MARAUDING TERRORIST ATTACKS

Making your organisation ready

CPNI
Centre for the Protection of National Infrastructure

COUNTER TERRORISM POLICING

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 CPNI. 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, CPNI 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.

Handling instructions

This guidance document is part of a series titled *"Marauding Terrorist Attacks: Making your Organisation Ready".*

It is intended to be circulated by CPNI Advisers and Counter Terrorism Security Advisers (CTSA) to key individuals within UK-based organisations.

Onward circulation is **strictly not permitted** unless authorised by the CPNI Adviser or CTSA.

Contents

INTRODUCTION

Intended audience

This document is intended for organisations in the public and private sectors. It is most useful for:

- Physical Security Managers
- Security Control Room Managers
- Security Control Room Supervisors.

It is also relevant for Chief Security Officers (CSOs) and Business Continuity Managers. The shorter companion document *“Marauding Terrorist Attacks: A busy reader’s guide to making your organisation ready”* is specifically aimed at senior managers.

Scope

Marauding Terrorist Attacks (MTAs) are fast-moving, violent attacks where assailants move through a location aiming to find and kill or injure as many people as possible. Most deaths occur within the first few minutes, before police are able to respond.

This guidance document discusses how your organisation can recognise an attack, take immediate action and facilitate the police. It is most relevant to office buildings, including multiple tenancy buildings. However, the principles of the advice may be usefully applied to all types of location including cinemas, hotels, hospitals, schools, shopping areas, shopping centres, stadiums, theatres, temporary event venues and transport hubs.

The response of the police to such attacks is detailed within national guidance (Operation Plato). That guidance refers to a wide range of attack methods, from attacks of low sophistication, such as those, using bladed weapons or vehicles, through to more complex attacks involving firearms or explosives. The emergency services’ response to an Operation Plato declaration is supported by a set of agreed principles. These Joint Operating Principles (JOPs) have been developed by the Home Office and the emergency services community in order to ensure that there is an interoperable response.

Defending your organisation against a marauding terrorist attack is undoubtedly a challenging task. A successful response cannot occur by chance. However, with well-developed procedures, security systems, training and rehearsal, lives can be saved.

This document discusses:

- Common features of marauding terrorist attacks and how people typically react
- Key actions required by security and front-line personnel to respond to an attack
- Actions that personnel and members of the public should take to respond to an attack
- Preparation and tools required to support all personnel including those with security and front-line roles
- How your organisation can continue to function and begin to recover in the aftermath of an attack
- How to manage your approach to becoming and remaining ready to face a marauding terrorist attack.

The guidance builds on the principles of ‘Run, Hide, Tell’ (published by the National Counter Terrorism Security Office, NaCTSO. See *Annexe A: STAY SAFE: Terrorist firearms and weapons attacks*).

The risk to your organisation

Organisations have a duty of care to their personnel and members of the public to give them the best chance of surviving. However, marauding terrorist attacks are fortunately rare events and the risk to organisations and individual sites varies significantly.

You must assess, manage and record the risks, even where the risk is determined to be so low that no further action is required. Records will help to ensure that the risk is adequately mitigated and that resources are being allocated appropriately. In the aftermath of an attack, records will also provide evidence to any police investigations, coroners' inquiries and public inquiries and also assist in defending against legal action; criminal charges or civil claims.

CPNI provides guidance on completing a risk assessment[1]. Risks change over time. Ensure the risk assessment is reviewed at least annually.

Basis of the guidance

The guidance in this document is based on:

- CPNI's extensive analysis of previous marauding terrorist attacks in the UK and elsewhere around the world
- Live simulations[2] of marauding attacks involving hundreds of people to understand where responses can fail and test the effectiveness of training, procedures and security systems
- Reviews of security arrangements at organisations forming part of the Critical National Infrastructure (CNI) that have highlighted common issues.

[1] CPNI guidance on completing a risk assessment: https://www.cpni.gov.uk/principles-risk-assessment

[2] Report on live simulations, available from your CPNI adviser: "ASCEND – Improving Organisational Response to *Marauding Terrorist Attacks: A Summary of Key Emerging Themes* from Trials Conducted in 2017 and Early 2018"

Associated documents

This document sits at the centre of a suite of guidance to help your organisation prepare for a marauding terrorist attack. A shorter document, aimed at senior managers, summarises the key points. Several supplementary documents provide necessary detail in a number of areas.

Documents in the suite are listed in *Figure 1:* Marauding terrorist attack guidance documents.

References to further guidance on a number of related topics are provided in footnotes.

Figure 1: Marauding terrorist attack guidance documents

MARAUDING TERRORIST ATTACKS: MAKING YOUR ORGANISATION READY	Principal guidance document
MARAUDING TERRORIST ATTACKS: A BUSY READER'S GUIDE TO MAKING YOUR ORGANISATION READY	Overview guidance for senior managers
MARAUDING TERRORIST ATTACKS: SUPPLEMENTARY GUIDANCE ANNOUNCEMENTS	Guidance on alerting personnel using live and recorded announcements
MARAUDING TERRORIST ATTACKS: SUPPLEMENTARY GUIDANCE LOCKDOWN	Discussion of considerations for locking doors to delay and frustrate attackers
MARAUDING TERRORIST ATTACKS: SUPPLEMENTARY GUIDANCE PREPARING PERSONNEL	Intended to assist your organisation in developing a programme to raise awareness and provide training
MARAUDING TERRORIST ATTACKS: SUPPLEMENTARY GUIDANCE WORKING WITH POLICE AND OTHER EMERGENCY SERVICES	Guidance on integrating your response with the emergency services and background on the emergency services' response to a marauding terrorist attack
MARAUDING TERRORIST ATTACKS: SUPPLEMENTARY GUIDANCE ACTIVE DELAY SYSTEMS	Guidance looking at benefits of certain technologies which can delay, disorientate and distract attackers.
MARAUDING TERRORIST ATTACKS: SUPPLEMENTARY GUIDANCE TESTING AND EXERCISING	Discussion of the importance of a security plan and that all tasks identified and considered should be tested and exercised.
MARAUDING TERRORIST ATTACKS: SUPPLEMENTARY GUIDANCE PHYSICAL BARRIERS TO DELAY AND DISCOURAGE ATTACKERS.	Intended to assist your organisation that certain barriers will delay attackers.

About CPNI and NaCTSO

The Centre for the Protection of National Infrastructure (CPNI) is the government authority for protective security advice to the UK national infrastructure. Its role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

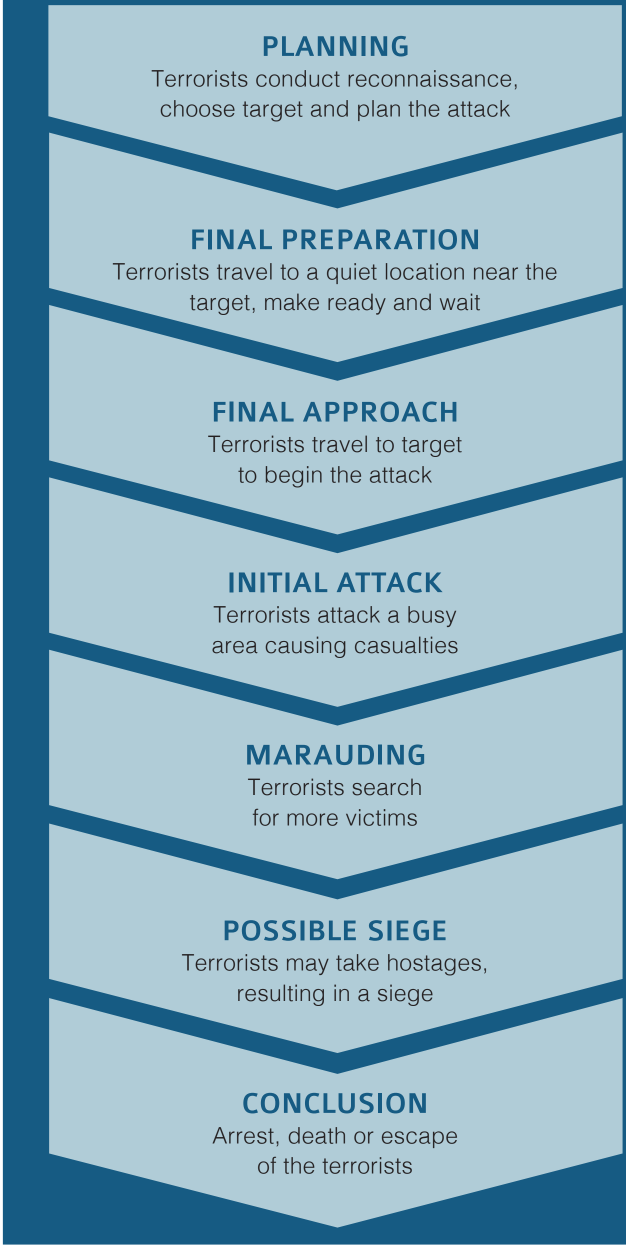
The National Counter Terrorism Security Office (NaCTSO) is a police unit within The National Counter Terrorism Police Headquarters (NCTPHQ) that supports the 'protect and prepare' strands of the government's counter terrorism strategy. It provides help, advice and guidance on all aspects of counter terrorism protective security to government and industry.

WHAT ARE MARAUDING TERRORIST ATTACKS?

Terrorists enter a busy area aiming to kill or injure as many people as possible. The attackers then begin marauding, travelling on foot or in a vehicle, to find and kill or injure more people. 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. The terrorists may take hostages, resulting in a longer siege. Attacks may conclude with the arrest, death or escape of the terrorists.

Terrorists typically use a quiet location where they expect not to be disturbed to make final preparations, ready weapons and wait for the appropriate moment to make their final approach to the target and launch the attack. Attacks often begin in areas that are not controlled by any single organisation (sometimes called 'grey space'). Most deaths occur during the initial attack and before police are able to respond.

