Responding to Terrorist Incidents

DEVELOPING EFFECTIVE COMMAND AND CONTROL

Edition 4, March 2023

National Protective Security Authority

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by the National Protective Security Authority (NPSA). The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, NPSA accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

© Crown Copyright 2023

Edition 4
March 2023

National Protective Security Authority

Home Office

NaCTSO NATIONAL COUNTER TERRORISM SECURITY OFFICE

This document has been developed in collaboration with the Home Office and National Counter Terrorism Security Office (NaCTSO).

Executive Summary

This guidance provides detailed information that those responsible for Security Control Rooms (SCR) should consider introducing. Sites are unlikely to provide an effective response to a terrorist incident unless:

- Control rooms are provided with the appropriate equipment, policies and procedures.
- Operators are given:
  - The necessary training and
  - Time to practice and exercise the response.

The National Protective Security Authority's (NPSA) research has shown that SCR operators struggle to complete tasks when working under pressure, become unclear on what tasks need to be prioritised, and whose responsibility each task is, resulting in duplication of effort and essential tasks being missed.

The guidance has been developed through detailed analysis of previous terrorist incidents, extensive research and development (R&D) that has included using live simulations of attacks as part of NPSA's Marauding Terrorist Attack (MTA) trials (also known as ASCEND) and surveys of existing Command and Control (C&C) capabilities at Critical National Infrastructure (CNI) sites. This R&D continues and it is envisaged that NPSA will be updating this guidance regularly.

The information contained within this guidance will provide an understanding of:

- The key features of a terrorist attack.
- The importance of prioritising the tasks undertaken by SCR operators.
- The crucial role of the SCR in responding to a terrorist attack.
- The tasks to be completed.
- The importance of communication within the SCR.
- The need for effective training and ongoing rehearsal of the key tasks.
- The detailed actions required to complete each of the priority tasks, for which additional information is included in the relevant detailed guidance.

The information is intended to help sites produce response plans that are fit for purpose and can be implemented by the SCR staff.

Whilst many of the concepts shared within the guidance have been fully developed through the NPSA Marauding Terrorist Attack trials, it is intended that the principles provided should be transferable and support the response to the majority of terrorist attacks and other serious incidents. Detailed guidance will be provided elsewhere concerning the response to several different types of terrorist attack.

Contents

1. **INTRODUCTION** 4

2. **TERRORIST ATTACKS** 7
   - 2.1 Attack types 8
   - 2.2 Terrorist attacks 8
   - 2.3 Marauding Terrorist Attacks 9
   - 2.4 Layered attack 10
   - 2.5 Final preparation 10

3. **SAVING LIVES THROUGH YOUR RESPONSE TO AN ATTACK** 12
   - 3.1 Identifying and prioritising tasks 13

4. **EFFECTIVE WORKING IN THE SECURITY CONTROL ROOM** 15
   - 4.1 Planning and preparation 16
   - 4.2 Using technology to detect the attack and inform a rapid initial assessment 19

5. **PRIORITISING TASKS** 21
   - 5.1 Critical response tasks 22
   - 5.2 Urgent response tasks 34
   - 5.3 Important response tasks 42

6. **SCR SECURITY AND YOUR SAFETY DURING AN ATTACK** 43
   - 6.1 Location and construction 44
   - 6.2 Dynamic assessment of risk to the SCR 45
   - 6.3 Evacuation of the SCR 45

7. **TESTING AND EXERCISING** 47

8. **ANNEX A: ATTACK PHASES** 49

9. **ANNEX B: SAMPLE STANDARD OPERATING PROCEDURES (SOP)** 51

1. Introduction

1. Introduction

Effective Command and Control is critical to mitigating the impact of terrorist attacks. Information is provided that is intended to enhance the capability of Security Control Room operators to respond to incidents.

This guidance document is intended to be used by those responsible for Security Control Rooms (SCR) within Critical National Infrastructure (CNI) sites, major events and crowded places. It is also likely to be of value to those working in other sites security or operational control rooms.

The information within the document consolidates and builds on the information concerning command and control contained in the NPSA Guidance document titled **Marauding Terrorist Attacks – Making your organisation ready**[1] and the associated supplementary guidance documents.

The guidance has been developed through detailed analysis of previous terrorist incidents, extensive research and development (R&D) that has included using live simulations of attacks as part of NPSA's Marauding Terrorist Attack (MTA) trials (also known as ASCEND) and surveys of existing Command and Control (C&C) capabilities at Critical National Infrastructure (CNI) sites. This R&D continues and it is envisaged that NPSA will be updating this guidance regularly.

Whilst many of the concepts shared within the guidance have been fully developed through the MTA trials, it is intended that the principles provided should be transferable and support the response to the majority of terrorist attacks and other serious incidents. Detailed guidance will be provided elsewhere concerning the response to several different types of terrorist attack.

The guidance provides detailed information that those responsible for SCRs should consider introducing. Sites are unlikely to provide an effective response to a terrorist attack unless:

- Control rooms are provided with the appropriate equipment, policies and procedures.
- Operators are given:
  - The necessary training and
  - Time to practice and exercise the response.

NPSA's research has shown that SCR operators are often unclear on what tasks need to be completed and whose responsibility each task is, resulting in duplication of effort and essential tasks.

1. https://www.npsa.gov.uk/marauding-terrorist-attacks-1

1. Introduction

The information contained within this guidance will provide an understanding of:

- The key features of a terrorist attack.
- The importance of prioritising the tasks undertaken by SCR operators.
- The crucial role of the SCR in responding to a terrorist attack.
- The tasks to be completed.
- The importance of communication within the SCR.
- The need for effective training and ongoing rehearsal of the key tasks.
- The detailed actions required to complete each of the priority tasks, for which additional information is included in the relevant detailed guidance.

The information is intended to help sites produce response plans that are fit for purpose and can be implemented by the SCR staff.

The information provided within this document is intended to prepare those operating within the SCR for the surge in demand and the immense pressure that they are likely to face in the event of a terrorist incident or suspected terrorist incident taking place. It is important to understand that planning and preparation for all SCRs should be based on these moments of heightened activity. NPSA recommends that three or more control room operators should deployed into an SCR.

This guidance is focused on the moment in time when an attack is discovered and the immediate aftermath of an attack when the actions of the SCR operators can have a significant impact on saving lives. These phases are described as the INCIDENT RESPONSE and the INCIDENT MANAGEMENT phases.

The National Counter Terrorism Security Office (NaCTSO) describes the response phases as:

1. Incident Response
2. Incident Management
3. Crisis Management
4. Business Continuity and Resilience
5. Business Recovery.

Detailed further information is available in Annex A.

There is a wide range of additional advice and training available to help you prepare and respond in the event of a terrorist incident. This includes:

- See, Check and Notify (SCaN) a joint NPSA and National Project Servator Team training initiative that aims to help businesses and organisations maximise safety and security using existing resources. It empowers an organisation's staff to know what suspicious activity to look for and what to do when they encounter it. As an added bonus, the skills they learn will help them to provide an enhanced customer experience[2].
- NPSA's Control Room web pages and guidance, which provides detailed information in relation to planning, preparing and managing your control room[3].
- NACTSO web pages for guidance on First Aid appropriate for a terrorist attack, as this can save lives if done quickly and competently[4].

As training is delivered it is crucial to keep an audit of decisions made in relation to the type of training given and who has received it.

2. See Check and Notify (SCaN) | Public Website (npsa.gov.uk)
3. https://www.npsa.gov.uk/control-rooms
4. https://www.gov.uk/government/publications/first-aid-advice-during-a-terrorist-incident

2.
Terrorist Attacks

2.1 - 2.2 Terrorist attacks

2.1 Attack types

A terrorist attack can present itself in many different ways; attack methodologies are continually developing as terrorists continue to identify new opportunities to carry out attacks. This guidance is not intended to cover all incident types, but to equip SCR operators to manage a dynamic incident using MTA as an example.

In this document, **terrorist attacks** are divided into three types (discussed in more detail in sections 2.2 to 2.4). These are attacks where the attacker(s) conduct:

- **Terrorist attack –** the attacker(s) conduct the attack at a single location.
- **Marauding terrorist attack (MTA) –** the attacker(s) move through various locations intending to attack multiple people.
- **Multi-layered attack –** where a combination of attack types are combined to deliver an attack.

The principles set out within the document will cover confirmed and unconfirmed attacks. Any incident that is considered by anyone dealing with it as a suspected terrorist attack should be treated as such until proved otherwise. This guidance will therefore include all incidents involving suspect packages, objects and people and bomb threats which are later proved to be hoaxes.

Attacks may include using one of, or a combination of, the following weapons as part of the attack:

- Bladed weapons
- Chemical, Biological, Radiological and Nuclear (CBRN)
- Improvised Explosive Devices (IEDs) – including suicide vests and vehicle-borne improvised explosive devices (VBIEDs)
- Fire as a Weapon (FAW)
- Firearms
- Unmanned Aerial Systems (UAS)
- Vehicles used as a weapon to run people down, force entry or a vehicle-borne improvised explosive device (VBIED).

It should be remembered that while terrorist attacks are fortunately rare, they are likely to have a very high impact when they do occur.

2.2 Terrorist attacks

Attacks may involve a terrorist taking a weapon to a site and undertaking or attempting to undertake an attack.

This may include:

- Use of an IED, which may be either person or vehicle-borne, delivered by a suicide attacker, or someone intent on escaping. This could include the use of an Unmanned Aerial System (UAS) to deliver an IED or firearm to an attack site.
- Delivery and triggering of a CBRN based device.
- Taking a firearm, knife or other weapons to a location intending to undertake an attack.

2.3 Terrorist attacks

2.3 Marauding Terrorist Attacks

Terrorists enter a busy area intending to kill or injure as many people as possible. The attackers begin to seek out new victims. Most deaths occur during the initial attack, and before police arrive. The terrorists may take hostages, resulting in a long siege. Attacks may conclude with the arrest, death or escape of the terrorists. Attackers are drawn by movement and deterred by seemingly unoccupied locations, as well as by anything that may take time and effort to overcome, such as a locked door.

MTAs can take many forms and include a combination of the following:

- A lone attacker, multiple attackers or multiple groups of attackers.
- Arrival at a location on foot, in a vehicle or an attack perpetrated by insiders.
- Entering without using force or forcing entry using an explosive device, a vehicle, coercion of someone with access or a combination thereof.
- Attackers armed with bladed weapons, firearms, pipe bombs, petrol bombs, suicide vests or multiple weapons.

