individuals

Certain events and individuals may well attract protest and activism. It is important to think widely in terms of your event and the protest it might attract. This might include event sponsors who have a protest following. If you think that this may be an issue at your event, then early engagement with the police is crucial. They will provide the necessary information and intelligence to assist you. Do not leave this until it is too late. With the diverse range of tactics available to protestors this could be the difference between a successful event and no event at all.

Equally, it is important to check with any security teams who may be protecting your artists and performers. Many artists and VIPs have fixated individuals who may carry malicious intent and whose description might need to be shared with staff.

Fixated persons can be deadly and more often are lone actors. A head of state or prominent person is more likely to be attacked by a fixated person than a terrorist. The Fixated Threat Assessment Centre (FTAC) can give guidance on individuals who may be attracted to your event by potential attendees. Access to FTAC would be through the police.

Chemical, Biological and Radiological Attacks (CBR)

The methods of initiating a CBR attack generally come under the following four headings;

a. Person Borne – brought to an area by an individual or individuals to distribute.

b. Placed – left in an area by attackers for victims to initiate or for remote initiation.

c. Delivered – sent by post or courier to an intended victim.

d. Dynamic Deployment – such as IED or drone.

Considerations

Chemical, Biological and Radiological (CBR) attacks are very rare. They do remain an aspiration for

terrorist groups, but thankfully they currently lack the capability. Following the incident in Salisbury in 2018, the profile of CBR, and the response to it, was raised in the UK. The government redrew its advice regarding the immediate actions in the event of an exposure and the Remove, Remove, Remove guidelines were drawn up - see poster below.



In the events industry it is more likely that there will be a risk of exposure to toxic industrial chemicals (TIC's). The response to the accidental exposure to these is exactly the same as to exposure to a CBR attack.

The published guidelines are pertinent to both TIC's and CBR. The guidelines can be found here.

It is essential that event staff are briefed on the response to these incidents. Any potential exposure, intentional or accidental, may well need to be considered a major incident. The ETHANE pneumonic and advice around response is covered below.

Professional advice is essential if considering CBR as a method of attack.

Fire as a Weapon (FAW)

Fire can be used as part of a layered attack. The use of fire and smoke can be a lethal mix, adding layers of confusion and panic to a crowd. It is essential that all processes and activities take the use of fire as a weapon into consideration.

A guidance document has been developed in collaboration with the Home Office, National Counter Terrorism Security Office (NaCTSO) and the National Fire Chiefs Council (NFCC). This document highlights the mitigation of the risks posed by terrorists conducting attacks that combine the use of fire with other attack methods, known as a fire as a weapon (FAW) attack.

Distance attack

a. Sniper

b. Rocket Propelled Grenade (RPG)

c. Mortar

d. Grenade

Although rarely seen in the UK the distance methods of attack should not be dismissed completely.

> *In 1991 a mortar was used to attack no 10 Downing Street.*
>
> *In 2000 an RPG was used to attack the MI6 building in London.*
>
> *In 2017 a sniper killed 60 people at a music event in Las Vegas, USA.*

Event organisers should consider that effective CT planning and a well-considered response to suspicious activity can all assist in the DETER and DETECT threads. Crowd management and evacuation procedures are key to minimising the casualties in the case of any terrorist attack.

Technical

a. Cyber

b. Communications – including radio and telephone systems.

c. Utilities – disruption to energy supply

Considerations

Most events rely heavily on the use of technical equipment that is connected to the internet in order to function successfully. This may be for the allocation of tickets, control of CCTV or even for simple things like staff rotas. It is crucial that event organisers have appropriate security in place for their technical systems. This is not just for counter terrorism but for criminals or protestors or just simple mischief.

The loss of critical systems could be catastrophic for an event and protection these needs to be considered.

Unmanned Aerial Vehicle (UAV)

a. Drone

b. Conventional Aircraft

The purple guide has a whole chapter dedicated to the use of drones at events. Familiarisation with the guidance and legislation presented in that chapter is essential to get a full understanding of the implications around these items.

Drones and UAVs are now a common site in the skies around many events. They are an integral part of the legitimate infrastructure at an event and undoubtedly add to the experience. However, the hostile use of drones should not be overlooked.

Although an attack using drones has not been seen in the UK, they remain a threat and attempts to use them as such have been interrupted by security services. As the drone's capability and usage increases, so does the threat they pose.