Figure 2: Common phases of a marauding terrorist attack



PLANNING
Terrorists conduct reconnaissance, choose target and plan the attack

FINAL PREPARATION
Terrorists travel to a quiet location near the target, make ready and wait

FINAL APPROACH
Terrorists travel to target to begin the attack

INITIAL ATTACK
Terrorists attack a busy area causing casualties

MARAUDING
Terrorists search for more victims

POSSIBLE SIEGE
Terrorists may take hostages, resulting in a siege

CONCLUSION
Arrest, death or escape of the terrorists

Marauding terrorist attacks can take many forms:

- 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, guns, pipe bombs, petrol bombs or multiple weapons.

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

An attack is highly likely to have been planned. Terrorists typically research multiple targets, searching for one where their attack is most likely to succeed. Attacks are typically perpetrated in order to generate publicity for the terrorists' cause and are fortunately rare.

Other terms used outside of this document for similar styles of attack include:

- *Plato* (sometimes capitalised to PLATO, often seen in the context of 'Operation Plato'); used by UK police and other emergency services
- *MTFA:* Marauding Terrorist Firearms Attacks; used within UK government and emergency services for attacks including but not limited to those involving firearms
- *Firearms and weapons attacks;* used in the 'Stay Safe: Run, Hide, Tell' UK public awareness campaign[3]
- *Active shooter or active assailant;* used to describe one or more individuals perpetrating an attack, including but not limited to those that are ideologically motivated. The term is often used to refer to the attack itself, including where the attacker uses a weapon other than a firearm.

How people react to a Marauding Terrorist Attack

Preparing people for an attack can greatly influence their behaviour and improve their chances of survival. How people react to a marauding terrorist attack depends on a variety of factors including:

- Their awareness of the general threat of marauding terrorist attacks
- How alert they are to their surroundings
- Whether they can hear an attack; people screaming, gunshots or explosions
- Whether they can see an attack
- The reactions of those around them
- Whether they have rehearsed their response.

People may be in a state of disbelief that a terrorist attack is occurring, taking no action at all or taking action that puts them in danger such as approaching the attackers or beginning to film using a smartphone.

Stress and fear cause different reactions in individuals. The body's physiological response to stress can lead to loss of peripheral vision and reduced hearing as well as a diminished ability to make decisions and process verbal instructions. People may:

- Freeze, being temporarily unable to process information or make decisions
- Flee, typically leaving using familiar rather than optimal routes or following a crowd
- Fight, even when their chances of winning are low.

When the best of course of action is unclear, people are led by the actions (or inaction) of those around them. This means that people may follow a crowd, even when others in the crowd are no better informed.

[3] 'Stay Safe' public awareness campaign: https://www.npcc.police.uk/NPCCBusinessAreas/WeaponAttacksStaySafe.aspx

Marauding Terrorist Attack incidents in Europe

London Bridge, London, UK, June 2017

Three terrorists drove a van, containing petrol bombs, into pedestrians on London Bridge, killing two people, before beginning to maraud. Armed with kitchen knives and wearing fake suicide vests, the attackers entered several bars and restaurants, killing six people with kitchen knives. Dozens of people were injured. The attackers targeted at least one building that had been locked but where the occupants were still visible having failed to hide. The attack lasted roughly eight minutes.

Westminster Bridge, London, UK, March 2017

A single terrorist drove a car into pedestrians on Westminster Bridge, killing five people and injuring more than 50. Running towards Parliament, he then stabbed and killed a police officer before being shot. The attack lasted 82 seconds.

Paris, France, November 2015

Three groups of terrorists killed 130 people and injured over 400 during a three hour long attack on central Paris using explosives and assault rifles.

One of a group of three suicide bombers blew himself and a by-stander up at an entrance to the Stade de France during an international football match, after being refused entry. The two other bombers, who may have been intending to target people as the stadium was evacuated, subsequently blew themselves up outside the stadium.

The second group, travelling by car, used assault rifles to kill patrons of bars and restaurants in a different area of Paris. The third group attacked the Bataclan Concert Hall resulting in a siege.

Paris, France, January 2015

Two terrorists, arriving by car and first incorrectly entering a neighbouring building, coerced an employee to gain entry to the office of the targeted magazine Charlie Hebdo and killed 12 people with assault rifles. After shooting at responding police, the terrorists escaped by car and killed a police officer nearby. The original vehicle was abandoned and the terrorists hijacked a car in order to escape.

SAVING LIVES THROUGH YOUR RESPONSE TO AN ATTACK

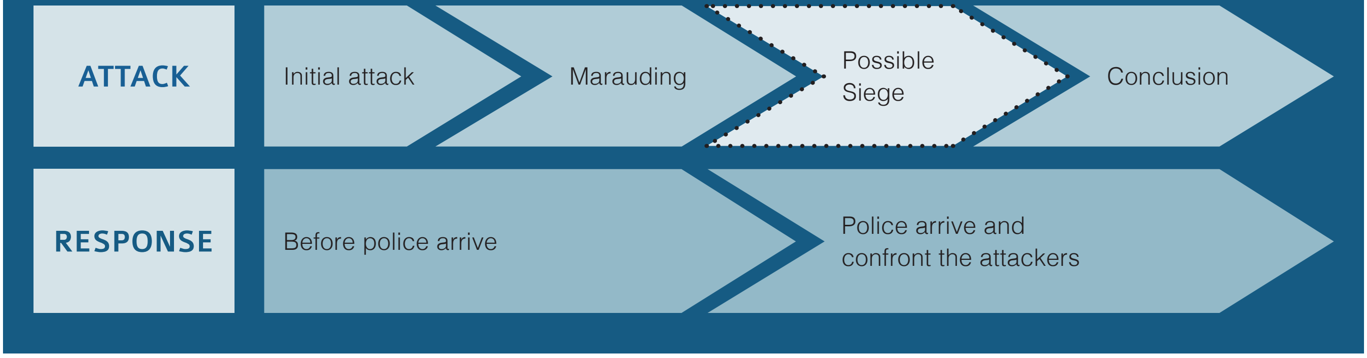
The fast pace of a marauding terrorist attack means it is necessary to take action immediately to save lives. Crucial response tasks are listed in the figure 3 below.

Figure 3: Suggested priorities for response tasks to be completed by security and front-line personnel. Your organisation must determine its response priorities and ascertain what is realistic through planning and testing.

CRITICAL	Detect the attack and make a rapid initial assessment Call, update and facilitate police Alert personnel and members of the public to take action Decide whether to instigate lockdown and use any active delay systems
IMPORTANT	Alert neighbours Keep personnel and members of the public updated Make a detailed assessment Direct front-line personnel
OTHER	Contact senior management Record events, decisions and actions

Preparation is essential to a swift and effective response. It is not enough to rely solely on the response from police. The pace (see Figure 4) of a marauding attack means that most of the deaths will have occurred before they arrive.

Figure 4: Typical concurrent MTA attack and response phases



ACTIONS OF SECURITY AND FRONT-LINE PERSONNEL

Personnel with a security role must act quickly and correctly to minimise the impact of a marauding terrorist attack. Those with such a role are not limited to dedicated security personnel (such as security control room operators and guards) and include other front-line personnel: stewards, receptionists, concierges and building facilities managers.

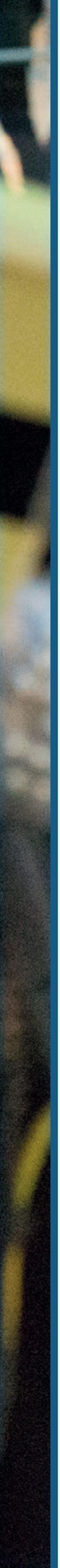
Empowering all security and front-line personnel to make decisions to counter a marauding terrorist attack prevents unnecessary delays that may cost lives. Where these personnel are trained and your organisation is confident in their ability, CPNI recommends that they are permitted to instigate response procedures rather than waiting for a senior colleague to investigate and confirm.

In the event of an attack, there are a number of critical tasks that must be completed before police arrive: assessing the situation, calling police, alerting personnel and members of the public to take action and deciding whether to lock doors to delay attackers (termed a `lockdown'). The responsibility for completing these tasks should rest with operators in your organisation's Security Control Room (SCR) if it has one.

CPNI's research has shown that security control room operators are often unclear on what tasks needs 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 security control room operators.
See section Effective working in the Security Control Room.

Organisations without a security control room must allocate responsibility for critical tasks to appropriate personnel. Typically this should be front-line personnel such as security guards, receptionists and concierges who are most likely to recognise an attack first and be able to guide the actions of personnel and members of the public.

It is important to test response plans to ensure they are realistic; CPNI's research has shown that organisations underestimate the difficulty of tasks and overestimate how much can be accomplished with a given number of security and front-line personnel.



Detecting the attack and making a rapid initial assessment

Rapid assessment of an attack determines which procedures should be followed, informs decision-making and enables security personnel to communicate information about the attack to police and other personnel.

CPNI's research has shown that it is difficult for security control room 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 improved configuration of technical security systems.

Often the first indication of an attack is people moving in the same direction forming a large crowd. However, the cause of this may not be possible to discern and there may not be a threat. For example, at Oxford Circus tube station, London in 2017, an altercation between two people on the platform resulted in a large crowd running from the area, falsely believe a marauding terrorist attack was in progress. In such situations, more information must be gathered to make an assessment. For example, a guard could ask members of the crowd for information or external CCTV could be used to look beyond your organisation's perimeter to identify the cause.

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 alert and even lock doors. Covert duress alarms at access control points are similarly useful in the situation where someone is coerced into granting access to an attacker.

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.

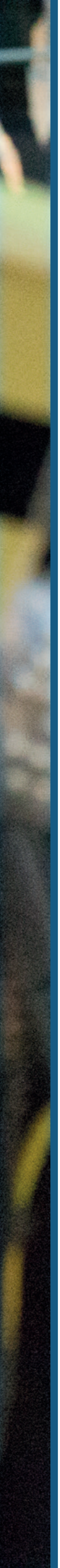
The coverage and display that is optimal for detecting and tracking a marauding terrorist attack is often different from the design that is best for meeting the requirements of business-as-usual. Comprehensive video coverage of entry points and thoroughfares, including stairwells, is needed to track the general location of attackers, personnel and members of the public. Routes likely to be used by attackers should be prioritised.

