WITHDRAWN

MARAUDING TERRORIST ATTACKS

Supplementary Guidance: Lockdown

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.

Contents

WITHDRAWN

INTRODUCTION

Intended audience

This document is most useful for:

- Physical Security Managers

- Security Control Room Managers

- Security Control Room Supervisors

- Training 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 document is supplementary to "*Marauding Terrorist Attacks: Making your organisation ready*", which discusses how your organisation can recognise an attack, take immediate action and facilitate the police.

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.

This document discusses a form of lockdown; locking doors to delay and frustrate attackers. Lockdown can be a highly effective way of reducing casualties but is not appropriate in all sites and all forms of attack. A poorly implemented lockdown can actually increase the risk to personnel and members of the public.

There is **no single solution** that is best for all sites and all forms of attack and therefore this document aims to provide information and points for consideration to assist organisations in their planning.

This document discusses:

- What lockdown means

- When lockdown can be beneficial

- Where and when lockdown may be impractical

- Planning whether and how lockdown should be used

- Ways of implementing lockdown

- Planning considerations for lockdown procedures

- Legislation to be considered when developing lockdown procedures.
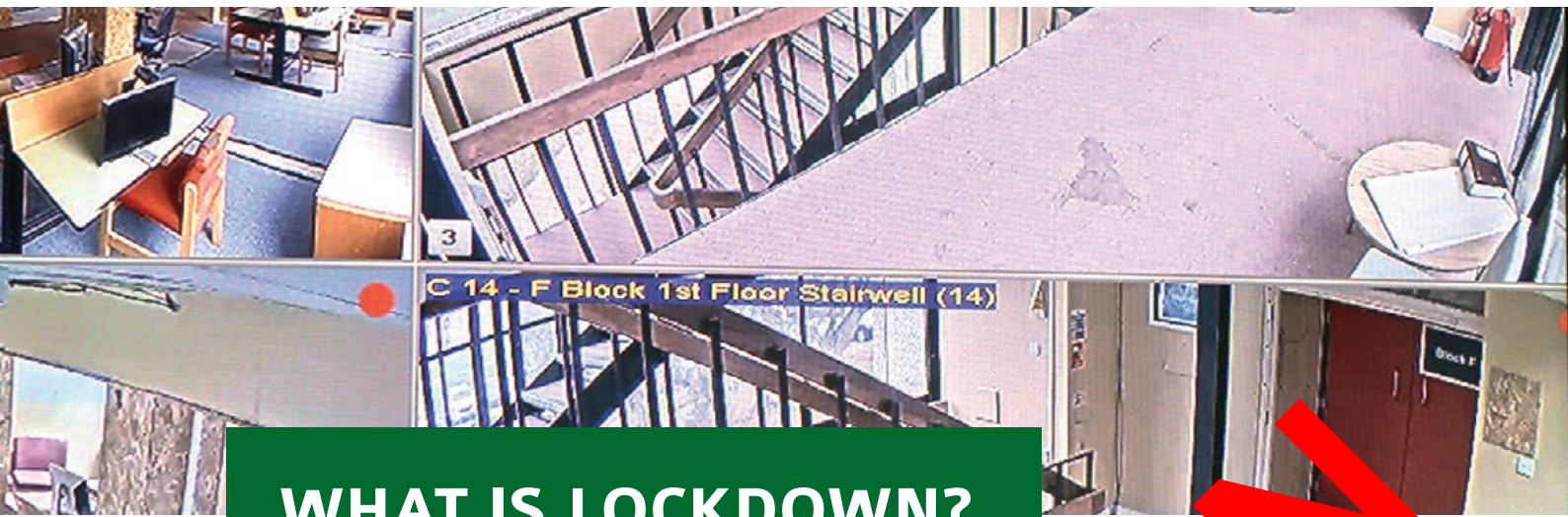
WHAT IS LOCKDOWN?

Instigating 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'.

Zones can be defined in any way including different buildings, different floors in a building or selections of corridors and rooms within a floor. For example, hospitals have wards to which only medical staff and in-patients have access. Shops typically have an area for a break room to which only staff have access.

Lockdown may be implemented in many ways and unfortunately there is no commonly agreed terminology. It is important when discussing lockdown with others to clarify exactly what is meant.

WHY INSTIGATE LOCKDOWN DURING A MARAUDING TERRORIST ATTACK?

Most deaths occur within the first few minutes of a marauding terrorist attack. Analysis of historic attacks, including the attack on London Bridge and Borough Market in 2017 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 attack from entering an area or deter them altogether.

The aims of lockdown are 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, lockdown is not appropriate for all sites and all forms of attack. A poorly implemented lockdown can actually increase the risk to personnel and members of the public. Lockdown is not 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.