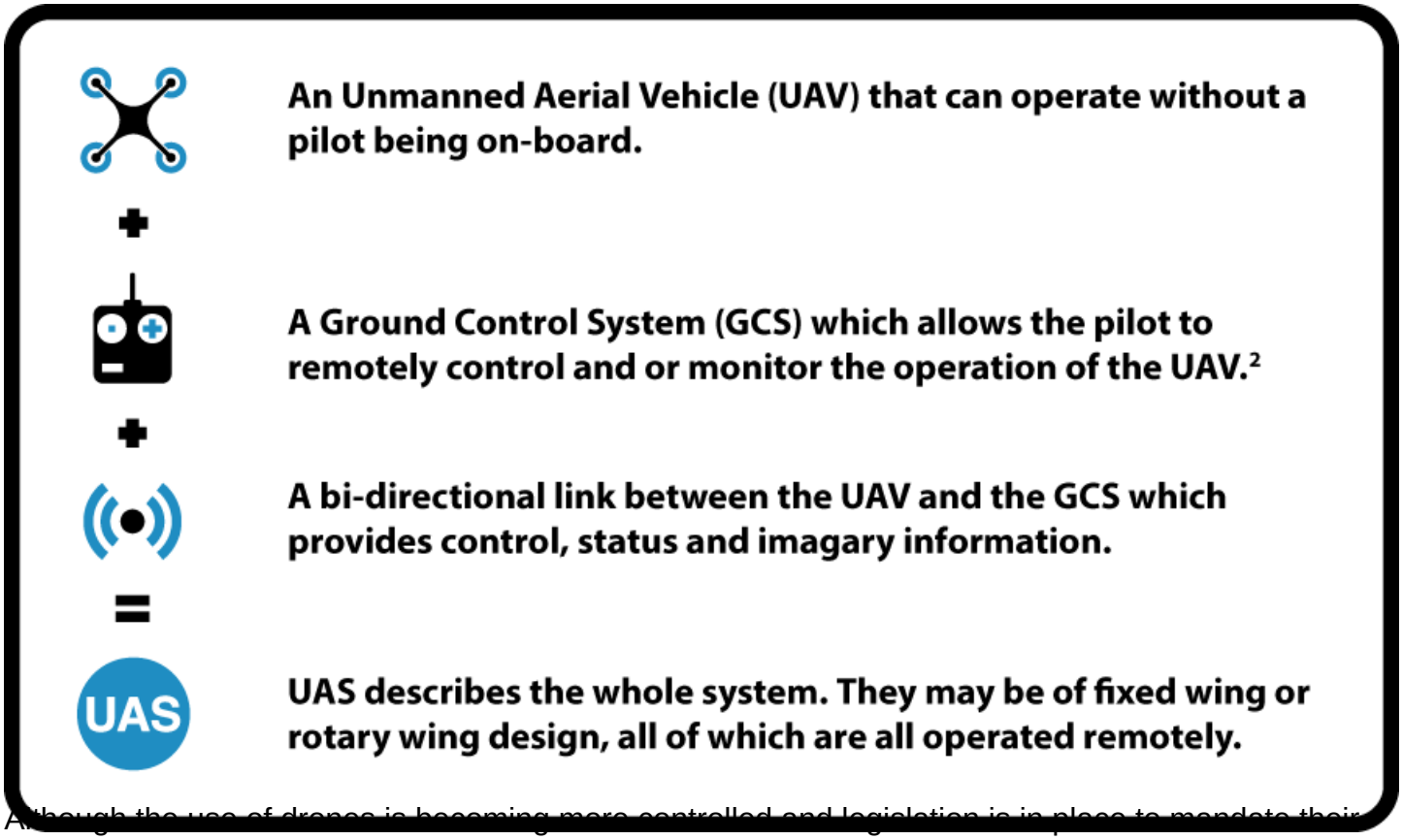
Any drones seen around an event site should be reported to the control room and a plan agreed as to how to respond. This plan should be developed with the emergency services or other experts.

Considerations

All staff should be briefed to be aware of drones, what to look for when trying to locate a drone pilot and how to engage should they suspect that someone is controlling a drone with hostile intent. The

image below illustrates the essential nomenclature of an Uncrewed Aerial System (UAS).

A plan to detect, track and identify UAS systems can be developed. Consideration should be given to vulnerable locations and times of the event. GIS and other mapping systems can be used to consider launch sites, flight paths and potential approach vectors.



Although the use of drones is becoming more controlled and legislation is in place to mandate their use, the placing of signs informing would be users of restrictions is a simple deterrent that could assist organisers.



Response

Any response plan for an event should include information around what to do in the event of a terrorist incident. The plan should draw guidance from the other chapters of the Purple Guide and be drawn up by a person experienced in such matters.

Chapter 4 – Resilience Activities for Events (Contingencies and Emergency Planning)
Chapter 13 – Crowd Management
Chapter 25 – Working in a SAG
Chapter 26 – Dealing with Crime and Disorder
Chapter 28 – Working with the Police.

NaCTSO have a guidance document and this is available here. This guidance is, however, generic and the preparation of a bespoke plan is to be encouraged, where possible.