A recording and playback function helps when attempting to identify the attackers and 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 CPNI's guidance on video monitoring[4] for more detailed information.

Attack detection systems

Technical options such as gunshot detection systems (GDS; see CPNI's document "Introduction to Gunshot Detection Systems") for firearms attacks and emerging technologies such as anomalous sound and video analytics can assist in detecting and later tracking an attack, for example by detecting screams during a bladed-weapon attack or detecting individuals lying on the floor. For CPNI-approved systems where there is a high degree of confidence in alerts, it may be beneficial for announcements or a security response to be initiated automatically.

[4] CPNI guidance on video monitoring: https://www.cpni.gov.uk/cctv



Critical response tasks for security and front-line personnel

Calling and updating 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 services need not be called separately.

CPNI's research has shown that 999 calls made by security personnel are often poor, with the caller being unprepared to supply the type of information that was required, telling the operator their incorrect interpretation of what was happening rather than what they had seen and ending the call prematurely, preventing them from providing ongoing updates. Training and practice bring improvement.

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 (see section Making a detailed assessment).

Understanding the conversation with a police call handler

The call will be made at a time when the caller is under extreme pressure, having just detected the attack or whilst in hiding. The police call handler will also be coming under increasing pressure as there is a rapid surge in the number of calls as a result of the attack.

Police will be seeking to triage calls and rapidly identify callers who have crucial information. The caller needs to facilitate this process by providing the key information in a useful format. When the caller is an operator in the security control room or, for sites without a security control room, the person primarily responsible for calling police, the caller should identify themselves as such and tell the police call handler that it is crucial that the line is left open.

What information to provide

The police call handler is likely to ask scripted questions. The caller may have valuable information that has not been specifically requested; this information should also be provided. If the police do not recognise that the caller has key information and the ability to provide more, the 999 call may be dropped in order to answer other outstanding calls.

The caller should report:

- That an armed terrorist attack is taking place now
- The address of the site where the attack is underway
- Their role at the site; for example the principal security officer or an operator in the security control room
- Any current and reliable information they have about the attack, particularly:
  - The number and descriptions of attackers
  - The number and type of weapons (knives, pistols, assault rifles, etc.) used
  - The current location of the attackers and the ability to track the attackers and provide updated information
  - The number of casualties
- The current best access routes into the site, if known
- Whether they are able to provide information about other security capabilities at the site, such as video monitoring, locking down and securing the venue, the location of safe rooms
- Whether they are able to use a public address system to pass information to people at the site.

If the police call handler believes a caller has critical information about the incident the call may be passed to a specialist police officer or they will call back. The role of the police is to obtain as much information about the ongoing situation as possible.

Each police force will have similar but bespoke call handling protocols. You should work with local police and other emergency services' planners to understand the information they require. For more information see the supplementary guidance document *"Marauding Terrorist Attacks: Supplementary Guidance – Working with police and other emergency services"*.

Clarifying unfamiliar and ambiguous terms

Personnel talking to police call handlers and the responding police officers should be aware that members of the emergency services use certain terms that have a specific meaning, which may differ from everyday use. Emergency services use their own terminology to describe the layout of buildings and sometimes use the phonetic alphabet to describe attackers and members of the public. CPNI's research has shown that this can cause misunderstandings. Personnel must not attempt to use emergency services' language and must seek clarification where meaning is unclear.

Similarly, personnel must use plain language and remember that the police call handler and responding police officers are unfamiliar with their site, its layout and its naming conventions.

Assisting police when they arrive

When police arrive at your site they may ask for assistance or provide instructions on what to do next. These may include:

- Requesting a concise report on the current situation
- How to obtain floor plans, keys and access tokens for the site
- Asking for a person with knowledge of the site to attend the Forward Command Post; the location from which the emergency services' response is managed
- Changes to lockdown to facilitate police access
- Specific content for announcements
- Sirens or alarms at the site to be switched off.

When it has not been possible to make contact with police officers before they enter the site, a security officer who is not under immediate threat should reveal themselves to the police (clearly announcing themselves with their hands in view), stating if they have direct communications with the security control room.

Alerting personnel and members of the public to take action

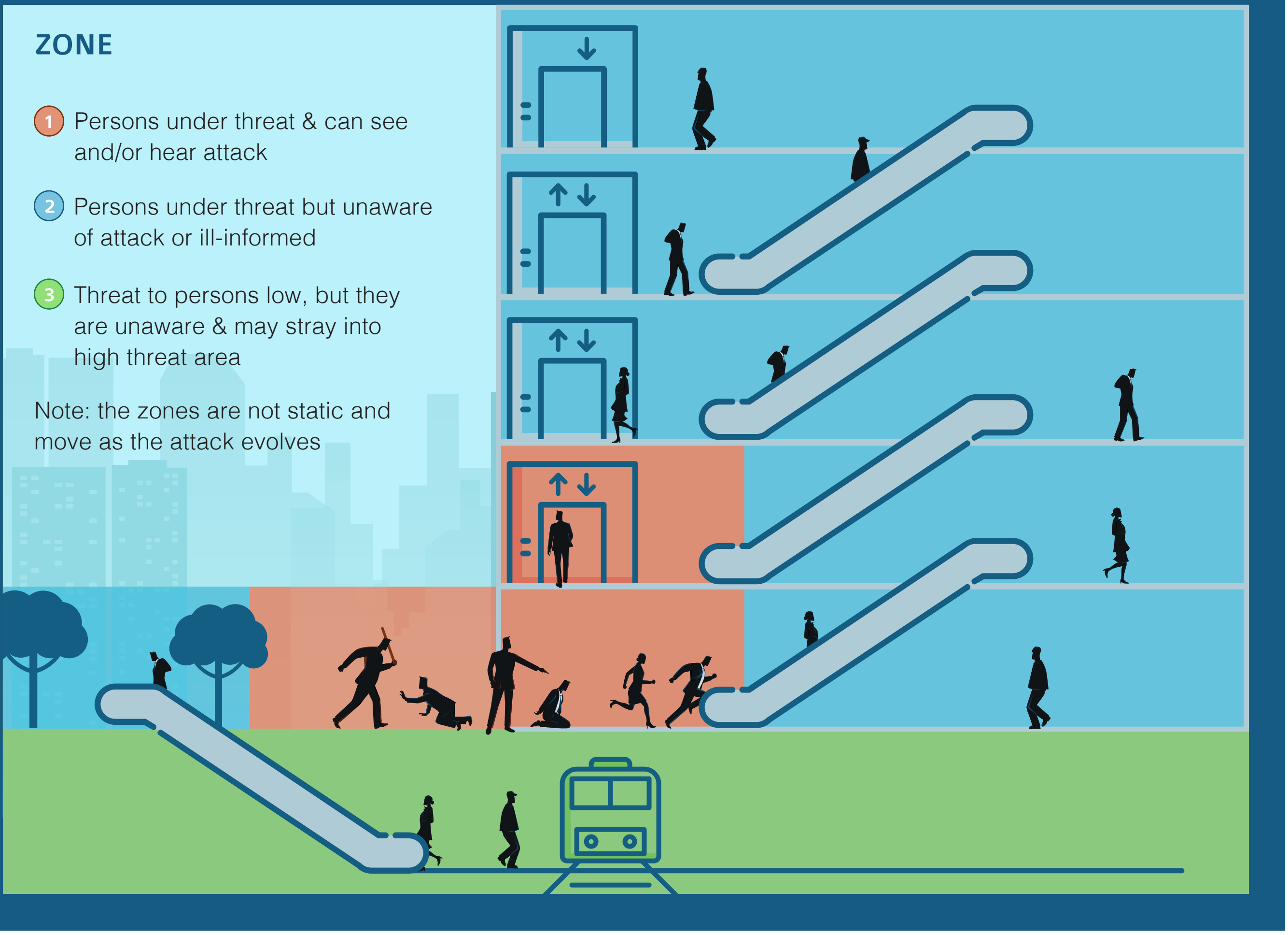
Personnel and members of the public must be alerted to the attack so they know to take action; see section Applying *'Run, Hide, Tell'* in your organisation. They must be given clear, concise and current information in order to make the right decisions to survive.

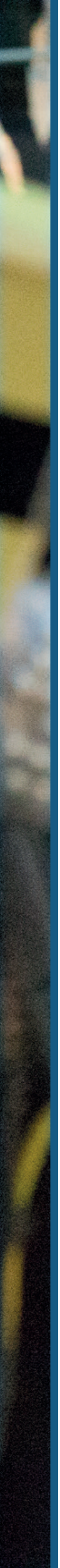
An announcement (using a Public Address – PA – system) is the best way to achieve this. CPNI's research has shown that both the content and delivery of announcements are critical for people to take appropriate action. It has also shown that security control room operators often make poor announcements that are inaudible, rambling, vague, misleading, incorrect and lack credibility. Training and practice has been shown to significantly improve the quality of announcements made by operators. Systems that do not have an alert sound preceding the announcement are desirable so that pertinent information can be communicated as quickly as possible. External speakers can help prevent people from entering a site that is under attack.

Other ways to reach people include digital signs, text message alerts and similar systems, such as smartphone applications.

Alerts should be aimed primarily at people who are at high immediate risk but may not be aware of the attack (those in zone 2 in Figure 5) and secondarily at people who are at lower immediate risk but may stray into a high risk area (those in zone 3 in Figure 5). People who are already in the midst of the attack (those in zone 1 in Figure 5) will gain more value from their own senses and until they escape the immediate threat are likely to ignore alerts and updates.