Bladed weapon attacks progress less rapidly than those involving firearms since attackers must be within striking distance of their victims and expend more energy on each victim.

2.4 - 2.5 Terrorist attacks

2.4 Layered attack

Layered attacks are attacks that have combined elements of both MTAs and terrorist attack types to form a layered attack.

2.5 Final preparation

Terrorists typically use a quiet location where they expect not to be disturbed in order to make final preparations, ready weapons and wait for the appropriate moment to make their final approach. Final Preparation Points (FPP) are often within or in close proximity to their chosen target, such as a toilet, a quiet area, has few people present and is not overlooked. They may be at the attack site or in the adjacent grey space. Attacks often begin or first come to notice in the grey space, areas that are not controlled by any single organisation. The grey space may be described as:

- The area outside a site and may be either a public or private space.

The grey space is discussed in more detail in section 5.2.1. Most deaths occur during the initial attack, and before police arrive.

2.5 Terrorist attacks

Icon	Description
	Firearm
	Petrol bomb or petrol tank
	Ricin or other poison
	Suicide vest or fake suicide vest
	Bladed weapon
	Improvised Explosive Device (IED)
	Vehicle as a weapon
	Vehicle of any description
N/A	Not applicable
N/K	Not known
WC	Toilets
FPP	Final Preparation Point

Date	Location	Method	Weapons used	FPP	Terrorist attack	MTA	Layered attack
March 2019	Christchurch, New Zealand	A lone and heavily armed right wing terrorist using automatic firearms attacked those attending two mosques. Travelling between sites in a car, which was subsequently found to contain two 5 litre petrol cans, intending to use them to augment the firearms attack.				✓	
June 2018	Cologne, Germany	German authorities arrested a Tunisian man, supporting international terrorism, who allegedly had successfully created ricin and was plotting to use it in an attack in Germany.		N/A	✓		
June 2017	London Bridge, UK	Three terrorists, supporting ISIL, drove a van, containing petrol bombs, into pedestrians on London Bridge before beginning to maraud. Armed with kitchen knives and wearing fake suicide vests, the attackers entered several bars and restaurants.				✓	✓
May 2017	Manchester Arena, UK	A lone ISIL terrorist entered the foyer area of Manchester Arena and detonated a homemade IED that had been placed into a backpack he was carrying. Twenty three people died, and 139 were wounded as a result of the attack.		WC	✓		
March 2017	Westminster Bridge, UK	A lone ISIL terrorist drove a car into pedestrians (VAW) on Westminster Bridge. Leaving the vehicle and running towards Parliament, he then stabbed and killed a police officer before being shot. The attack lasted 82 seconds.				✓	✓
November 2015	Paris France	Three groups of ISIL supporting terrorists conducted a three hour-long attack on central Paris using explosives and assault rifles. One group travelling by car used assault rifles to kill patrons of bars and restaurants. 2nd group attacked the Bataclan Concert Hall resulting in a siege, while the third concentrated efforts on the national stadium.				✓	✓
January 2015	Paris, France	Two international terrorists, arriving by car coerced an employee to gain entry to the office of the targeted magazine Charlie Hebdo. After shooting at responding police, the terrorists escaped by car and killed a police officer nearby.		N/K		✓	
January 2013	In-Amenas, Algeria	Al-Queda linked terrorists using firearms and IEDs hijacked vehicles to gain entry to a secure gas facility, took hostages and over four days killed 39.		On route		✓	✓
May 2010	New York, USA	A vehicle-borne improvised explosive device was left in Times Square in a Nissan SUV. The vehicle was set on fire, but the device misfired and was discovered.			✓		

3.

Saving lives through your response to an attack

3.1 Saving lives through your response to an attack

3.1 Identifying and prioritising tasks

The fast pace of a terrorist attack means it is necessary to take action immediately to save lives. Figure 1[5] sets out the tasks that NPSA recommends should be prioritised when responding to an attack and can maximise the effectiveness of the SCR response in an attempt to reduce casualties/ fatalities. These tasks should be completed as soon as possible after an attack has been discovered; this is likely to be before police arrive. The information in the **Prioritising Tasks** section provides a summary of the detailed actions involved with delivering each task. More detailed information is provided in relation to a number of the more complex tasks within this guidance.

The information set out in figure 1 and the other infographics within the document can be used within the SCR as prompt/action cards to provide a check list of key tasks that need to be completed. They can be adapted to reflect site specific tasks and printed in smaller sizes so they can be carried by security staff as pocket action cards.

Priority tasks

These tasks have been split into three groups:

- CRITICAL
- URGENT
- IMPORTANT

The focus of the SCR should be to start the CRITICAL tasks. These tasks will continue through the response to the attack, as time and resource allow the URGENT tasks should then also be started and finally, the IMPORTANT tasks.

SCR operators must be empowered and trained to act quickly and correctly to minimise the impact of a terrorist attack. Enabling all personnel with a security role to make decisions in response to a terrorist attack prevents unnecessary delays that may cost lives.

Where personnel are trained, and your organisation is confident in their ability, NPSA recommends that they are permitted to rapidly instigate response procedures avoiding a situation where a senior colleague needs to be informed and provide authorisation to act.

Several different factors will determine the ability to complete these tasks. Including, the number of operators deployed within the SCR and the type and location of the attack taking place. The fewer operators available, the fewer the tasks it will be possible to complete and the greater the need for effective prioritisation.

It is not anticipated that a SCR will be allocated staff numbers based on the volume and speed required to deliver tasks during a terrorist attack. Staff numbers are likely to be based on the day to day demand on the control room (NPSA recommends that 3 or more operators are deployed into an SCR). However, this then means that decisions must be made as to how those tasks that do need completing are prioritised.

5. This is the first of three infographics included within the document that can be printed and made available for all operators in a control room, placed on noticeboards and printed off for their use.

Figure 1: Prioritising tasks

This page can be printed and made available for all operators in a control room, placed on noticeboards and printed off for their use.

OFFICIAL

PRIORITISING TASKS

RESPONDING TO A TERRORIST ATTACK

CATEGORY	TASKS
1 CRITICAL	**Make a rapid assessment:** What is happening? ✓
	Call the police: Provide as much detail as possible. ✓
	Sound the alarm: Alert everyone to take action. ✓
	Be decisive: Should you activate security lockdown/delay systems? ✓
2 URGENT	**Alert your neighbours** ✓
	Provide updates: staff, public and police. ✓
	Track the hostiles: Keep reassessing the situation. ✓
	Give clear directions to personnel ✓
	Locate casualties: Mobilise first aid. ✓
3 IMPORTANT	**Contact your senior management** ✓
	Complete Incident log: record events, actions decisions taken. ✓

4.
Effective Working In The Security Control Room

4.1 Effective Working In The Security Control Room

In the event of an attack, SCR operators will be responsible for completing key time-critical tasks. Terrorist attacks are one of the most challenging types of incidents you and your organisation will ever face. Fortunately, they are also rare, and most people will never encounter one. This means that training and rehearsal are, in the main, the only ways for SCR operators to gain and practice the necessary skills.

This section sets out:

- The planning and preparation that should be undertaken in advance of an attack.
- The technical equipment that is available to help enable an effective response.

4.1 Planning and preparation

SCR planning should focus on the times of highest demand and pressure on staff. It is likely that if planning is focused on steady-state operations, then when a surge in activity is required to respond to a terrorist attack or another major incident, that the planning will not be effective and the actions of the SCR will have less impact on saving lives.

4.1.1 Understanding roles and responsibilities

NPSA's testing has shown that defining roles and assigning the tasks in advance will increase the likelihood operators are trained and able to complete the tasks expected of them and know exactly what their role is.

Ensure operators are provided with appropriate training to allow them to perform each role within the SCR, so creating greater resilience.

Make sure that the role of each operator position is clearly defined and that tasks to be undertaken are assigned and easily understood.

It is likely some tasks within the SCR can only be performed from specific workstations.

Analysis has shown that organisations often overestimate what each operator can accomplish. It is important to test response plans and procedures at your site to determine how roles are best defined.

Tasks should be assigned to a workstation rather than a person, with the person deployed to that workstation having the requisite skills to perform the necessary tasks.

4.1 Effective Working In The Security Control Room

The precise roles depend on the number of operators and the capabilities at your site. For example, roles for a three-person SCR might be:

- **Police liaison:** responsible for making the 999 call, updating and facilitating the police and other emergency services. It is recommended that this role is the role of the supervisor.
- **Assessor and tracker:** responsible for making the initial assessment, using security systems to track attackers and gathering more information.
- **Announcer and lockdown operator:** responsible for making announcements, and when appropriate instigating an evacuation or a lockdown and monitoring their status.

This three person model is adopted for the purposes of this guidance and should be adjusted to meet the requirements of each site.

The roles and the tasks assigned to each operator position should be defined within the site terrorist attack response plan. The actions required of each operator to implement should be set out within the Standard Operating Procedures (SOPs). Prompt or action cards, as described at 3.1, should also be used as check lists within the SCR to reinforce the key tasks within each SOP that the SCR operators should consider completing.

Some sites may have both a security control room and another control room covering safety, fire and/or operational issues. Discussions will need to be held in advance to agree who has responsibility for making critical decisions and acting on them, as there will be no time for such discussions in the event of an attack.

4.1.2 Clear leadership and teamwork

Testing has shown that the SCR is likely to function more effectively and operators work better as a team if there is no confusion about who is in charge in the SCR.

Ensure that the SCR supervisor is identified, aware of their responsibilities and provided with appropriate training.

Some SCRs will have a designated supervisor who will perform this role. A clear order of empowerment should be established so that whichever operators are on duty and present, there is always someone who will take charge.

The performance of the individuals within an SCR is likely to be enhanced if they can work closely and effectively with their colleagues in the SCR. There will be considerable benefit in building cohesive SCR teams.

Competent teams are unlikely to develop through chance. Consideration should be given to:

- The hard and soft skills required.
- Avoiding chopping and changing team members. Working together will help build teamwork.
- Rotation of roles will assist with improving motivation, increasing interest and focus and build resilience. However, it is important to recognise the skills and limitations of each individual.
- Providing leadership and skills training.
- Providing opportunities to exercise and practise their skills.
- Allowing teams to have open discussions and learn from their training, exercising and live experience.