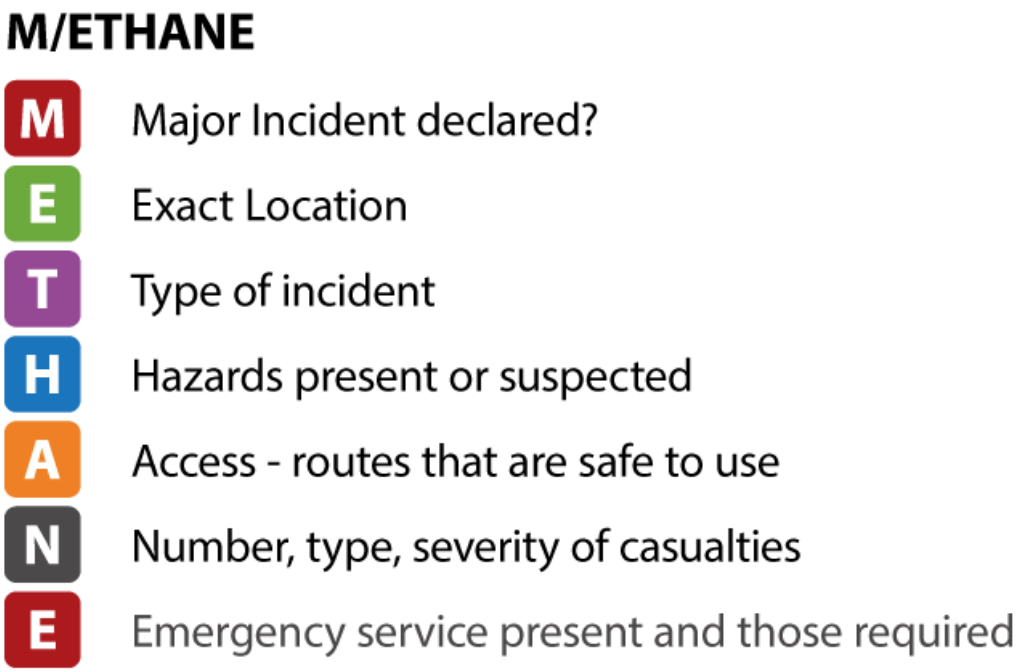
Consideration for response should include plans around:

1. Evacuation
2. Invacuation
3. Lockdown
4. Protected spaces
5. Actions on a find

Properly qualified and experienced persons should be consulted in order to prepare these plans if they are beyond the skills of those involved in the event.

Event organisers should consider the use of printed materials to be available to all staff to consider in the event of an emergency. Having posters and an aide memoire available to staff will encourage them to become familiar with what is expected of them.

As a minimum, the agreed information required by the emergency services is covered by the pneumonic (M)ETHANE and should be passed to them as soon as possible if there is an incident.



Joint Emergency Services Inoperability Principles (JESIP)

The Joint Emergency Services Interoperability Principles, or JESIP for short, were established following reviews into a number of major incidents around the UK. The findings were simply that the emergency services needed to work better together.

This resulted in JESIP and a number of doctrines were published and processes established to enable the response to an incident to be better controlled and more efficient.

Joint Decision Model

The joint decision model is a method for all of the emergency services to help bring together the available information, reconcile objectives and make effective decisions - together.



Like most decision models, the JDM centres around three primary considerations:

Situation	Direction	Action
What is happening?	What do you want/need to achieve in the first hour (the desired outcomes)?	What do you need to do to resolve the situation and achieve your desired outcomes?
What are the impacts?	What are the aims and objectives of the emergency response?	
What are the risks?	What overarching values and priorities will inform and guide this?	
What might happen and what is being done about it?		

As an event organiser it is likely that you will be expected to be present to contribute to the decisions being made. A strategic coordinating group (SCG) may be formed and the input of the event organiser is invaluable, especially if the emergency services have not been involved in the event until this point.

Briefing and training

It is absolutely essential that where a response plan has been agreed that the plan is:

A) Briefed to those expected to be carrying it out

AND

B) Practiced and rehearsed by those responsible. This can take the form of a table top exercise or a more practice-based operation.

The briefing should include everything that is expected of every member of staff in relation to the principles of Deter, Detect, Delay, Mitigate and Respond.

If necessary, staff should be invited to attend specifically for briefing and training around these issues. If the same staff are being used by companies for a whole event season, then the investment in their training at the start of the season will pay dividends throughout the year.

Management and supervisor training should also be considered separately as they will have unique requirements and should be treated differently.

Record keeping

As with all aspects of event planning it is essential that you record everything that you do, just as important, what you do not do. It is essential that every decision is rationalised at the time it is made in order that this is not forgotten about.

A “decision log” should be kept where all aspects of the planning are recorded. This could be in the form of a physical journal or log or could be in the form of command-and-control software.

A copy of the JESIP joint decision log is available at appendix A.

It is essential that these decisions are recorded as all of these decisions could be called upon in court should an incident happen and an enquiry be established. These records would be disclosable as evidence in an inquiry, criminal trial or in possible civil litigation. It is important that these are retained for a minimum of six years after the event.

APPENDIX A

Bomb Threats Checklist

A useful document to be used in control rooms for recording the details of a threat received.

Methane Document

A document to be completed to assist with the management of the initial stages of a major incident.

Remove, Remove, Remove poster

A poster to display to highlight the actions to take in response to a suspected exposure to a CBR incident.

H.O.T poster

A poster to display explaining the principles to assist with confirming a suspicious item.

Joint Decision Log

A log to be completed when recording decisions that affect how an event is run and the protective measures around it.