Figure 5: Public announcements should be aimed at zones 2 and 3


ZONE
1 Persons under threat & can see and/or hear attack
2 Persons under threat but unaware of attack or ill-informed
3 Threat to persons low, but they are unaware & may stray into high threat area
Note: the zones are not static and move as the attack evolves



✓ An example of a good announcement:

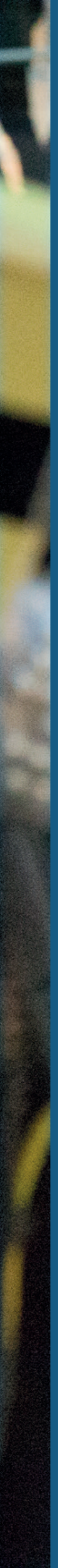
"The building is under armed attack. There are multiple attackers located in main reception. Evacuate the building if you can, hide if you cannot. Police have been called. The building is still under armed attack. There are still multiple attackers located in main reception. Evacuate the building if you can, hide if you cannot. Police have been called."

✗ An example of a poor announcement:

"[Announcement alert tone] Ladies and gentlemen, may I have your attention, please. This is the security control room. There is a security incident currently in progress on this site. Would all staff please leave their belongings where they are and make their way to the nearest fire exit in order to leave the building."

The content of the announcement should align with your response procedures for personnel and members of the public. For example, some buildings may require a phased evacuation or have dedicated shelters to which people might be directed.

For more information see the supplementary guidance document *"Marauding Terrorist Attacks: Supplementary Guidance Announcements"*.



Instigating lockdown and using active delay systems

Most deaths occur within the first few minutes of a marauding terrorist attack. Analysis of historic attacks and CPNI's research have shown that instigating lockdown in the event of a marauding terrorist attack can be a highly effective way of reducing casualties. It is typically most useful when an attack begins outside a site or building, where lockdown can delay attackers from entering an area or deter them altogether.

Lockdown, sometimes referred to as `dynamic lockdown', means locking doors (or other barriers such as turnstiles) to prevent access to part of a site or building. It is most likely to be of use to deter and delay attackers attempting to enter a building from the outside. Lockdown aims to reduce the immediate threat of harm by:

- Delaying attackers' progress in finding and killing victims
- Preventing people inadvertently putting themselves into the path of attackers.

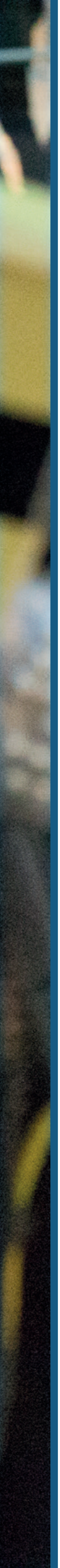
However, a poorly implemented lockdown can actually increase the risk to personnel and members of the public. Lockdown may not be suitable in situations including:

- Sites where access is generally not restricted and there are no barriers to lock
- Sites with limited escape routes where the risk of a crush may be too high if people's exit were slowed or stopped
- Buildings with many doors that are locked and unlocked manually, where the speed of instigating or cancelling a lockdown would be too slow
- Attacks beginning within a building where locking doors would impede people's escape
- Where there are insufficient security personnel to monitor and maintain lockdown integrity.

Lockdown requires careful planning of procedures and security equipment as well as training of personnel. For more information, see the supplementary guidance document *"Marauding Terrorist Attacks: Supplementary Guidance – Lockdown"*.

Active Delay Systems (ADS) inhibit attackers' senses to slow their progress. Such systems use a variety of methods including security fog, strobe lights, LED and glare lights as well as darkness. The effectiveness of active delay systems depends on where and how they are used.

These systems may also inhibit the ability of people to escape and emergency services to respond. Consider and test whether automated or manual activation is more appropriate for your site. For more information see CPNI's document "Introduction to Active Delay Systems".



Important response tasks for security personnel

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

Alerting neighbours

Marauding attackers will enter surrounding locations looking for further victims. By alerting your neighbours to the attack you allow them to take action to evacuate or lockdown premises.

This requires that a means of communication such as a shared radio channel or a shared channel/chatroom/group on an instant messenger application has already been established and given to operational security personnel (see section Neighbouring organisations and landlords).

Updating personnel and members of the public

Equipping people with current information about the progress of the attack and the whereabouts of attackers means that they can make the best decisions about what action to take. CPNI's research has shown that people in hiding may emerge and put themselves in danger if they are not told that the attack is still in progress. People are reassured by regular announcements. For live voice announcements, updates should be issued approximately every minute, even if there is no change to the situation.

The police may request that particular announcements are made depending on the circumstances of the incident. Unless the police make a specific request to do so, it should not be announced that the police have arrived since doing so would inform attackers and removing the police's advantage. Instead, continue to reassure people by announcing that "police have been called".

For more information see the supplementary guidance document *"Marauding Terrorist Attacks: Supplementary Guidance – Announcements"*.

Making a detailed assessment

Gathering more information about the attack will inform your decisions and enable you to pass information to personnel and members of the public as well as police. Assessing the attack in more detail requires a competent operator using a video monitoring system with coverage of thoroughfares and a playback facility. It will take several minutes. The assessment should identify:

- The number of attackers, likely requiring live monitoring of their movements
- What they are wearing and carrying
- Weapons (whether they have knives, pistols, assault rifles, explosive vests for example)
- Whether they have split up or remain as a single group.

If possible, obtain still images of the attackers to assist police.

Directing front-line personnel

Front-line personnel, such as guards, stewards, concierges and receptionists can be directed over a shared radio channel with more detail than can be communicated using public announcements. Those already in the midst of the attack are unlikely to be able to listen or answer.

Radio protocol

CPNI's research 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. It is crucial that people are concise when conveying information and are 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).

Effective communication undoubtedly becomes more difficult under pressure and it is important that this skill is regularly practiced following training.

Radio system

The radio system for communication between personnel may not function between all areas of the site. Guaranteeing comprehensive coverage is typically unrealistic and cost-prohibitive. However, you should take a risk-based approach to ensure that there is coverage where it is important for your response plans, such as at entry points. Consider headsets for front-line personnel to enable them to receive transmissions whilst in hiding without being heard by attackers.

Other response tasks for security personnel

Life-saving tasks must take priority when responding to a marauding terrorist attack. However, as soon as practical, without disrupting other tasks, contact senior management and record a log of events and decisions.

Contacting senior management

Senior managers should be made aware of the attack so that business continuity and post-attack recovery procedures, such as engaging with the media, can be activated (see section Recovering from a marauding terrorist attack).

Recording events, decisions and actions

When there is time available to do so without delaying other tasks, create a record of the incident detailing:

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

In a security control room an automated system (such as a video and audio recorder) can be used to record what actions operators take and when, though a written record is still useful to explain why those actions were taken.

The record will assist your organisation and others in improving their preparations for responding to a similar incident. It will also be important in providing evidence to any investigations, coroners' inquiries and public inquiries into the attack.

EFFECTIVE WORKING IN THE SECURITY CONTROL ROOM

If your site has a Security Control Room (SCR), its operators will be primarily responsible for making time-critical, operational decisions and completing key tasks in the event of an attack.

A security control room staffed by dedicated personnel provides security monitoring of a site and manages the response to security incidents, typically in coordination with a guard force. CPNI provides detailed guidance[5] on preparing your security control room.

Many of the skills and supporting tools required to respond to a marauding terrorist attack are different from those required during business-as-usual. Training, practice and rehearsal are essential to enable personnel to develop necessary competence.

Defined roles

Roles for responding to a marauding terrorist attack should be defined and assigned tasks to be completed. The precise roles depend on the number of operators and the capabilities at your site. For example, roles for a three-person security control room might be:

- Assessor and tracker: responsible for making the initial assessment, using security systems to track attackers and gathering more information
- Police liaison; responsible for making the 999 call, updating and facilitating police
- Announcer and lockdown operator; responsible for making announcements, instigating lockdown and monitoring its status.

CPNI's research has shown that organisations often overestimate what each operator is able to accomplish. It is important to test response procedures at your site to determine how roles are best defined.

Clear leadership

In the event of an attack, there must be no confusion about who is in charge in the security control room. Establish a clear order of succession so that whichever operators are on duty and present, everyone understands who will take charge to make decisions and assign roles.

Effective communication between operators

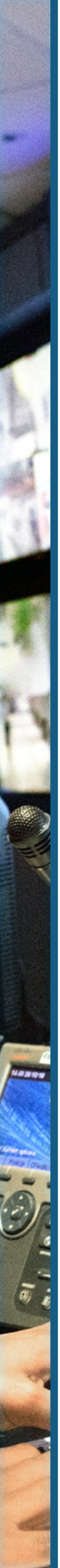
Security control room operators need to work closely together to complete key tasks. For example, one operator may be tracking the location of attackers whilst another is announcing the attackers' location to enable personnel and members of the public to make well-informed decisions.

CPNI's research has shown that poor quality communication between security control room operators significantly degrades the quality of the overall response. It is rare that security control room operators need to work so closely under such pressure. Regular practice provides an opportunity to build skills and working relationships.

Knowledge of response procedures

Security and front-line personnel will be primarily responsible for making operational decisions in the event of an attack. It is essential that they have a comprehensive knowledge of your organisation's response procedures so that they are able to implement decisions that have been carefully thought through in advance. It is valuable to include security personnel during table-top exercises.

[5] CPNI guidance on security control rooms: https://www.cpni.gov.uk/control-rooms



Optimised configuration of operators' terminals and video wall

Being able to comprehend a quickly changing situation is critically dependent on video monitoring coverage and how the information is presented. The optimal layout of a video wall to track a marauding terrorist attack is likely to differ from the arrangement for business-as-usual, requiring an overview of your site with a geographically logical, easily interpreted layout. It is unrealistic to expect that fast-moving attacks may be tracked by manually selecting cameras to view. Consider how the configuration may be rapidly switched over in the event of an attack.

The configuration of each control station should be optimised for a defined role (see section Defined roles) whilst taking into account that some operators may be absent (for example, on a toilet break) as an attack begins.