4.1 Effective Working In The Security Control Room

4.1.3 Communicating with other SCR operators

NPSA's analysis has shown that poor quality communication between SCR operators significantly degrades the quality of the overall response. SCR operators rarely need to work so closely under such pressure and in a situation where each decision made may cost lives. Regular practice provides an opportunity to build skills and working relationships. Practice will help SCR operators to act decisively and effectively in the event of a terrorist attack.

SCR operators need to work together to complete key tasks. Sharing critical information and decisions will improve the response.

For example, one operator may be tracking the location of attackers while another is announcing the attackers' location to enable personnel to make well-informed decisions.

As the attack develops, the operators will need to share critical information between them about the attack and the actions they are taking. This may involve **occasionally pausing** all activity to make certain there is a shared understanding of the threat and the response plan; this is essential for operators to maintain situational awareness. Each operator, as they identify critical information or take significant action, should make sure the others know what is happening. Operators are likely to focus on completing their own tasks, and it is necessary to draw each other's attention to what is taking place. This may involve raising their voice or standing up to draw their colleague's attention.

4.1.4 Familiarisation with the operating area

SCR operators should NEVER assume a message containing critical information that they pass to others has been received and understood by that person. To avoid miscommunication, confirm that critical information has been received and understood.

It is important operators:

- Are Accurate, Brief and Clear (ABC)
- State what they know, not what they think they know
- Avoid using jargon as this can lead to confusion unless everyone is well trained

4.1.5 Sharing plans with the emergency services

Once complete, the plan should be shared with the emergency services. This will allow them to check that it is compatible with their own planning. Changes may then need to be made in response to their feedback. The plan should then be regularly reviewed in response to changes in: threat and risk, buildings and the surrounding area and key personnel. The updated plan should then be shared with the emergency services.

4.2 Effective Working In The Security Control Room

It is important that all SCR staff are familiar with the area they are operating in. They should be aware of and understand:

- The vulnerabilities associated with the key assets within the site that are either essential to the operations of the site or of specific organisational value. These may be physical items, data stored or transmitted in any format, personnel with specific knowledge or skills or crowded places.
- The measures in place to protect those assets.
- The operating environment that the site and surrounding area are sat within. It is essential they know and understand how the site works. This includes understanding the layout of the site, buildings within the site, the street and building names, landmarks and escape routes. Operators should be provided with time to familiarise themselves with the site.
- Plans and mapping tools should be made available that contain all the necessary information.

4.2 Using technology to detect the attack and inform a rapid initial assessment

NPSA's testing has shown that it is difficult for SCR operators to detect an attack and ascertain what is happening, resulting in a delay to a response. This can be improved through training as well as the improved configuration of technical security systems.

Identify the optimum configuration for the SCR and ensure operators are trained and practised at using the available equipment.

Coordinating the response to a terrorist attack typically requires control room systems to be configured differently to that used to support day to day business. This may include a different arrangement on a video wall. Operators should be confident operating systems in that configuration and should be trained on all systems in the SCR. Where new systems are implemented, each SCR operator should have the opportunity to be trained and practice using them as they would during a terrorist attack.

The response to attacks can be improved if operators can use the technical equipment that is available to the best effect.

As well as knowing how to operate each system, SCR operators should understand how to use systems to best effect to accomplish tasks specific to terrorist attacks.

An operator tasked with tracking attackers should understand that a gunshot detection system may offer a rapid way of locating attackers but using video monitoring systems allows individual attackers to be tracked even when they are not firing.

The systems described below have all been seen to add considerable value in the response to terrorist attacks.

4.2.1 Panic buttons and duress alarms at entry points

Panic buttons that are carried or mounted at entry points enable front-line personnel to provide an immediate alert into the SCR and, in the right circumstance put the site into lockdown. Covert duress alarms at access control points are similarly useful in the situation where someone is coerced into granting access to an attacker. Such alarms may enable front-line staff to rapidly inform the SCR staff of the attack and will allow them to trigger a response.

4.2 Effective Working In The Security Control Room

4.2.2 Video monitoring systems (CCTV)

Detecting an attack directly using video monitoring (closed-circuit television – CCTV) is difficult. Secondary indicators such as a running crowd or casualties lying on the floor are more easily spotted. Pro-active, continuous monitoring of the most vulnerable areas offers the best opportunity for rapid detection of an attack. SCR operators should know where the most vulnerable points of their building/ site/event are, and be familiar with the wider area so that they can give full and clear information to police and notify neighbours.

The coverage and display that is optimal for detecting and tracking a terrorist attack are often different from the business-as-usual design.

Comprehensive video coverage is needed to track the location of attackers, personnel, members of the public and the emergency services. Routes likely to be used by attackers should be prioritised and are likely to include:

- Entry points
- Thoroughfares
- Stairwells

A recording and immediate playback function is important when attempting to identify the attackers and the nature of their weapons, to pass to responding police officers. Supplementary discreet cameras that the attackers may not readily identify during attack planning can also be useful. See NPSA's guidance on video monitoring for more detailed information[6].

CCTV systems can be used to provide a wealth of information to support the management of an incident. This includes:

- Detection and/or verification of the attack/security issue.
- Tracking of the incident that will provide critical information regarding decision making.
- Providing further detail/information about the subjects of interest – such as the description of person/belongings/weapons, direction of travel, historic information such as what they were doing immediately before the attack, who they were with etc.

4.2.3 Attack detection systems

Technical options, such as gunshot detection systems[7] (GDS) for detecting firearms attacks and emerging technologies such as anomalous sound and video analytics, can assist in detecting, and later, tracking an attack, e.g. detecting screams during a bladed-weapon attack or detecting people lying on the floor. For NPSA-approved systems, where there is a high degree of confidence, it may be beneficial for announcements or a security response to be initiated automatically.

6. https://www.npsa.gov.uk/cctv
7. For more information, see NPSA's document **"Introduction to Gunshot Detection Systems."**

5. Prioritising tasks

5.1 Prioritising tasks

The assessment section provides a summary of the priority tasks that need to be undertaken and how they should be prioritised.

5.1 Critical response tasks

Focusing on priority tasks is likely to reduce the number of casualties.

5.1.1 A rapid assessment of an attack must be made as soon as possible.

This will inform the decision making that will, in turn, determine how terrorist attack response plans and high-level tasks should be implemented.

Consider the adoption of a decision making model that can be used to support how tasks are prioritised, decisions made and reviewed.

A decision making model is provided in **figure 2**.
This provides a continuous cycle of:

- Gathering information
- Assessing the situation
- Identifying options
- Taking action and reviewing the impact

The decision model provided below recommends that a regular review takes place of the situation and the tasks being completed. This may require the supervisor to call a brief halt to activity and confirm there is a shared understanding of the situation and that the plan being implemented remains relevant and does not require adjusting.

Figure 2: Decision making model

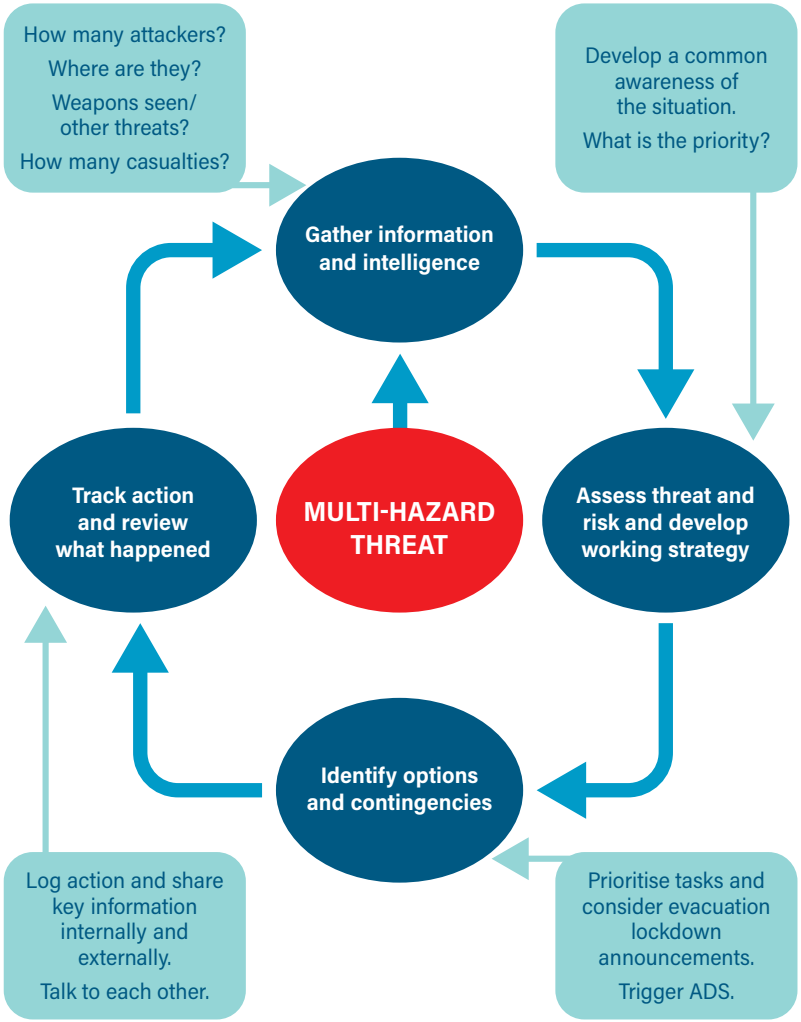
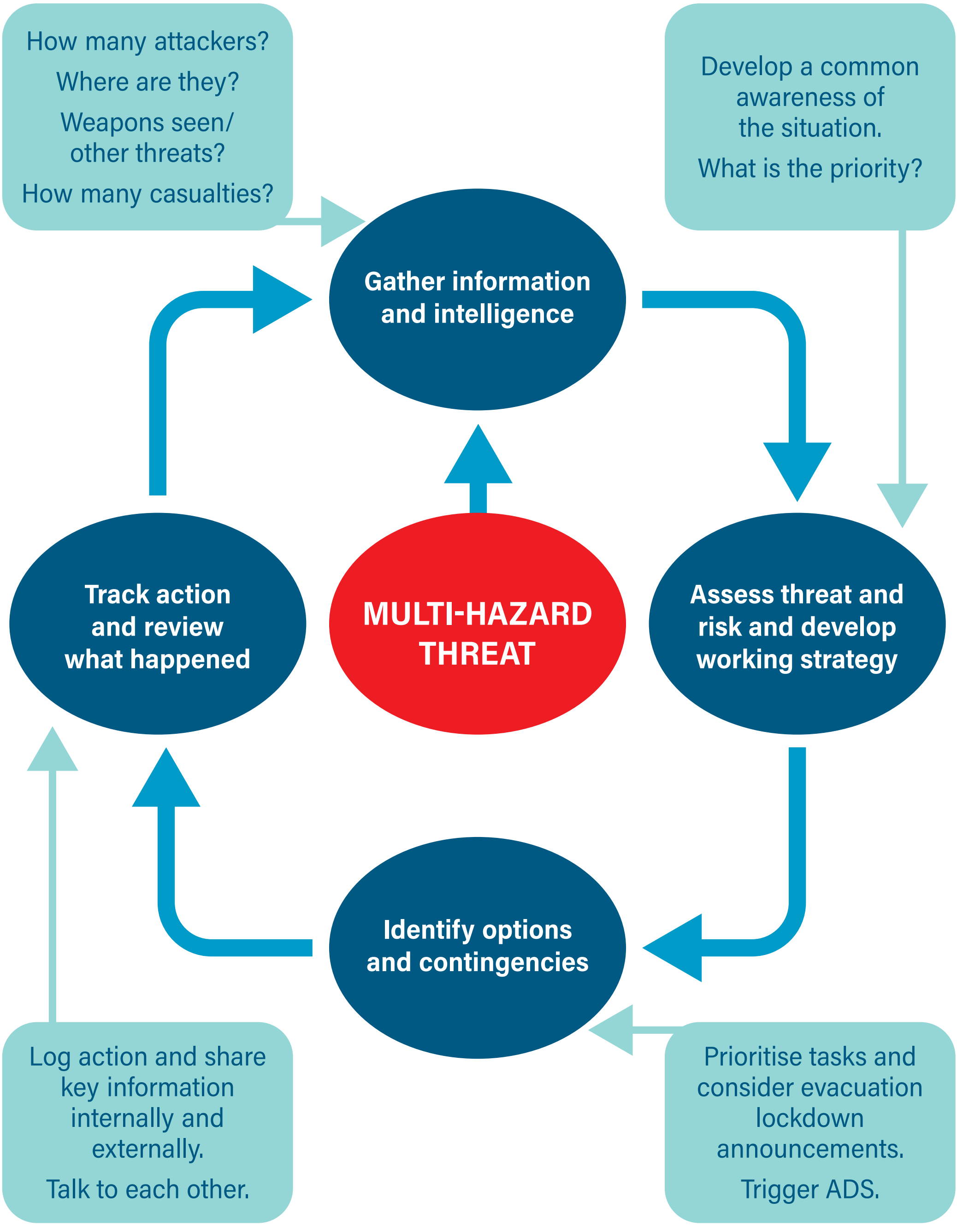