Planning a lockdown

When deciding whether and how lockdown would function in the event of a marauding terrorist attack your organisation should consider:

- The impact a lockdown could have to reduce casualties

- The risks of a lockdown increasing casualties

- What form a lockdown would take

- What type of lockdown could be technically achieved for your site using its existing systems

- Under what circumstances lockdown should be instigated

- Under what circumstances lockdown should not be instigated

- Any investment required in infrastructure to enable lockdown.

Lockdown procedures should be developed, tested and refined to ensure that it will protect people as intended. Keeping records of what you are aiming to achieve with lockdown and why, how it will be implemented, procedures to be followed and the outcomes of tests and rehearsals will assist your planning and refinement process.

Ways of implementing lockdown

Lockdown is a term that covers a range of implementations depending on the capabilities available at a site and how an organisation has designed its procedures. This section discusses ways of implementing lockdown and raises points for consideration.

Centralised lockdown management

Centrally managed lockdown requires a security control room with systems that can remotely lock and unlock doors (such as an automated access control system[1] – AACS – operating electronic locks). Such systems typically also monitor whether the door is open or locked shut. Managing lockdown from a central location ensures that individual doors are locked and unlocked in a coordinated fashion.

Where lockdown management can be centralised, consider also allowing local control where front-line personnel are empowered to initiate lockdown at an entrance (for example, by operating a panic button) without the need to wait for security control room operators to act.

Instigating lockdown automatically with attack detection systems

It may be possible to configure your alarm system to instigate lockdown automatically without human intervention. For example, an alert from a gunshot detection system could activate door locks. Automated instigation may be particularly useful at sites without a security control room. Given the potential disruption caused by false alarms, only CPNI approved detection systems with a low false alarm rate are suitable.

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

Manual lockdown

Manual lockdown is the only option where there is no centralised capability to lock doors. Doors might be secured:

- By a person operating a nearby control (such as a panic button or the closing mechanism on a roller shutter)

- Using a key or thumb-turn to engage the locking mechanism

- Fitting a door-blocker or chain.

Manual lockdown is typically only practical where barriers may be locked quickly from a safe location. For example, a shutter on a shop front should be operated from the rear of the shop rather than requiring someone to push a button whilst standing exposed to advancing attackers at the entrance. It is very difficult to implement lockdown effectively where there are multiple doors with conventional locks and keys.

A coordinated approach for multiple entrances requires strong radio communication skills between personnel responsible for locking each entrance.

Partial lockdown

Partial lockdown means that only some doors are locked; typically at main entrances. Partial lockdown is often chosen where locking and unlocking doors is cumbersome (see section Manual lockdown) or exposes the person operating the lock to significant danger.

Partial lockdown keeps some escape routes open. It may be appropriate, for example, if attackers are inside the main area of a shopping centre the main entrance of a shop could locked but a loading-bay entrance at the rear could remain open to allow people in the shop to get away from the attackers.

Two-way lockdown

Two-way lockdown means all doors cannot be opened from either side. This may be where a key is required to unlock a door on both sides or where token readers, release buttons and break-glass switches (actually made of plastic) have been disabled for an electronic lock.

This method of implementing lockdown requires careful planning:

- A crowd may flee towards an exit they cannot use, potentially causing panic or a crush

- If attackers gain entry to the locked zone people will be unable to escape.

Allowing people to leave an area with one-way lockdown

One-way lockdown means that doors cannot be opened from one side but can be opened from the other. This allows people to leave an area but not re-enter it; for example, leaving an office to enter a stairwell in a shared-tenancy block. This type of lockdown is often a strong choice since it leaves escape routes available, making compliance with fire safety legislation more straightforward. However, there is a risk that people opening the doors will allow attackers to gain entry to the locked zone.

One-way lockdown may be achieved with mechanical locks using doors fitted with night latches or panic bars (such as would typically be fitted to fire exit doors). Most often, doors with electronic locks have release buttons on the inside to allow people to open the door. Automated access control systems often include functionality to disable the reader on the outside of the door, preventing attackers using stolen access tokens.

Note that whilst many doors with electronic locks can be opened by activating a break-glass switch on the inside, this typically leaves the door unlocked for the duration of the attack, potentially giving access to marauding attackers.

It is unrealistic to achieve one-way lockdown where opening a door requires security or front-line personnel to open the lock, for example a guard standing by a locked door with a key. The guard may need to leave the door to keep themselves safe or may be injured or killed, leaving other people no obvious method to open the door.

Instigating lockdown in specific zones

Instigating lockdown of individual zones within a site or a building can often be achieved with automated access control systems. However, a complex system of zones that are individually controlled is impractical to manage at the fast pace of a marauding terrorist attack.