The configuration of systems should be trialled and optimised through rehearsals.

Dedicated mechanism for communicating with police

The ability to communicate with police is essential. An assured mechanism, accessible from control stations, for making and receiving calls with police should be available. Dedicating a line and handset only for communication with police ensures that calls from police (for example, if called back by a specialist police officer following a 999 call) can be easily prioritised.

Ensure backup communication methods are available such as a mobile phone with charger and hands-free kit.

Integration with security control rooms of landlords and neighbours

Sites with landlords such as offices in a shared-tenancy block or shops in a shopping centre should ensure that their security control room is able to work alongside the security control room of their landlord. Neighbouring organisations such as nearby office buildings, may also be willing to facilitate close working of security control rooms to mutual benefit. A coordinated monitoring and response capability will reduce the impact of a marauding terrorist attack. This is achieved by:

- Co-locating security control room operators where appropriate
- Working together to develop and test response procedures
- Establishing a common way of referring to locations, buildings, corridors and stairwells (see section Assisting orientation and navigation)
- Enabling straightforward two-way communication between control room operators in different rooms and buildings
- Integrating technical security systems to communicate alerts between control rooms and allow monitoring of relevant video feeds.

Monitoring of news and social media

News channels and social media are useful sources of alerts of incidents in the vicinity of your site, which may enable operators to take action to secure your site before an attack reaches it. Ensure these are monitored in the security control room. Software for accessing social media software can often be configured to provide alerts when new posts meet defined criteria (for example the name of the area where your site is located in combination with 'terrorist' or 'attack').

Location of an on-site control room

A compromise is required when choosing a location that is protected from attackers but may also be reached by police responding to an attack. To provide protection, it is recommended that the room is located inside your site (not on the perimeter) and on a floor that does not have external access points (not on the ground floor). A room on the first or second floor, facing the interior of your site, close to a stairwell that runs from an entrance is ideal. The location of the security control room should not be widely advertised and discreet signs should be used.

Construction materials

Operators, who will be under significant pressure, should feel confident that they will be protected from the attack whilst within security control room. CPNI provides guidance on security walling systems[6] and security doors[7].

Securing systems on evacuation of the security control room

It may be necessary to evacuate the security control room, for example in the event of a fire. To ensure that security and monitoring systems cannot be used by attackers, the systems should be secured as the room is abandoned. Typically, simply locking the door to the security control room is adequate. Where it is necessary to lock terminals, consider providing a straightforward mechanism such as an emergency stop switch. Manually locking or powering down systems is likely to be time consuming, putting operators in danger.

[6] CPNI document: "A Guide to Security Doorsets and Associated Locking Hardware"
[7] CPNI document: "A Guide to Security Walling Systems for the Protection of Important Assets"

COMPLETING CRITICAL RESPONSE TASKS WITHOUT A SECURITY CONTROL ROOM

For organisations without a security control room, the responsibility for completing critical response tasks (see section Critical response tasks for security and front-line personnel) must be allocated to appropriate personnel. Typically, this should be front-line personnel who are best placed to recognise an attack and guide the actions of personnel and members of the public. Response tasks may be very difficult to complete since front-line personnel must also take action to save themselves.

It is unlikely that front-line personnel will be able to complete tasks additional to those that are critical. There is a risk that front-line personnel may be killed or injured before they are able to complete their assigned tasks. Plan for more than one person to complete a task to offer redundancy. It is crucial that the police are called and therefore does not matter if they receive more than one call from the same organisation.

Technical solutions such as automated voice alarms and door locks activated by panic buttons (see section Panic buttons and duress alarms at entry points) or CPNI-approved attack detection systems (see section Attack detection systems) can enable tasks to be more rapidly completed. Two-way communication with any landlord's security control room is essential.

APPLYING 'RUN, HIDE, TELL' IN YOUR ORGANISATION

People must recognise an attack and take action to run or hide. Inaction may cost people their lives.

People should take action following the principles of 'Run, Hide, Tell' (published by the National Counter Terrorism Security Office, NaCTSO). These general principles were written as part of a public awareness campaign and are intended to be applicable to any location. Organisations must build on these principles to enable their personnel to make the best choices using knowledge of the site, its capabilities and your organisation's emergency procedures. Visitors and members of the public are likely to be less able to recognise an attack as well as less familiar with your organisation's site layout, environment and procedures. They should be guided by knowledgeable personnel.

Escaping from the threat and leaving the area of an attack altogether is ideal. However, running is not always the best option. Buildings are designed for evacuation in the event of a fire, not a terrorist attack. It may take many minutes for buildings to be evacuated with some requiring a phased evacuation to avoid a crush. Attempting to leave a location may bring people into the path of oncoming attackers. If lockdown (locking doors to separate people from attackers) is instigated at your organisation's site, people are likely to be safer sheltering in a locked area that attackers cannot reach. People who are less able to escape, such as young children and those with health conditions or impairments should reach a nearby lockable room to shelter and hide.

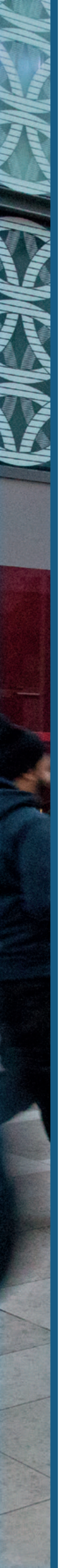
Increasing people's awareness improves their ability to recognise a marauding terrorist attack and enables them to make choices that will save their own lives and those of others. The supplementary guidance document *"Marauding Terrorist Attacks: Supplementary Guidance – Preparing personnel"* is intended to assist your organisation in developing a programme to raise awareness and provide training.

Changes to your site to enable people to orientate themselves, navigate and easily escape. Introducing doors and other obstacles delays attackers.

'Run' applied in your organisation

Personnel must:

- Locate the threat using their sight and hearing or with information from announcements
- Decide whether to run or hide using their knowledge of your organisation's response procedures, information from announcements and guidance from front-line personnel
- Decide where to run to rather than follow a crowd without thinking:
  - A building or site exit, followed by leaving the area
  - A purpose-built shelter
  - Lockable rooms
  - High floors and centres of buildings
- Choose an escape route using knowledge of the site layout and information about the location of attackers
- Move quickly but quietly, avoiding making noise that would attract marauding terrorists
- Disperse and leave the area once they are outside the immediate area of the attack.



Creating escape routes

People must have alternative escape routes available so that they are able to flee from an attack without becoming trapped. Escape routes need to allow people to disperse as soon as practical rather than funnelling them to a point where they may be more vulnerable to attack. Consider which routes may not be usable during likely attack scenarios (most often because they form part of the attackers' likely access route). Determine whether the remaining escape routes will be sufficient to handle the number of people using them; methods used in fire safety calculations can be applied.

Additional escape routes at entrances where there are security doors or barriers may require particular consideration. For example, where people enter into a public lobby but access into the rest of the building is restricted, people in the lobby would need a route to use for escape if attackers were blocking the main entrance. Where additional perimeter doors are required to provide escape routes, ensure they do not introduce vulnerable points that attackers could use to gain access.

Assisting orientation and guiding navigation

Enable people to make rapid decisions about their escape by helping them:

- Ascertain where they are in relation to the threat
- Navigate in order to escape.

CPNI's research has shown that people listening to announcements were frequently unable to use location information when the locations were arbitrarily named (for example "leave using stairwell 1" or "attackers are on the ground floor of block F") since they did not connect the named location to their environment. This reduced their ability to make appropriate decisions about where to go.

Consider how to refer to locations, buildings, corridors and stairwells to make navigation more straightforward, particularly in combinations with any public announcements. In locations with a well-known and logical layout, numbers and letters may be useful. For example, in a rail station "the exit on platform 3" is useful since the platforms are typically arranged adjacently in numerical order. However, in most locations, using landmarks or other identifying features is preferable to using arbitrarily assigned letters or numbers. For example "the exit opposite the Roast Bean café" is likely to be more readily understood than "exit P". In locations without obvious landmarks, consider introducing visual or other sensory cues to aid people in orienting themselves.

Signposts provide a way to guide people to a location by the shortest route. Site or building plans are also useful, though unlike signposts require those fleeing to stop or slow down in order to consult them.

Discreet signs for use by responding police are an effective method of marking a route to sensitive areas such as the security control room without assisting terrorists.
For more information refer to forthcoming guidance to be published by National Counter Terrorism Policing[8] (NCTP).

[8] National Counter Terrorism Policing: https://www.npcc.police.uk/CounterTerrorism/CounterTerrorismPolicing.aspx

‘Hide’ applied in your organisation

After the initial phase of killing, terrorists will begin to maraud to look for more victims. They are deterred by doors and other physical barriers that will cost them time and also by seemingly empty areas. Marauding terrorists are attracted to movement and noise.

Personnel who have not escaped must:

- Use lockable shelters with substantial walls such as purpose-built areas, back offices and meeting rooms where possible
- Otherwise use opportunistic hiding places such as inside cupboards, under desks and behind doors as they are opened; these can be very effective since attackers are moving so quickly
- Lock or barricade doors to delay attackers, ensuring that doing so does not attract attackers by making it obvious there is someone inside
- Stay silent, avoiding making noise that will attract attackers
- Stay still, avoiding being seen – the human visual system is highly attuned to movement
- Make an area seem unoccupied, for example by switching off lights and other equipment
- Set mobile phones and other devices to silent, with vibrate off and dim the screen.

Accessible hiding places or shelters

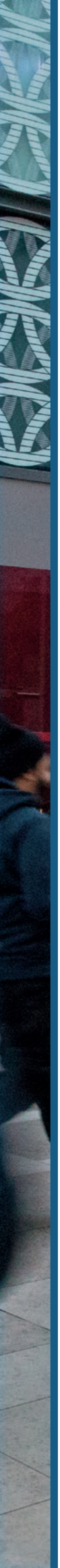
You must plan for people who are less able to escape such as young children and people with health conditions or impairments. A strong option is to provide accessible locations throughout a building for people to hide such as rooms with lockable doors and blinds covering internal windows. Where the intended occupants may have difficulty remaining quiet (such as young children) install basic soundproofing so marauding attackers are less likely to recognise that the room is occupied.