Figure 2: Decision making model

This page can be printed and made available for all operators in a control room, placed on noticeboards and printed off for their use.



5.1 Prioritising tasks

5.1.2 Calling and updating the police

NPSA's analysis has shown that 999 calls made by security personnel are often poor, with the caller being unprepared to supply the type of information required, and providing an incorrect interpretation of what was happening. There was also evidence of callers terminating the call prematurely, preventing them from providing ongoing updates.

Provide operators with training and allow them to practice making calls to the police.

The initial call to the police using the 999 emergency number is key to obtaining a police response as swiftly as possible and should be made as soon as an attack has been recognised. The ambulance and fire and rescue services need not be called separately.

Conveying the initial information is likely to take several minutes. It is important to be specific and accurate. The caller should stay on the line to keep the police updated as the attack progresses, and more information becomes available. The SCR operators need to plan accordingly as this will reduce their capacity to undertake other tasks.

The information that should be passed is summarised in **figure 3**.

Detailed guidance on calling the Emergency Services is provided in Marauding Terrorist Attacks – Supplementary Guidance: Working with police and other emergency services.

5.1 Prioritising tasks

5.1.3 Alerting personnel and members of the public to take action

The key messages of the National Counter Terrorism Policing **'Stay Safe'** Campaign are increasingly recognised by members of the public, including the principles of **'RUN HIDE TELL'**. The Stay Safe public awareness campaign sets out the three key steps to keep the public safe in the event of a firearms or weapons attack. As organisational responses are developed, consideration should be given as to how the familiar messages of RUN HIDE TELL, are developed as part of the campaign, can be incorporated. Additional information is available using the link below[8].

Personnel and members of the public must be alerted to the attack, so they know to take action.

Operators should understand the principles of RUN HIDE TELL and use this easily understood language when telling people to take action.

Detailed information is available in relation to the STAY SAFE: RUN HIDE TELL campaign from National Counter Terrorism Policing or the NPSA Guidance document titled Marauding Terrorist Attacks – Making your organisation ready

8. https://www.npcc.police.uk/NPCCBusinessAreas/WeaponAttacksStaySafe.aspx

This page can be printed and made available for all operators in a control room, placed on noticeboards and printed off for their use.

OFFICIAL

CONTACTING THE POLICE

REPORTING A TERRORIST ATTACK

CALL 999 IMMEDIATELY

- **Ask for the police. They will transfer information to fire and rescue and the ambulance services.**
- The police will pass information about any casualties and fire to the other emergency services.
- This initial call may take several minutes to make.

THE CALL IS CRUCIAL

- Tell police this is a priority call. Information passed will determine the police response.
- Use plain English. If in doubt seek clarification.
- Confirm key information is received.
- Provide information until the police deploy to the SCR.

My venue is under attack NOW.

I am _____

I am calling from _____

My Tel No. is _____

I have critical information about:-

- Numbers and descriptions of attackers
- Type and number of weapons seen – *knives, firearms, IEDs, suicide vests or petrol bombs*
- The last known location of the attackers and if you have the ability to track them
- The number of casualties

I have important Information about the venue

- Video monitoring with playback capability.
- Locking down and securing the venue.
- The location of safe rooms.
- How the Public Address Voice Announcement system can communicate to the building occupants.

Provide updates as the attack progresses

- The attackers changing location.
- More detail on descriptions and the weapons seen.
- The location and numbers of people injured.
- The status of the routes in and out of the location.

5.1 Prioritising tasks

5.1.4 Making announcements

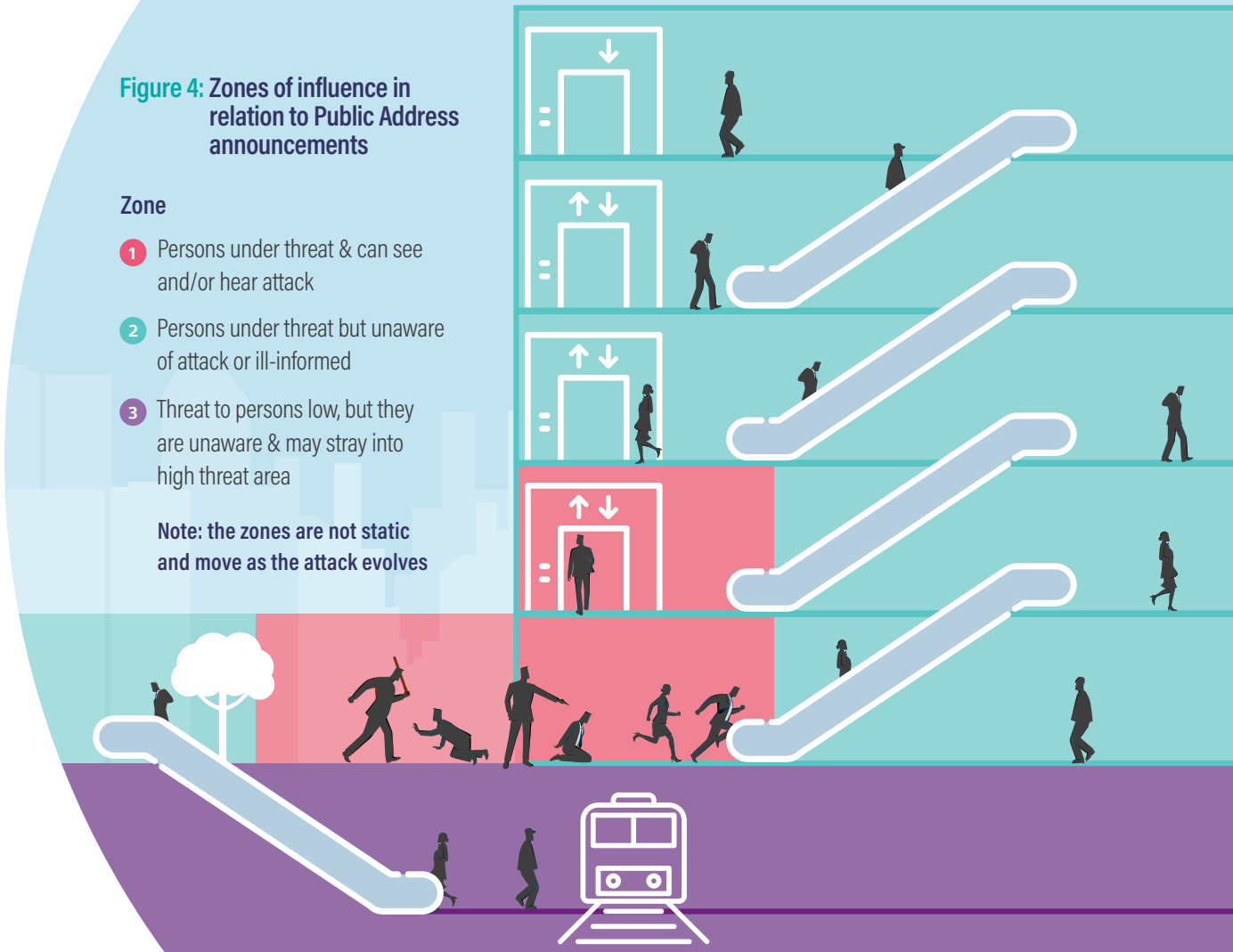
An announcement using a Public Address-Voice Announcement system (PA-VA) is the best way to warn people an attack is taking place. NPSA's research and analysis have shown that both the content and delivery of announcements are critical for people to take appropriate action. It has also shown that inexperienced and untrained SCR operators often make poor announcements that may be inaudible, rambling, vague, misleading, incorrect or lack credibility.

Training and practice will significantly improve the quality of announcements made by operators.

SCR operators should therefore practice making announcements and be familiar with the PA system. They should also practice writing down what they are going to say in advance to develop their confidence and technique. It is vital that announcements are clear, concise and confidently delivered. Announcements should be focused on fact, rather than judgement. For example, saying **"attackers at entrance 2"**, rather than **"exit via entrance 1"**.

Those in and close to the building must be given clear, concise and current information to make the right decisions to survive.

Figure 4: Zones of influence in relation to Public Address announcements



5.1 Prioritising tasks

Announcements should be aimed primarily at people who are at high and immediate risk but may not be aware of the attack, followed by those at lower and immediate risk but who may stray into a high risk area. The target audience for the announcements, therefore, is not those in the midst of the attack, but those on the periphery.

Systems that do not have an alert sound preceding the announcement are preferable so that pertinent information can be communicated as quickly as possible. Placing speakers outside a site can warn people an attack is taking place and stop them entering.

Organisations should carefully consider how they can use announcements on their site. This should be underpinned by an assessment of how announcements are likely to impact on the mass movement of people in different circumstances. See **section 5.16** on considering the impact of messages. The key considerations about making announcements for a simple office block have been summarised in **figure 5**. These may vary for a sport stadium, shopping centre or other crowded places.

Table 1: Summary of the zones of influence

Zone 1	Persons are being attacked or are close enough that they can either see or hear the attack. Communications to this group is important, but many will be distracted and their ability to act on information given impaired.
Zone 2	Persons are under imminent/approaching threat, but they are unaware of the attack or ill informed. In Figure 4, all persons within the building are under threat. Communications to this group is vital as there is a good opportunity to reduce their exposure to harm and they are likely to listen to PA-VA announcements
Zone 3	Persons in this area are not directly exposed to the threat, but may wander into the area of attack, putting themselves at risk. Communications to this group is also vital to minimise their exposure to harm.

Detailed information about announcements is provided within the Marauding Terrorist Attacks Supplementary Guidance: Announcements

Figure 5: Key considerations when making announcements for an office block. See caveat at 5.1.4

This page can be printed and made available for all operators in a control room, placed on noticeboards and printed off for their use.

OFFICIAL

MAKING ANNOUNCEMENTS

RESPONDING TO A TERRORIST ATTACK

KEY CONSIDERATIONS AS TO **WHEN TO SAY IT**.
WHAT TO SAY AND **HOW TO SAY IT** WHEN MAKING ANNOUNCEMENTS.

WHEN

- MAKE ANNOUNCEMENT AS SOON AS AN ATTACK IS DETECTED.
- IMMEDIATELY **REPEAT** KEY CONTENT.
- PROVIDE **FREQUENT** UPDATES AND NEW INFORMATION EVERY 60 SECONDS.
- OVERIDE AUTOMATED MESSAGES, WHEN APPLICABLE.
- KEEP MAKING ANNOUNCEMENTS UNTIL TOLD OTHERWISE BY THE POLICE.

HOW

- ANNOUNCE THE **SPECIFIC** LOCATION AND **GENERAL** DESCRIPTION OF ATTACKERS.
- STATE POLICE HAVE BEEN CALLED (EVEN AFTER THEY HAVE ARRIVED).
- SAY WHAT TO DO – EVACUATE IF YOU CAN, HIDE IF YOU CANNOT.
- TELL PEOPLE **SPECIFICALLY** WHERE TO AVOID – NOT WHERE TO GO.
- PROVIDE REGULAR UPDATES ON LOCKDOWN STATUS.

WHAT

- BE **CONCISE** AND **AUTHORITATIVE** – NO WAFFLE. USE EASILY UNDERSTANDABLE WORDS.
- LOCATIONS MUST BE CLEAR AND EASILY IDENTIFIABLE.
- SOUNDS CONFIDENT AND **REASSURING**.

5.1 Prioritising tasks

5.1.5 Other ways to communicate to those on a site

Announcements are very effective at alerting people that an attack is underway, but other methods of mass communication should also be considered.

Consideration should be given as to which other means of communicating with building occupants could be adopted.

It may also be necessary to use these to deliver communications during an attack if:

- There is no PAVA.
- People are working in an area with no PAVA.
- There are occupants with serious hearing impairments or there is continual loud background noise.
- There are people still entering the building during the attack.
- Others that need to know what is going on and are working from another location.

Different types of communication systems may be used, these could include:

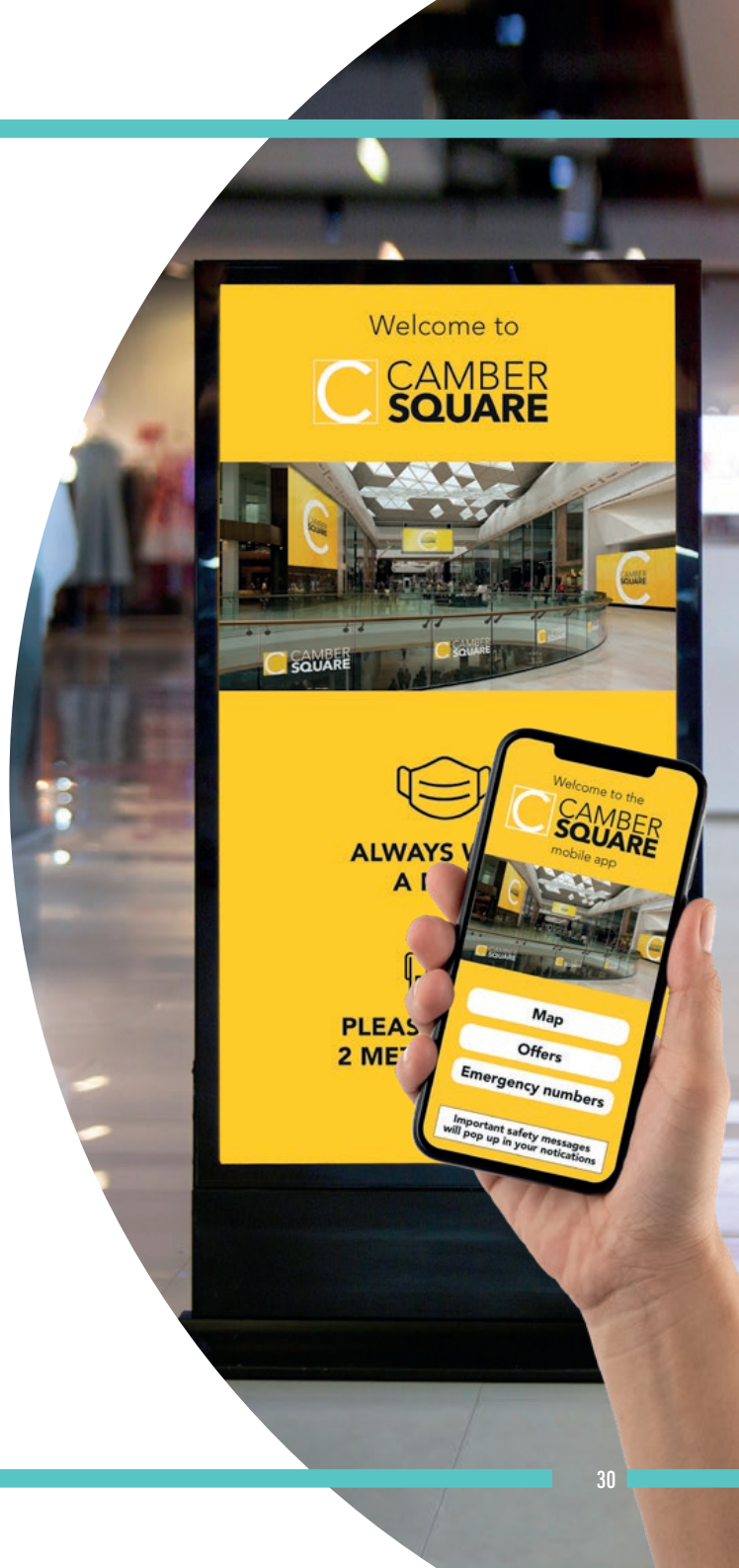
- Digital display signs
- Text message alerts
- Smartphone applications
- Visible warning lights

The use of any such warning system will likely be time consuming in the midst of an attack and may distract an operator from other tasks that are also of a high priority. Consideration should, therefore, be given as to how warnings can be drafted in advance and set up for different systems so that triggering their use becomes faster and easier.

Considering the impact of messages on crowd safety

People make decisions during an attack, based on available information. Organisations should assess the likely impact of messages relayed by PA-VA announcements or by other methods, including in-person via the guard force. The assessment should particularly look to identify and prevent circumstances that may lead to injury and the blocking of escape routes, and:

- Consider how the message is likely to impact on the mass movement of people in different circumstances.
- Identify any areas where high crowd density is likely (e.g. entrance/exit areas) and where the impact of messages may result in overcrowding and/or risk of crush.
- Consider whether occupants have been trained using fire drills and how this may impact their response to alarms and messages during an attack.



5.1 Prioritising tasks

5.1.6 Make key decisions about evacuation, invacuation or lockdown

Operators need to continue to use the decision-making model to rapidly evaluate and make decisions about the implementation of evacuation, invacuation or lockdown. Research has shown that a delay in making decisions is likely to have a detrimental effect on the number of casualties.

Evacuation

Most buildings are designed, and evacuation plans prepared, for an evacuation in the event of a fire, not a terrorist attack. Such fire evacuation plans are likely to call for building occupants to be evacuated to predetermined assembly points. In the event of a terrorist incident, those being evacuated should be instructed to disperse well away from the building. This will reduce the likelihood of a secondary attack being able to target those that have been evacuated. It may take many minutes for buildings to be evacuated with some requiring a phased evacuation to avoid crowded conditions and/or crush.

- Evacuations are more efficient with free-flowing crowd movement. Evacuation plans should consider whether the escape routes have enough capacity (i.e. are they wide enough, are there enough of them?)
- Planning should consider several different threat scenarios and the impact this might have on evacuations. For example, if several escape routes may be become unusable, will there be enough remaining capacity to evacuate the full building or will a phased evacuation be required?
- High densities reduce the speed a crowd can escape, and pose safety risks (e.g. slips, trips and falls).
- Routes should not narrow along their length, unless there are other mitigating measures in place.

Detailed training and practise are typically provided in relation to fire evacuation procedures. This often lacks information about the speed at which a fire can spread or the hazards associated with fire, smoke or the compromise of fire compartments. A basic awareness of these risks is likely to be of considerable benefit when dealing with a security incident, such as a FAW, where fire is present.

- Where occupants have been trained to respond to fire evacuations (e.g. using fire drills), they may respond this way during an attack if they hear an alarm and do not understand the situation correctly. This can lead people towards instead of away from danger.
- Advance training and the delivery of effective messaging during an attack (see section 5.1.4 on announcements and 5.2.3-7 on communications) can help to ensure they do not default to a fire evacuation response.