Lockable doors and barriers

Every door and security barrier on your site will delay the progress of an attack. For offices or other sites with areas of restricted access, dividing an area into zones using physical barriers such as turnstiles and security doors in combination with an automated access control system[9] (AACS) provides the best protection.

Any barrier is valuable, even those that are not designed for security use or are physically insubstantial. Lockable doors for staff areas and meeting rooms, doors fitted with closers (which also limit the speed with which they may be opened), collapsible gates on shop fronts and even fire doors will delay attackers and may discourage them from entering an area altogether if they perceive the barrier to be too difficult to overcome.

[9] CPNI guidance on access control systems: https://www.cpni.gov.uk/access-control-and-locks



Consider how doors may be closed and locked quickly from a safe location. For example, installing a control at the rear of a shop to operate a motorised roller shutter is preferable to a control at the front of the shop where the person operating it would be exposed to attack.

For more information see CPNI's guidance document "Introduction to physical barriers to delay hostile incursions."

'Tell' applied in your organisation

Running and hiding to ensure their safety are people's priorities. Using a phone or other device should only be attempted once a person is not in immediate danger. Calls to 999 may take several minutes and the situation may change quickly putting the caller in danger.

People must:

- Choose a time to call when there is no immediate danger, being mindful of the noise and light generated by mobile phones and other devices
- Where it is not known if police have been called, contact the police by telephone to report the attack; see section Calling and updating the police
- Where possible, use a hands-free kit with a headphone (but not a loud speaker) whilst making the call so their peripheral vision is not impaired
- If using social media, post only facts, not speculation and avoid insensitive photographs of those who are dead or injured.

Contacting the police by telephone

Calling 999, asking for police and speaking with a call handler is the most efficient way to report the attack to police. Where the call handler cannot confirm a response, the caller can press 55 to be connected to police, though they will need to speak quietly to give details. The location of a mobile phone is not automatically sent to a police call handler.

Contacting the police by text message for people who are deaf, hard of hearing, or speech-impaired

It is possible to contact the police by text message, using the emergency SMS service[10] which is aimed at people who are deaf, hard of hearing, or speech-impaired. However, it is necessary to register a phone number before using the service by sending the word 'register' to 999 followed by 'yes'.

Emergency messages should contain the service[10] to be contacted, the nature of the emergency and the location, ideally with precise address and landmarks. For example "Police. Knife attack. Inside Nibbles Pizza. Glossop Road Sheffield S10".

[10] emergencySMS service: https://www.ngts.org.uk/how-to-use-ngt/contact-999-using-ngt.html

RECOVERING FROM A MARAUDING TERRORIST ATTACK

In the immediate aftermath of an attack demands will be placed on your organisation by personnel, members of the public, emergency services and the media. Your business will need to continue to meet customers' needs without access to the site that has been attacked and with many staff dead, injured or otherwise unable to work.

The attack will affect your organisation and its personnel for many years afterwards. Your business should plan to support personnel through their long journey to recovery.

Immediate aftermath

What to expect

In the immediate aftermath of an attack, police will designate the site of the attack and surrounding area as a crime scene, establishing cordons to restrict access to police officers and staff. This means that the area will not be accessible to personnel or members of the public. Police may want to take statements from personnel and members of the public. The ambulance service will seek to treat people's injuries.

Accounting for personnel

It can be difficult to establish who has been injured or killed during an attack due to staff holidays, sickness, remote working and hot-desking. Many personnel may already have left the area and others will be receiving medical treatment. Personnel may have been separated from their mobile phones.

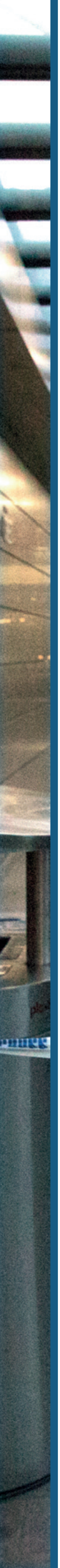
Consider using a hierarchical reporting system with managers checking on the well-being of their staff and providing a way for staff to report in following an incident such as a web application, automated text service or a telephone number routed to an external call-centre.

Medical treatment

Many people will require medical treatment for physical injuries as well as mental distress. Some people may have incurred a physical injury that has been masked by adrenaline during the attack. Working with the ambulance service, ensure that all personnel and members of the public are checked and given medical treatment where needed.

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[11].

[11] First Aid advice during a terrorist incident: https://www.gov.uk/government/publications/first-aid-advice-during-a-terrorist-incident



Providing for the needs of people who are separated from their possessions

People may have abandoned personal possessions when fleeing. These may include warm clothing, waterproof jackets and umbrellas, wallets, purses, car keys, house keys and mobile phones. It will not be possible to retrieve these whilst the police investigate. Your plans should include providing for the needs of personnel and members of the public.

Support for families and friends

Families and friends of those present will be seeking information and many may arrive at the scene of the attack. Plan to establish mechanisms through which information can be issued such as a dedicated telephone number, website or social media feed. Consider setting aside an area where people may be reunited with family and friends.

Handling the media

Local, national and international media will be searching for information to report and people to interview. Many news crews will arrive at the scene. Plans for handling the media should include a designated spokesperson, coordinating statements with the police, a means for providing continuous updates, and prepared responses to likely questions.

Business Continuity

Since the attacked site and surrounding area will be designated as a crime scene they will be inaccessible. Business continuity plans should include moving functions to an alternate location and covering the duties of personnel at the affected site.

Arranging vigils

Consider designating a place where people may leave tokens of remembrance. Organising a vigil provides an opportunity to allow people to begin to grieve and to offer support to those in need.

Long-term recovery

Medical and compassionate leave

Surviving employees may not be ready to return to work for an extended period. Consider how such leave may be managed as medical or compassionate leave. Think about offering financial support to employees, arranging cover for their duties and offering remote working.

Grief and trauma counselling

The psychological impact of such a violent event should not be underestimated. Each individual reacts differently. Consider facilitating grief and trauma counselling for all personnel, irrespective of whether they were present during the attack.

Anniversaries and memorial services

Acknowledging anniversaries of the attack with memorial services allows those affected by the attack to recover from the experience and allows former colleagues to reconnect. Anniversaries can bring buried emotions to the surface, particularly since there may be significant media coverage. Prepare to offer assistance to individuals who require it.

MAKING YOUR ORGANISATION READY TO RESPOND

Having learned what action is required and what tools are required to support that action, this section helps you manage your approach to preparing your response and becoming and remaining ready to face a marauding terrorist attack.

At the moment of crisis, trained personnel must follow well-rehearsed procedures to escape, aided by well-designed site layouts and technical systems able to delay attackers until police respond and engage. An effective response requires:

- Planning
- Development, followed by repeated testing and refinement of procedures
- Working with others internal and external to your organisation
- Changes to your site, security equipment and ways of working.

A list of planning tasks is provided in Annexe B: Marauding Terrorist Attack planning checklist.

Planning your approach

Make an individual responsible for planning and implementing your organisation's preparations. Governance arrangements should be clear with ultimate accountability at the highest level of your organisation.

It is crucial to keep records of decisions made and the reasoning behind them. Records will help to ensure that the risk is adequately mitigated and that resources are being allocated appropriately.

In the aftermath of an attack, your organisation will come under intense scrutiny by the media, law enforcement and other agencies to determine what, if anything, could have been done to prevent or better contain the attack. Records of your decisions will also provide evidence to any investigations, coroners' inquiries and public inquiries and assist in defending against legal action; criminal charges or civil claims.

Probable attack scenarios

Develop several attack scenarios to focus your planning. Preparing for every possible type of marauding terrorist attack is impractical. The scenarios you plan for will be guided by your overall risk assessment but should typically include:

- An attack starting outside your site
- An attack starting inside your site
- A possible attack signalled by a large crowd of people moving quickly towards your site without an obvious cause.

Each scenario should include:

- The likely types of weapon to be used (knives, guns, explosive devices, fire, hostile vehicles as a weapon)
- The number of attackers
- Whether the attackers remain grouped or split into multiple groups.

Terrorists will plan an attack to exploit weak points in your organisation's security. You need to understand where those weak points exist and how they might be used in the attack scenarios you have identified.

Think like an attacker. Begin by looking outside the perimeter of your site to identify locations where terrorists may choose for waiting and making final attack preparations. Consider where terrorists might attempt to enter your site and the routes they might subsequently follow. Consider what combination of methods an attacker would be likely to choose to overcome or bypass your security procedures and systems.

Developing response procedures

The response to an attack must be swift and decisive. Thinking through the response to attack scenarios in advance reduces the number of decisions that need to be made in the midst of an attack, when time is critical. How your organisation will respond in the event of a marauding terrorist attack should be captured in standard operating procedures (SOPs) which should form the basis for training personnel.

Developing procedures requires a process of repeated testing and refinement. An effective way to test your response during the development process is to use table-top exercises to work through hypothetical instances of the attack scenarios.

There are often conflicting requirements without obvious solutions. Determining the actions that are likely to lead to the best outcomes can only be achieved by gaining a full understanding of the risks and being creative in finding balanced options.

Testing components and later full integration of your procedures using practical rehearsals will highlight real-world issues and areas for further improvement.

Rehearsing

Rehearsing the response to a marauding terrorist attack is the only way to ensure that the procedures and technical systems function as expected and to highlight areas for improvement. Rehearsals are also key in preparing security and front-line personnel since the actions required of them during an attack do not form part of their usual duties.

Rehearsals need not disrupt the usual business of your organisation and can be conducted at different levels of complexity.