Planning should consider how an evacuation could take place if evacuation routes become unavailable. This may be because of structural damage caused by the incident, the location of the threat or mass casualties being located along the route.

Invacuation

If the threat involves an IED, an alternative to an evacuation may be to have a managed invacuation. This will involve moving the building occupants to a safe haven within the building. As plans are being developed consideration should be given as to the most suitable location within a site. A survey may therefore be necessary to understand how different parts of a building are likely to stand up to a blast taking place in an adjacent or nearby area.

- As when planning evacuation routes, invacuation procedures should consider whether the internal routes have enough capacity to safely move occupants all at once.
- The safe haven should have enough space to hold occupants safely.
- Stepped locations should be avoided as muster points due to the risks of holding high-density crowds on stairs.

5.1 Prioritising tasks

SCR operators must understand how lockdown works for your site:

- How would lockdown function at your site?
- In what circumstances could lockdown be instigated?
- How will the integrity of lockdown be monitored?
- Who has the authority to instigate lockdown?
- Why is it important to tell people that lockdown has been instigated?
- How to make an effective announcement about lockdown?
- What is the procedure for cancelling lockdown?
- What are the lockdown procedures for common and high-risk attack scenarios?

Lockdown can be a highly effective way of reducing casualties but is not appropriate for all sites and all forms of attack. A poorly implemented lockdown may increase the risk to personnel and members of the public.

The lockdown message should not be complicated by providing information about different types of lockdown. Such messages have been seen to cause confusion amongst personnel and members of the public.

SCR operators need to continually monitor the status of the lockdown. They need to deliver announcements every minute to reassure personnel and members of the public that the lockdown is still in place, and they should remain hidden. Alternatively, they must inform personnel and members of the public immediately if the attackers breach the lockdown. An announcement must also be made as soon as it is safe to leave the site. The decision to make this announcement will be determined by the circumstance at that time and may need to be made after dialogue with the police and the security teams at adjacent sites.

Detailed information is available in relation to lockdown in the NPSA Guidance document titled Marauding Terrorist Attacks – Supplementary Guidance: Lockdown

5.1 Prioritising tasks

5.1.7 Active Delay Systems (ADS)

ADS deployed in response to an attack are intended to save lives by:

- Preventing or delaying attackers' progress in finding and killing victims.
- Disrupting attackers by causing confusion, creating uncertainty and discomfort, and reducing confidence.
- Preventing building occupants inadvertently entering the attack zone.

ADS are divided into three types:

- Conventional Barriers - manual or automatic activation of a physical barrier.
- Vertical Transport Systems (VTS) – A change to the state of lifts or escalators within a building.
- A rapid deployment of one or more sensory effectors that inhibits the senses, coordination, concentration or communication.

The effectiveness of ADS depends on where and how they are used. These systems may also inhibit the ability of people to escape and the emergency services to respond. Consider and test whether automated or manual activation is more appropriate for your site.

Detailed information is available in relation to ADS in the NPSA guidance documents titled Marauding Terrorist Attacks – Supplementary Guidance: Active Delay Systems.

5.1.8 Knowledge of response procedures

SCR operators will be primarily responsible for making the operational decisions that implement the delivery of the priority tasks. Increasing their knowledge of response procedures will improve their ability to deliver an effective response.

SOPs should be developed that set out the detailed actions that need to be completed to deliver each of the priority tasks.

SCR operators should have a comprehensive knowledge of the relevant SOPs for the site. The SOPs will set out how the priority tasks should be delivered into the operational environment. This will enable the implementation of decisions that have been carefully thought through in advance.

5.2 Prioritising tasks

SOPs should be:

- Readily available
- Quick to understand
- Easy to follow and implement
- Regularly reviewed.

Examples are provided in Annex B of SOPS that can be tailored to each site and made available to the staff. The information within the SOPS is sensitive and should, therefore be carefully and securely handled.

Examples of SOPS are provided at Annex B

5.2 Urgent response tasks

Alerting neighbours, updating personnel and members of the public, making a detailed assessment to update police and directing front-line personnel are all urgent tasks. However, it is highly unlikely that any of these will be completed unless your site has a security control room with several operators.

5.2.1 Alerting neighbours – Grey space and sites of multiple occupancy

Many attacks are likely to be launched from and may first come to notice in the grey space. The grey space may be described as:

- The area outside a site and may be either a public or private space.

Areas outside a site may be undefended and potentially only covered by limited CCTV monitoring. It may be that no organisation has specific responsibility for the security of the area. Site security personnel are unlikely to deploy into this area. However, terrorists may have identified this area as a potential location from which to launch an attack. This may present a significant vulnerability to the safety and security of the site, its occupants and the surrounding area.

In contrast, sites of multi-occupancy may have several security regimes operating in isolation within the same site. This could mean that there is more than one SCR and security team operating within the same site. This could easily confuse the emergency services who may receive calls from more than one. Sites of multi-occupancy may be described as:

- Common areas in a multi-occupancy site, such as a large and multi-tenanted office block.

5.2 Prioritising tasks

This issue will become more complex where different security providers or facilities companies need to work together.

If possible, one site, with the agreement of neighbouring owners and operators, should take control of the grey space.

The agreement should be based on thorough discussions and a practical analysis of which site can most effectively monitor that space. This should include understanding how each site uses security measures in these areas.

Each organisation must consider the impact their actions may have on the occupants of adjacent sites and how they could work together to respond to an attack. This may include considering how an evacuation ordered at one site may impact on the flow of people already evacuating from a neighbouring site. It is important that time is spent during the planning phase comparing plans with neighbours and co-tenants to deconflict potential issues. Plans should then be jointly exercised to confirm their compatibility.

Detailed consideration will need to be given to how adjacent organisations communicate between each other and the emergency services, establishing how they can use a common radio channel or other mass communication methods, such as texting or mass communications apps.

It will be important that announcements that are made from one site to another are coordinated and compatible.

Many sites of multi-occupancy may either have multiple control rooms or a single site may have different control rooms covering different facets of a site's operation. This may include having control rooms for security, safety and transport operation. If this is the case time must be spent in planning and agreeing how tasks are split and who will have primacy for different types of issue.

There will be considerable benefit from the collocation of control rooms that cover a shared site for different organisations or different functions within the same organisation. Failing to address these issues is likely to lead to poor situational awareness, decision making and inefficient communications and deployments.

5.2 Prioritising tasks

5.2.2 Making a detailed assessment and continue to make decisions

Building an increasingly comprehensive understanding of the attack that is unfolding at any site is very important and will improve decision making. The ability of the site and the emergency services to respond will be improved as a richer picture is developed.

Configure CCTV equipment so that the system provides the necessary coverage of thoroughfares and an immediate playback facility. Train staff how to use the system in the event of an attack.

To make an effective assessment, the operator should be able to identify:

- An estimate of the number of attackers, requiring live monitoring of their movements.
- The clothes they are wearing and what they are carrying.
- Weapons (whether they have, for example, knives, pistols, long barrelled weapons or explosive vests).
- Whether attackers have split up or remain as a single group.
- An estimate of the number and location of casualties.
- An estimate of the number of people hiding in the building.

Establish the best way for the SCR to obtain still images of the attacker(s) and other attack scenes that may assist the emergency services response. How can CCTV snapshots be grabbed and saved so they can then be easily viewed by all SCR operators and shared with the police?

In the confusion of the attack, it is easy for information not to be passed between operators and then not used to best effect.

As more detailed information is gathered, it must be shared across the SCR. The information gathered must then be used to best effect. The response plan should be reviewed when significant information is received. It may be that no change is necessary or that the plan should be adjusted.

New information gathered by tracking the attackers must be:

- Shared between the operators.
- Used to review decisions about lockdown, evacuation and other actions taken.
- Passed to the police.
- Included in announcements to those on the site.

5.2 Prioritising tasks

5.2.3 Communicating with front-line personnel

When detailed and sensitive messages need to be passed between the SCR and front line staff, they should not be passed using public announcements as key detail is likely to be lost. A radio is likely to be the best method to communicate in such circumstance. Consideration should be given as to how to avoid sharing sensitive information with attackers. They may hear information passed using public announcements or being transmitted or received over the radio.

Detailed and sensitive information may most effectively be communicated to front line staff, using a radio with a hands-free kit, including an earpiece. This should mean that movement is not restricted and sensitive messages that are being received cannot be overheard. Those using radios should also be careful when transmitting messages that they do not cause unnecessary alarm to those around them or alert attackers to key information.

An assessment should be made of the numbers and type of radio equipment supplied to front line staff. All security officers are likely to require a personal issue radio and hands-free kit to facilitate communications.

Font line staff using a radio and already in the midst of the attack are unlikely to be able to listen or answer.

Consideration should be given as to how radio channels can be linked or a dedicated incident channel used to bring users together during the response to any terrorist incident.

An assessment should be made of who should be equipped with a radio. It is likely that security officers and other key front line staff will need their own radio. Sharing radios may work whilst in steady state operations but in the event of an incident this is likely to cause issues and significantly impair communications and degrade the response.

5.2 Prioritising tasks

5.2.4 Coded Messages

The use of pre-determined coded messages is well established in the crowded places environment. They provide a useful mechanism for alerting members of staff that an incident is being investigated without alarming the public. They can be used in relation to a wide variety of different incidents. This could be a medical emergency or other incident where an operational response is required.

During the initial response to a suspected terrorist incident they can be used to alert members of staff that an incident is being investigated and an assessment is being made before a full response is triggered. They can be used to instruct staff to take a preparatory and pre-planned action that will then speed up the initiation of the full response. This may include taking up emergency positions such as:

- Moving to an exit gate and being ready to unlock it to support an evacuation.
- Moving to an entrance point and being ready to lock a site down.

It is important that the meaning of the code is not shared beyond those that need to know.

Code messages can be communicated using either a radio channel or the PA-VA system. Regular updates should be provided to inform staff that the incident is either:

- Still being investigated
- Being stood down or
- A full response should be triggered.

If a full response is triggered the coded message should no longer be used and the response should be triggered using PA-VA, alarms, full radio messages or other communication system.

5.2.5 Radio protocol

NPSA's analysis has highlighted that security and front-line personnel seldom practice radio communications in the context of an emergency. People talk over one another, broadcast unnecessarily long, rambling messages blocking others on the channel and ask for updates rather than trusting that updates will be provided when available.

SCR operators and front line staff should be trained in and practice radio procedure.

People must be clear and concise when conveying information and be fluent in your organisation's radio protocol (such as saying 'over' when ending a transmission that expects a reply and 'out' when ending an exchange).

Key messages, including the conveying of vital updates or instructions should be repeated, and confirmation sought from the recipient that they have been received and acknowledged. This will reduce the likelihood that important information will not inadvertently be ignored.

Effective communication undoubtedly becomes more difficult under pressure, and this skill should be regularly practised following training.

5.2 Prioritising tasks

5.2.6 Radio system or push to talk apps

Both the available coverage and technical capability of a communications system will influence the effectiveness of the operational response.

Take a risk-based approach to ensure that there is radio coverage where it is important for your response plans, such as at entry points.

Communications may not always function between all areas of a site. However, it is important to maximise coverage as lack of coverage can have considerable consequences. It is vital that all vulnerable locations (e.g. entrances, locations where large crowds gather etc) have coverage.

Multiple different communications systems can be used to enable communications within sites. A radio system is likely to be the traditional system, but push to talk applications using smartphones are also increasingly used for communication between personnel.

Consideration should be given as to the availability of a radio interrupt facility that will allow the SCR to deliver priority messages and ensure effective command and control.

5.2.7 Training and rehearsing

Security officers and other front line staff must understand how to use the radios they are provided with. This will involve the provision of training that provides an understanding of the functionality of the equipment and the local protocols for its use. Staff should be provided with opportunities to practise making critical radio transmissions in a training environment that simulates a terrorist attack.

5.2 Prioritising tasks

5.2.8 First aid

The Manchester Arena Inquiry has recommended that to help save lives, first aid training relevant to the injuries that are most likely to occur should be undertaken. During an incident, a Security Control Room (SCR) has a crucial role in the mobilisation and support provided to those giving first aid.

It is critical to provide an expert medical intervention as quickly as possible. In the absence of such a response being immediately available first aid should be provided as soon as it is safe.

First aid should only be provided when a decision has been made that the immediate threat from the attack has diminished and it has been assessed that the scene is safe to enter. The SCR should establish that there is no immediate risk from the attackers and there are no significant risks created as a result of the attack on buildings or other infrastructure.

As the attack ends and before the emergency services can provide a significant response, there is likely to be a period during which the actions of the SCR can have a considerable impact as:

- Deploying people to give first aid, to the right location, with the right equipment will save lives.
- Gathering information about the number, nature and location of casualties and passing it to the emergency services will enable them to rapidly mobilise.

Figure 6 provides a summary of the immediate actions to take in relation to the delivery of aid.

Further guidance is available in:

NPSA guidance titled **Responding to Terrorist Incidents – Developing Effective Command and Control. Supplementary Guidance – First Aid**

The National Counter Terrorism Security Office (NaCTSO) have published a first aid awareness product which informs the considerations to providing safe and effective first aid following a terrorist incident.

Figure 6: **Is your site security control room ready to save victims of a terrorist attack?**

This page can be printed and made available for all operators in a control room, placed on noticeboards and printed off for their use.

OFFICIAL

DELIVERY OF FIRST AID AFTER TERRORIST ATTACKS

IMMEDIATE ACTIONS FOR CONSIDERATION

ACTING FAST WILL SAVE LIVES

ASSESS

THE THREAT AND HAZARDS. IS THE SCENE/SITE SAFE TO ENTER?

TELL

999

EMERGENCY SERVICES LOCATION, NUMBER AND NATURE OF CASUALTIES.

SECURE THE AREA

IF THE THREAT IS OUTSIDE OR TO PREVENT LARGE NUMBERS EVACUATING THROUGH A SCENE WHERE THERE ARE MASS AND SEVERE CASUALTIES.

First aid

1. MOBILISE FIRST AIDERS
2. DEPLOY FIRST AID KITS
3. SEARCH FOR SERIOUS CASUALTIES
4. IDENTIFY SAFE ROUTES
5. DIRECT THOSE WITH MINOR INJURIES TO MOVE

5.3 Prioritising tasks

5.3 Important response tasks

Life-saving tasks must take priority when responding to an attack. However, as soon as practicable, without disrupting other tasks, the SCR should contact senior management and make a record in a log of key events and decisions.

5.3.1 Reassurance of senior management support

People may hesitate when they are fearful of making an incorrect decision for which they fear they may be blamed. This hesitation within the context of an SCR may cost lives during a terrorist attack.

Senior managers need to approve the policies and procedures which set out the actions the SCR may take if an attack is discovered. This will allow operators to make decisions without requiring prior approval from senior managers.

Security and front-line personnel have significant responsibility in the event of an attack. Personnel should be reassured that they will have the full support of senior management when implementing procedures that have been planned and agreed.

During an attack, the SCR should be allowed to operate with a minimum level of intrusion from senior managers.

5.3.2 Recordkeeping

Recording the times of key events during an incident will create an additional burden but it will be particularly useful in enabling operators to rapidly recover CCTV footage. Doing so will enable them to quickly identify the time specific incidents came to their notice, find important information during the incident and develop a fuller picture of events as the incident develops.

Practising recordkeeping during rehearsals will improve this skill as well as providing an opportunity for personnel to reflect on areas for improvement.

In addition, an automated system (such as a video and audio recorder) can be used to record the actions operators take. NPSA strongly advocates the use of such systems, as they will assist with learning from training and exercising and support post-incident investigations. Recordings provide more accurate records, which can help defend the actions of operators and organisations.

Operators should each create a basic record of key events and decisions made as the incident develops.

During an incident creating a record may include nothing more than the time and a few words. Operators should look to log information about the following:

- What happened, and when?
- What decisions were made, why and when?
- What action was taken, and when?

This will help in confirming vital information for the emergency services about:

- The number of attackers and their descriptions.
- The type and number of weapons they are carrying.
- The number and location of casualties.

6.
SCR Security and Your Safety During an Attack

6.1 SCR Security and Your Safety During an Attack

6.1 Location and construction

The location and construction of the SCR may play an important part in a site's ability to respond to a terrorist attack. Time should be spent at an early stage in the design and planning of a site at deciding on the most appropriate location and construction of the SCR. Detailed guidance is provided concerning these issues in the NPSA guidance titled **Control Room Location**.

Detailed guidance is provided in relation to the location and construction of control rooms in the NPSA document titled "Control Room Location".

6.2 - 6.3 SCR Security and Your Safety During an Attack

6.2 Dynamic assessment of risk to the SCR

The SCR can play a significant part in saving those in and around a building that is under attack or adjacent to the attack location. However, during an incident the safety of those in the SCR is also important.

During an attack, the SCR staff should be making an ongoing dynamic risk assessment of their own safety. This should assess the circumstance of the attack, the level of protection offered by the building and their own safety.

The SCR should consider the following points:

- Remain only when it is safe to do so, but noting their actions during the attack can save lives.
- Constantly evaluate the safety of the SCR and the means of escape.
- The control room should be designed to a certain level of security – operators need to know what level of protection is provided and for how long against different threat/hazard types.
- SOPs should identify under what circumstances the SCR should be evacuated.
- The SCR may contain PPE to assist with the evacuation – such as Smoke Hoods.
- The SCR may contain other safety features, such as fire extinguishers or mats to absorb accelerants – again training in the use of these should be provided.

It is imperative to have regular training in the use of the PPE and firefighting equipment that has been provided. Time should be made available to rehearse the use of the evacuation SOPs through a series of different circumstance.

6.3 Evacuation of the SCR

It may be necessary to evacuate the SCR, for example, in the event of a fire. All operators should be aware of the available emergency escape routes and understand in what circumstance they may need to be varied. Consideration should be given as to the protection of the SCR and if this should be enhanced. This should include the level of fire protection. Plans should be made for the evacuation of the SCR, which will also set out the fallback arrangements. It is important that as the plans are developed, they are tested and then exercised on a regular basis to make sure that staff remain aware of the plan and that all the equipment in the fall back site remains operable.

If the SCR is evacuated all systems should be secured, this will ensure that attackers cannot exploit security and monitoring systems. This should be included in the operators training, and they should know the procedure to be followed. Simply locking the door to the SCR could be adequate and ensures the operators may exit swiftly.

As the SCR is evacuated, announcements should be made to the building occupants that makes them aware:

- Of the latest situation as to the location and type of threats they face.
- There won't be any more announcements.

They should follow their own instincts as to whether they should evacuate or hide. As these announcements are being made, it is important not to provide information that could be used by the attackers to identify the available evacuation routes or the approach of the police and emergency services.

6.3 SCR Security and Your Safety During an Attack

In the event of an evacuation, it is highly likely that the Command and Control functions will need to continue and therefore be transferred to another location. This could be either a fallback site at a nearby location or at a similar off-site location within the same organisation from where other operators will be able to undertake the same tasks. This will include considering if and how the different technical capabilities available within the SCR are made available within any fallback location. A SOP should be developed and exercised for the transfer of the command and control capabilities to the fallback site.

The local police force control room may have access to site CCTV via a link directly into the SCR. If this is the case, consideration should be given to allowing the police to continue to remotely monitor the cameras prior to the evacuation taking place.

The following questions will need to be considered:

- How long can the site operate without full control of the technical security capabilities?
- Which security functions must continue to operate from a fallback site?
- Is information security being fully considered within the fallback site?
- What is the most appropriate site for the fallback SCR?
- Can key systems be accessed securely from a remote location and has this been tested?
- Where necessary have the protocols been agreed with the emergency service?

7.
Testing and exercising

7. Testing and exercising

Many of the skills required to respond to a terrorist attack are different from those needed during business-as-usual. It is vital that SCR operators rehearse their role following training.

Operator performance significantly improves with practice. Rehearsals need not be disruptive and are usefully undertaken on a single system as well as using a combination of systems. For example:

- An SCR officer could practice making clear and concise announcements using a public address voice announcement system appropriate for a possible attack scenario playing out.
- A video wall could be used during busy hours to attempt to track a member of the security team taking a possible attack route through your site.
- Radio communications protocol could be rehearsed by working through a scenario with security officers and an SCR operator in different rooms.

NPSA's research has shown that SCR operators are often unclear on what tasks need to be completed and whose responsibility each task is, resulting in duplication of effort and essential tasks being forgotten.

Planning, training and rehearsal improve the response capability of the SCR.

A testing and exercising plan should be developed that sets out all testing and exercising activities and tracks ongoing activity. The plan should include the collection of learning from the testing and exercising activity and a process for deciding how policies, plans and procedures can subsequently be improved.