Rehearsing response components

At the component level, rehearsals should be conducted daily or weekly. Individual technical systems and individual aspects of the response can be usefully tested. For example:

- A security control room officer could practice making clear and concise announcements using a public address voice announcement system appropriate for a possible attack scenario playing out
- An automated access control system could be tested during quiet hours to ensure that a lockdown function works as intended
- A video wall layout could be trialled 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 guards and a security control room operator in different rooms.

Rehearsing the integration of response systems

Rehearsing responses using a combination of components can be more complex but is valuable for revealing issues that rehearsing individual components cannot. Rehearsals should be conducted weekly or monthly. For example:

- A small number of people acting as building occupants could attempt to obey voice announcements to avoid a person walking a planned route through the building, integrating rehearsal of voice announcements and tracking using video monitoring
- A person acting as a police officer could make contact from outside and attempt to reach a location inside the site, integrating rehearsal of procedures to deal with police with radio communications and control of the access control system
- A security control room operator could rehearse locating a person shouting, integrating rehearsal of a sound detection system with video monitoring.

Integrating more components of the response into a rehearsal increases the complexity but also increases the learning value.

Full response rehearsals

Conducting a full rehearsal of your response to a marauding terrorist attack is most valuable once your processes have been refined through component and integrated rehearsals. Whilst likely to interrupt the day-to-day business of your organisation, full response rehearsals offer an unrivalled learning opportunity for all participants and build the confidence of personnel. Inviting police to participate allows them to become more familiar with your site's response as well as rehearsal of external communication elements. It is recommended that full response rehearsals are conducted at least annually. Speak to your Counter Terrorism Security Adviser and CPNI adviser about how the police and CPNI can assist with full response rehearsals.

> *You can go so far with briefing documents, videos and lectures but when you put these people into safe and managed stress test situations that's where you start to see the real benefit of a full rehearsal.*
>
> *Many organisations shy away from this approach for fear of getting it wrong, upsetting people or other organisations, or are just overwhelmed with the planning required, and I understand all of this, but put the effort in, engage with law enforcement and your people, and the benefits will be obvious.*
>
> *The feedback and learnings from the live exercise drill we carried out were so valuable and could not have been gained in any other scenario, and certainly not from a desktop exercise.*
>
> *We are planning more. Why? Because our people asked for more training, because it tests our internal security procedures, capability and systems, and because it's not a work lesson, it's a life lesson*

Director of Group Corporate Security, Aviva

Working with stakeholders

Preparing for a marauding terrorist attack requires working with multiple stakeholders both inside and outside your organisation. Plan how:

- Stakeholders will be managed and coordinated
- Responsibilities will be agreed with each stakeholder
- Strands of work will be assigned
- Progress will be tracked
- Stakeholders will be held to account for delivering agreed strands of work.

Departments within your organisation

Planning and delivering the means to respond to marauding terrorist attacks will require input from many parts of your organisation including:

- Business continuity; your organisation should continue to function in the aftermath of an attack
- Communications; your organisation should inform personnel and visitors about security procedures, promote security measures and be prepared to engage with the media following an attack
- Corporate security; your organisation should monitor the risk of an attack
- Facilities management; sites designed to delay attackers must remain functional for business-as-usual and provision should be made for granting access to emergency services
- Guarding; your organisation's guard force should be able to detect an attack and have rehearsed their actions
- Human resources; personnel should receive training on what action to take in the event of an attack and their needs must be met in the aftermath
- Information technology; alerting people in the event of an attack and accounting for them in the aftermath will likely require technology as part of the solution
- Legal; possible responses to attacks including locking people in the building and overriding fire alarms must be lawful
- Physical security; personnel in the security control room have a key role in detecting and responding to an attack
- Procurement; your organisation may need to make purchases to implement site design changes and install new security systems
- Safety; your response to an attack should not put personnel at unnecessary risk.

Police and other emergency services

Local police and other emergency services may be able to work with you to optimise and coordinate your response plan. Organisations at high risk are likely to be prioritised and detailed support may not be available.

Key aspects for discussion are:

- Optimising the initial 999 call
- How to best facilitate police (providing site plans, access tokens and keys)
- How to meet the needs of emergency services in the immediate aftermath of an attack (for example providing extra bandages and tourniquets relevant to likely injuries).

For more detailed guidance on working with police and other emergency services see the supplementary guidance document *"Marauding Terrorist Attacks: Supplementary Guidance – Working with police and other emergency services"*.

Neighbouring organisations and landlords

Neighbours may be the occupants of surrounding units in a shopping area, other tenants in an office block or surrounding companies in a business district. Landlord organisations such as the owner of a multi-tenant office or a shopping centre are often responsible for security at entrances and other shared areas as well as front-of-house personnel such as concierges.

Collective response development

Preparation requires working with neighbouring organisations and landlords to develop collective plans for a coordinated response to a marauding terrorist attack. Attacks typically begin in areas that are not controlled by a single organisation and affect multiple organisations as terrorists maraud.

Your organisation should identify and engage with relevant organisations at an early stage. Coordinating provides opportunities for sharing work and increasing the power of your organisation's ability to detect an attack and respond effectively.

Coordination of daily security activity

Cultivating and maintaining a strong relationship with those responsible for day-to-day security at neighbouring sites means that your organisation is more likely to be alerted to suspicious activity or an attack outside your perimeter, improving the speed of your response. Consider how such alerting would operate in practice:

- Establish a simple means of communication such as a shared radio channel or a shared group on an instant messaging smartphone application

- Ensure the means to communicate are available to security officers at an appropriate level: those who are in a position to observe suspicious activity and those who are in a position to take rapid action.

Deterring attackers

Marauding terrorist attacks are highly likely to have been planned, with online and on-site research (termed 'hostile reconnaissance') conducted by the terrorists to choose a vulnerable target. Terrorists are deterred by strong security measures being promoted and demonstrated and when they are unable to gather reliable information about a potential target.

CPNI provides detailed guidance[13] on understanding and deterring hostile reconnaissance.

Promoting security measures

Promoting your site's security measures (without revealing operational details, such as CCTV, guard dogs and close cooperation with police) deters terrorists since they perceive that an attack would be more difficult to plan without detection and enact without failure. This may be achieved by:

- Advertising security capabilities on posters, signs and your organisation's website

- Drawing attention to security measures in place; for example using screens displaying video monitoring images at an entrance or painting security barriers in eye-catching colours.

Demonstrating security vigilance

If a terrorist does progress to conducting hostile reconnaissance on your site, demonstration of security vigilance provides a significant deterrent. This could be achieved by:

- Members of a motivated guard force proactively engaging in conversation with visitors to a site

- Receptionists, shop assistants, concierges, stewards and other front-of-house staff proactively engaging visitors as part of good customer service

- Moveable cameras (termed Pan-Tilt-Zoom, PTZ) being actively used to scrutinise a site.

Denying information

Making it more difficult for terrorists to gather information about your site increases the difficulty of their planning and makes them less certain that an attack would be successful. Methods of denying information include:

- Ensuring that site and floor plans, detailed site photographs and technical information about security measures (such as makes and models of security equipment) are not published on your organisation's website or those of partner organisations

- Where published sensitive information cannot be removed, publish alternative misleading information

- For sites where entry is restricted, obscuring entrances visible from public areas using architecture, plants, corporate branding or films to limit the value of online images and make observation from the outside more difficult

- Creating uncertainty by introducing unpredictability into security arrangements at a site; for example by varying the timing, type and location of security patrols

- In key areas where a terrorist is able to gather information, deploy visible security and proactive video monitoring to intimidate and detect.

[13] CPNI guidance on hostile reconnaissance: https://www.cpni.gov.uk/understanding-hostile-reconnaissance

Reducing the risk to personnel and members of the public

The design of a site, its security procedures and its technical capabilities can protect personnel. Relatively small changes to existing sites can have a significant impact.

Removing people from high risk areas

Crowds of people present a desirable target for marauding terrorist attacks. Consider how a site and its procedures can be designed to reduce the number of people in high risk areas such as entrances. For example, visitors to an office building could undergo rapid initial processing before being taken to a separate waiting area rather than remaining in the reception area.

Protecting front-line personnel

Organisations have a duty to protect all their personnel, including those with a security role. Front-line personnel such as guards, stewards, receptionists and concierges who typically work close to site perimeters and are responsible for raising the alarm are at greater risk from a marauding terrorist attack.

Where the risk is assessed to be high, consider:

- Locating personnel out of the direct line-of-sight of the entrance to make them a less obvious target
- Increasing the distance from a site entrance to where personnel are located (for example, the front desk in a hotel or office block) to provide more time for them to react
- Using architecture, plants, corporate branding or window films to reduce visibility of personnel from outside the building
- Locating static guards inside a building rather than outside in view, noting that doing so reduces the value of the guard as a visible deterrent and their ability to detect an attack
- Locating external guards behind a barricade to reduce the risk from an attacker armed with a knife
- Whether it is appropriate to issue personal protective equipment (PPE) such as body armour[14].

Screening at entry points

Screening bags and people at entry points may prevent weapons being smuggled inside the perimeter. Where possible, such screening is best conducted in a confined area to delay an attacker who uses force to overcome security officers. See CPNI's guidance[15] on screening for more information.

Understand site evacuation

Buildings are designed for evacuation in the event of a fire, not a terrorist attack. Fire evacuation plans may allow many minutes for people to leave a building or require a phased evacuation so that escape routes are not overwhelmed. When planning what people should do in the event of an attack, consider the risk of a crush if many people attempted to use an escape route. In some instances it may be safer for some people to seek shelter and hide rather than attempt to leave the building.

Further information

CPNI publishes guidance on physical security, terrorist attacks and more detailed advice on aspects of marauding terrorist attacks. For assistance specific to your organisation contact your CPNI adviser.

[14] CPNI guidance on body armour: https://www.cpni.gov.uk/body-armour-civilian-security-staff
[15] CPNI guidance on screening: https://www.cpni.gov.uk/screening-people-and-their-belongings-0

ANNEXE A: STAY SAFE: TERRORIST FIREARMS AND WEAPONS ATTACKS[16]

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

RUN

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

HIDE

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

TELL

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

- Location - Where are the suspects?
- Direction - Where did you last see the suspects?
- Descriptions – Describe the attacker, numbers, features, clothing, weapons, etc.
- Further information – Casualties, type of injury, building information, entrances, exits, hostages, etc.
- Stop other people entering the building if it is safe to do so.

[16] Annexe content from: https://www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat#stay-safe--terrorist-firearms-and-weapons-attacks

ARMED POLICE RESPONSE

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

OFFICERS MAY

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

You must STAY SAFE

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

Further advice

CitizenAID™ is a simple, clear teaching aid for immediate actions and first aid[17] for a stabbing, bomb incident or mass shooting. Building on Run, Hide Tell, this helps people understand what to do in the event of an attack.

[17] Note that since the information in this annexe was published a new guide on first aid, which should be used in preference to the first aid guidance in CitizenAID™ is available at https://www.gov.uk/government/publications/first-aid-advice-during-a-terrorist-incident

ANNEXE B: MARAUDING TERRORIST ATTACK PLANNING CHECKLIST

Preparing your organisation's response to a marauding terrorist attack requires many strands of work. This annexe provides a list.

Planning

- □ Make an individual responsible for managing delivery of the plan
- □ Establish governance: which individual at the highest level of your organisation is ultimately accountable?
- □ Assess and record the overall risk of a marauding terrorist attack
- □ Develop probable attack scenarios to use in planning
- □ Identify and engage with relevant departments inside your organisation
- □ Engage with emergency services via your Counter Terrorism Security Adviser
- □ Engage with landlords to coordinate planning
- □ Engage with neighbouring organisations to coordinate planning
- □ Plan how to manage stakeholders to assign strands of work, track progress and hold them to account

Developing and maintaining procedures

- □ Write an initial draft of procedures using internal workshops
- □ Use table-top exercises within your organisation to test and improve the effectiveness of procedures
- □ Use rehearsals within your organisation to test and improve components of the response
- □ Use rehearsals within your organisation to test and improve integration of response components
- □ Use table-top exercises with landlords and neighbouring organisations to test and improve the effectiveness of procedures and coordination
- □ Use rehearsals to test and improve a coordinated response
- □ Use table-top exercises with emergency services, landlords and neighbouring organisations to test and improve the effectiveness of procedures and coordination
- □ Use large rehearsals to provide as realistic test of all procedures as possible
- □ Review and update schedule established

Deterring attackers

□ Deny online information by removing website content on site layout and pictures

□ Deny on-site information by obscuring entrances

□ Promote security measures

□ Encourage security vigilance

Reduce the risk to personnel and members of the public

□ Reduce the number of people in high risk areas

□ Consider repositioning front-line personnel and equipping them with PPE and panic buttons

□ Introduce screening at entry points

Site layout

□ Establish escape routes and determine their capacity

□ Determine the time required for site evacuation and decide whether it is adequate

□ Introduce signs, landmarks and a logical naming system to assist orientation and navigation

□ Add locks to doors, zoned access control, door closers and blockers to delay attackers

□ Install blinds on internal doors and windows of rooms that may be used to hide

□ Ensure there are accessible rooms for people who are less able to escape to shelter and hide (with basic soundproofing if required)

Installing and configuring technical systems

□ Video monitoring covering thoroughfares and stairwells

□ Automated access control system configured for lockdown

□ Active delay systems tested

□ Public announcement system with external speakers

□ Handheld radio system with necessary coverage

Security Control Room

□ Constructed to withstand probable threats, such as a fire, gun or knife attack

□ Systems optimised for MTA response

□ Dedicated telephone line and handset for communication with police

□ Monitoring of news and social media

□ Integration and communication with landlord's and neighbours' control rooms

□ Consider an automated system to record actions of operators during an attack

Security Control Room operators

- □ Clear leadership and succession
- □ Response roles defined and assigned key tasks to be completed
- □ Comprehensive knowledge of response procedures
- □ Able to recognise an MTA from the security control room
- □ 999 call planned and practiced
- □ Communication between operators practiced
- □ Announcements written and practiced
- □ Radio protocol established and practiced
- □ Record-keeping procedures written
- □ Time for practice allocated
- □ Rehearsal schedule established

Front-line personnel: guards, concierges, stewards, receptionists, building facilities managers

- □ Able to recognise an MTA
- □ Knowledge of relevant response procedures
- □ Knowledge of site layout including escape routes and suitable locations for people to hide and shelter
- □ Competent on radio use and protocol
- □ Concise reporting to the security control room or police practiced
- □ Equipped with necessary PPE, panic buttons and/or radios
- □ Trained for first aid on likely MTA injuries
- □ Time for practice allocated
- □ Rehearsal schedule established

All personnel

- □ Awareness of the MTA threat
- □ Knowledge of relevant response procedures
- □ Familiarity with site layout include service stairs and lifts
- □ Aware where to run
- □ Aware where and how to hide
- □ Aware who and how to tell
- □ Understand lockdown as implemented at your site
- □ Understand risks of mobile phone use
- □ Familiar with likely announcements

ACRONYMS

AACS	Automated access control system
ADS	Active Delay Systems
ARV	Armed Response Vehicle
CBRN	Chemical, biological, radiological or nuclear
CCTV	Closed Circuit Television
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
CSO	Chief Security Officer
CTSA	Counter Terrorism Security Adviser
FCP	Forward Command Point
GDS	Gunshot detection systems
HART	Hazardous Area Response Teams
HM	Her Majesty's
JESIP	Joint Emergency Services Interoperability Programme
JOP	Joint Operating Principles
LED	Light emitting diode
LRF	Local Resilience Forum
MERIT	Mobile Emergency Response Incident Team
MTA	Marauding Terrorist Attack
MTFA	Marauding Terrorist Firearms Attack
NaCTSO	National Counter Terrorism Security Office
NCTP	National Counter Terrorism Policing
NHS	National Health Service
PA-VA	Public Address - Voice Alarm
PHE	Public Health England
PPE	Personal Protective Equipment
PTZ	Pan Tilt Zoom camera
RVP	Rendezvous point
SCR	Security Control Room
SMS	Short Message Service - Text
SOPs	Standard Operating Procedures
STAC	Scientific and Technical Advice Cell
TIC	Thermal Imaging Cameras
TCG	Tactical coordination group
VAW	Vehicle as a Weapon attack

GLOSSARY

Airsoft weapons	Airsoft guns are replica weapons used in sports and firearms training. They are essentially a special type of very low-power smoothbore air guns designed to shoot non-metallic spherical projectiles which are typically made of plastic or biodegradable resin materials. The pellets have significantly less penetrative and stopping powers than conventional air guns, and are generally safe for competitive sporting and recreational purposes if proper protective gear is worn.
ASCEND	CPNI's MTA work involves the repeated physical simulation of an MTA in a building environment – Project ASCEND. This involves subjecting a building population to a simulated attack and looking at factors that can either improve or reduce survivability before the arrival of an armed police response.
CitizenAID™	CitizenAID™ empowers the general public in situations of emergency and allows them to be effective in aiding the injured with medical support prior to the arrival of emergency services. It is comprised of simple and logical actions and is designed to guide the public to react safely and effectively as well as communicate correctly with emergency services. The powerful combination of organisation and treatment will save lives in dangerous situations.
Exercises	Allow personnel to validate plans and readiness by performing their duties in a simulated operational environment. Activities for a functional exercise are scenario-driven. A full-scale exercise would involve a live time simulation of a potential real event and involve multi-agency participation.
Hostile Incursion	As per MTA however the intent of those involved may be broader than terrorism.
Hostile reconnaissance	The information gathering phase by those individuals or groups with malicious intent, is a vital component of the attack planning process.
JESIP	A programme created specifically to further improve the way ambulance, police and fire and rescue services operate together on scene in the early stages of their response to major incidents.
Lockdown	Lockdown means locking doors and other physical barriers (such as turnstiles) to restrict entry to and/or exit from a site or one or more zones within a site. It is sometimes referred to as 'dynamic lockdown'.
Maglocks	The Magnetic lock or mag lock uses an electrical current to produce a magnetic force. When a current is passed through the coil, the magnet lock becomes magnetised. The door will be securely bonded when the electromagnet is energised holding against the armature plate.
Marauding	As defined by Cambridge Dictionary - Going from one place to another killing or using violence, stealing, and destroying.

GLOSSARY

MTA	Marauding Terrorist Attacks can take many forms. • 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, guns, pipe-bombs, petrol bombs or multiple weapons.
PA-VA	PA-VA systems are used for making announcements or providing public information and delivering automatic alarm and emergency messages. Public Address (PA) systems (often known as Tannoy Systems) and VA (Voice Alarm) systems provide a quick and simple means of direct and clear communication. Voice Alarm (VA) or Voice Evacuation Systems are used for delivering pre-recorded emergency messages.
Personnel	Used to describe any member of staff, contractor, visitor or other occupant to a building.
RUN HIDE TELL	The National Counter Terrorism Policing's Stay Safe campaign to advise the public how to respond if they are caught up in an firearms or weapons attack.
Security Control Room	The hub of a site's security, continuously receiving information from a range of security staff and systems. Many of the principles of an SCR can be carried over into an event or operations control room.
Security Management System	Integration of technical security systems, such as access control and CCTV, into a single management platform.
Security Fog	Thermally generated white smoke specifically used as a security measure. Current security smoke machines use glycol or glycerine mixed with distilled water to produce a dense white fog which obscures vision and presents a confrontational barrier to any intruders.
Situational Awareness	Being aware of what is happening around you in terms of where you are, where you are supposed to be, and whether anyone or anything around you is a threat to your security and health and safety.
Table top exercise	Discussion based sessions where team members meet to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios.
Vulnerable people	Those who may need to be provided with assistance or special arrangements made, such as children and people with health conditions or impairments.