More detailed information about rehearsals is available in the *MTA – Supplementary Guidance – Are you ready? Testing and Exercising*

8.
Annex A: Attack phases

8. Annex A: Attack phases

The response to any terrorist incident is split into several phases.

These phases are set out within the NaCTSO Crowded Places guidance titled Managing Risk, Business Continuity and summarised in table[8]. This guidance is focused on the **Incident Response and Incident Management phases**.

Phase	Description
Business as usual (BAU)	The site is running in its steady state. No response has been initiated. ***During this phase sites are encouraged to use deterrence and security minded communications.***
Incident Response (IR)	Incident response deals with the immediate impact of an incident. It is a short phase that focuses on escalation and activation, ensuring people and the environment are supported and made safe wherever possible. ***This period will cover a sites immediate response and the attendance of the Emergency Services to resolve the incident.***
Incident Management (IM)	IM refers to how the organisation will manage the consequences of the business interruption at the scene through command, control, coordination and communication. (IM covers who is in charge, how to keep stakeholders informed, escalation processes, coordination of resources, etc.)
Crisis Management (CM)	Crisis management is about your arrangements to manage strategic, complex and unprecedented events. It is rarely standalone and will require integration with other disciplines.[9]
Business Continuity & Resilience (BC)	These are the arrangements you should develop in order to maintain critical and urgent business activities to a pre-determined level i.e. what work your business must continue to do to survive the disruption from a terrorist attack.[10]
Business Recovery (BR)	A Business Recovery Plan usually takes place over a long duration, with wider stakeholder engagement and detailing the priorities for rebuild, recovery and restoration. It should detail how and in what order you will return to the new normality following a disruption[11]

The phases will overlap; the tasks relevant to one phase are likely to be running as the tasks relevant to subsequent phases have been activated.

The nature of communication during each phase will change. During the business-as-usual (BAU) phase, there is likely to be a lower intensity of communication. This will be focused on routine activity and non-urgent activity. There is likely to be a rapid and significant increase in communication as an incident is identified, and the "incident response" phase commences.

As the attack is discovered, people will be working under immense stress, and there is likely to be considerable confusion. As a result, communications may be unclear and confused. Users may forget procedures, and may struggle to articulate themselves (e.g. stuttering, freezing and rambling). Other tasks will become more difficult to complete and users will struggle with multitasking, such as taking notes whilst speaking. However, a person's ability to respond during this phase can be improved through preparation, training and effective practice. Keeping policies and procedures simple will make them easier to follow. The use of Standard Operating Procedures (SOPs) that set out the actions that need to be taken will be of considerable benefit at moments of high pressure. SOPs can be reinforced by the use of action or prompt cards, which will provide a useful checklist of the key tasks to be completed.

During the incident management phase, the nature of the communications is likely to change. The situation will start to become under control as situational awareness increases, and response procedure are implemented. Pressure on all those delivering the response will remain high. The need for them to make decisions will continue and the demand to provide detailed information is likely to rise.

8. https://www.gov.uk/government/publications/crowded-places-guidance/managing-risk-business-continuity
9. For more information see https://www.npsa.gov.uk/crisis-management-terrorist-related-events
10. For business continuity see https://www.npsa.gov.uk/business-continuity-planning
11. For both business continuity and recovery see https://www.gov.uk/topic/public-safety-emergencies/emergencies-preparation-response-recovery

9.

Annex B: Sample Standard Operating Procedures (SOP)

An introduction to standard operating procedures to support the security control room response to terrorist attacks

9. Annex B: Sample Standard Operating Procedures (SOP)

An introduction to Standard Operating Procedures to support the Security Control Room response to terrorist attacks.

This document provides a generic example of a Standard Operating Procedure (SOP) for a Security Control Room (SCR) to be used by those responsible for the development of SOPs.

It assumes that the SCR will have three operators working at any one time. It is intended that it should be adapted to the number of operators deployed in each SCR.

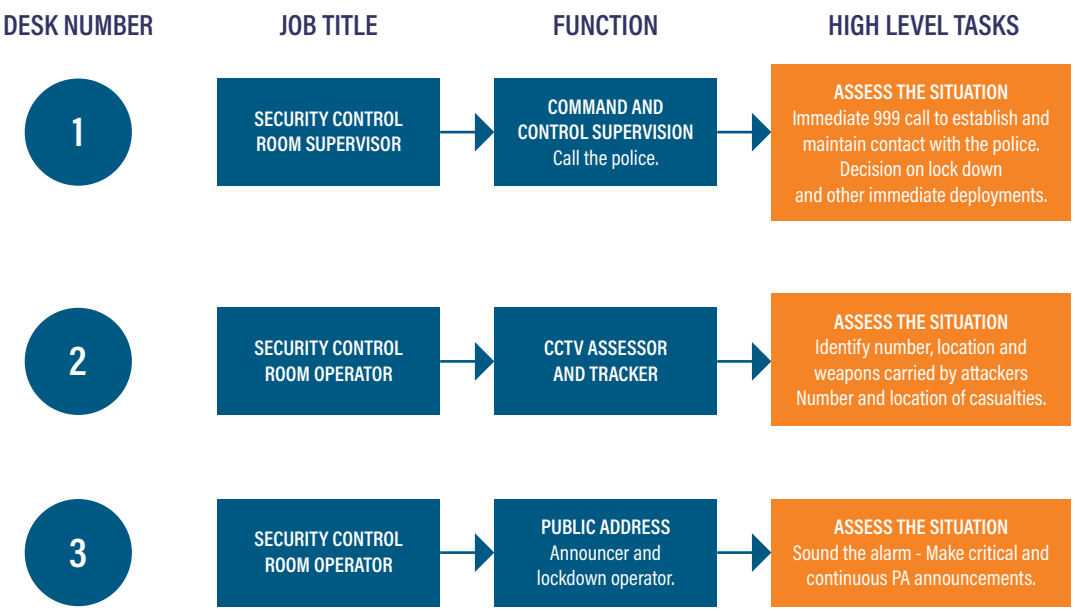
This page sets out the key roles and high-level tasks assigned to each operator. Pages 54, 55 and 56 provide examples of the detailed and specific tasks that each operator needs to complete in the event of an attack.

These SOPs are not intended to be definitive, but provide a guide that will help those responsible for developing site-specific SOPs. They should contain site-specific information.

They will contain a straightforward list of tasks that each operator should then consider completing.

It is assumed that each operator will be trained to complete each task and that the information contained within the SOPs will provide a reminder as to the tasks they need to complete.

Urgent tasks in response to a terrorist attack



9. Annex B: Sample Standard Operating Procedures (SOP)

This page can be printed and made available for all operators in a control room, placed on noticeboards and printed off for their use.

Urgent tasks in response to a terrorist attack

DESK NUMBER	JOB TITLE	FUNCTION	HIGH LEVEL TASKS
1	SECURITY CONTROL ROOM SUPERVISOR	COMMAND AND CONTROL SUPERVISION Call the police.	ASSESS THE SITUATION Immediate 999 call to establish and maintain contact with the police. Decision on lock down and other immediate deployments.
2	SECURITY CONTROL ROOM OPERATOR	CCTV ASSESSOR AND TRACKER	ASSESS THE SITUATION Identify number, location and weapons carried by attackers Number and location of casualties.
3	SECURITY CONTROL ROOM OPERATOR	PUBLIC ADDRESS Announcer and lockdown operator.	ASSESS THE SITUATION Sound the alarm - Make critical and continuous PA announcements.

9. Annex B: Sample Standard Operating Procedures (SOP)

Please fill in the fields below, print and place in suitable area.

Organisation:

.....

Security control room:

.....

In an emergency, call:

.....

Supervisor/Police Liaison

Assess the situation,
Make decision on lockdown/evacuation,
Call 999 immediately.

Report a terrorist attack is happening now

Provide the address of the site the attack is taking place

Explain you are calling from Security Control Room

Provide current and reliable information:
The number and descriptions of attackers,
The type of attack,
Weapons carried,
The location of the attackers,
The number of casualties.

The best access route to the site

Provide information about:
Video monitoring capability,
Lockdown,
Location of safe rooms,
Public address and Voice Announcements.

Provide updates as the attack progresses on:
The attackers changing location,
Detailed descriptions of attackers and weapons,
The location and numbers of people injured.

Until the incident concludes continue to:
Gather updates from SCR operators and other sources.
Reassess the situation.
Review decisions.
Inform other operators and police of key information and decisions.

Create incident log Recording:
- Key events
- Decisions made
- Attackers details
- Times of key events

Gather updates from SCR operators and other sources.

Reassess the situation.

Review decisions.

Inform other operators and police of key information and decisions.

9. Annex B: Sample Standard Operating Procedures (SOP)

Please fill in the fields below, print and place in suitable area.

Organisation:

Security control room:

In an emergency, call:

CCTV Operator

Detect an attack Assess the situation
Pro-active, continuous monitoring of the most vulnerable areas for rapid detection

Confirm an attack is taking place, using:
- Attack detection systems
- Radio reports
- Running crowds
- Casualties lying on the floor

Track and identify attackers to gather:
- Numbers
- Descriptions
- Weapons carried

Take Stills of attackers to aid identification by police

Change CCTV Configuration for MTA to cover likely routes for attackers

Continue to track movements of attackers

Identify numbers and locations of serious casualties

Until the incident concludes continue to informother SCR staff of key information

Create incident log Recording:
- Key events
- Decisions made
- Attackers details
- Times of key events

Inform other SCR staff of key information

9. Annex B: Sample Standard Operating Procedures (SOP)

Please fill in the fields below, print and place in suitable area.

Organisation:

.....

Security control room:

.....

In an emergency, call:

.....

PA Announcer

Assess the situation
Immediately commence announcements on the PAVA system

The building/location is under attack.
There is a single/multiple attackers located in/at with knives/guns.
Evacuate if you can hide if you cannot.
The police have been called.
Announce if lockdown is triggered.

Immediately repeat above message

Regularly update on lockdown situation

Deliver updated announcements every 1 minute

Announcements to be repeated – even to report no change

Continue to assess and make announcements about lockdown situation

Continue to advise police have been called.
Do not say that they have arrived.

Police may require specific announcements to be made to assist their response

Until the incident concludes continue to inform other SCR staff of key information

Create incident log Recording:
- Key events
- Decisions made
- Attackers details
- Times of key events

Inform other SCR staff of key information