Simple application of zonal lockdown can be useful. For example locking the perimeter of a building is the best option when all attackers are outside of that perimeter. With internal doors unlocked, people inside may move freely to safer locations such as higher floors. In this example, the locked zone comprises the whole building.

Losing power to electronic locks: fail safe or fail secure

When electronic locks lose power, their design and/or configuration can cause them to fail 'safe' or fail 'secure'.

'Safe' in this context refers to the safety of people where a means of escape, such as a fire exit, must be open and in most situations is the better option. However, this potentially compromises the integrity of lockdown, risking letting attackers inside.

'Secure' in this context means that the door will remain and locked in the event of power loss. It is typically used for storage areas containing valuable assets. Opening the door requires power to be restored or a key or access token. 'Secure' configuration can trap people and has implications for fire safety as well as marauding terrorist attacks.

Electrically locked doors often have a mechanism by which they may be opened from the inside in the event of a fire (typically with break-glass). In many installations, activating this mechanism will cause the lock to fail 'safe'; that is the lock will be released.

Cancelling lockdown by unlocking doors

Consider whether it would be possible to cancel a lockdown by unlocking doors. Where there is centralised control of door locks this is typically straightforward. However, front-line personnel who have manually locked doors may no longer be nearby.

Locking down lifts and escalators

Preventing lifts and escalators being used by attackers to progress through the site is ideal but typically difficult to implement. In practice it is only feasible where the building management systems and security systems are integrated. Otherwise it will represent another task to complete for security control room operators at a time when they are likely to be overloaded.

Doors and barriers for lockdown

Every door and security barrier on your site will delay the progress of an attack. For campus or other sites with areas of restricted access, dividing the site into zones using physical barriers such as turnstiles and security gates in combination with security walling and an automated access control system provides the best protection.

However, any barrier is valuable and may be used for lockdown, even those that are not designed for security use or are physically insubstantial. Lockable doors for offices and meeting rooms and even collapsible gates on shop fronts will delay attackers and may discourage them from entering an area altogether if they perceive the barrier to be too difficult to overcome.

For more information see CPNI's guidance documents:

- "Introduction to physical barriers to delay hostile incursions"

- "A guide to security doorsets and associated locking hardware"

- "A guide to security walling systems for the protection of important assets".

EMPOWERING SECURITY AND FRONT-LINE PERSONNEL TO INSTIGATE LOCKDOWN

Where security and front-line personnel are trained and your organisation is confident in their ability, CPNI recommends that those personnel are permitted to instigate lockdown, rather than waiting for a senior colleague, since a delay may cost lives.

Panic buttons on the perimeter of your site can enable guards, concierges and receptionists to instigate a site-wide lockdown or at least alert operators in the security control room to do so.

Monitoring lockdown integrity

The integrity of lockdown may be compromised if personnel, members of the public or attackers leave a door open or otherwise gain entry to a locked area. The results of this can be catastrophic if attackers gain access to an area that people cannot leave.

Whilst there are people within a locked area, it is essential that the integrity of the lockdown is continually monitored. Where it is not possible to use technical monitoring (such as intruder detection systems) it is strongly recommended that locked doors can still be opened from the inside to allow people to escape (one-way lockdown; see section Allowing people to leave an area with one-way lockdown).

Announcements and lockdown

Instigating lockdown may significantly alter the best course of action for personnel and members of the public. It is therefore crucial that people are aware that lockdown is in effect. Public voice announcements are the best way to achieve this.

There are many considerations for making useful announcements. For more guidance see the supplementary document: *"Marauding Terrorist Attacks: Supplementary Guidance: Announcements"*.

Preparing personnel for lockdown

Preparing personnel, including security and front-line personnel, for lockdown is at least as important as the technical implementation. For more guidance see the supplementary document: *"Marauding Terrorist Attack: Supplementary Guidance: Preparing personnel"*.

All personnel

All personnel should understand:

• How lockdown would function at your site

• How they should act during lockdown

• How they will know that lockdown has been instigated and cancelled (typically achieved using announcements).

Those who do not understand lockdown or are unaware that it is in effect may put themselves and others in danger by leaving locked areas and allowing attackers to gain entry.

Electrically locked doors often have a mechanism by which they may be opened in the event of a fire (typically with break-glass unit). In many installations, activating this mechanism will release the lock until it is manually reset, potentially allowing attackers to access an area where people are otherwise locked in. It is important ramifications of using these mechanisms to leave a locked area are understood.

Security and front-line personnel

CPNI has found that security and front-line personnel are often insufficiently prepared for lockdown. These personnel must understand:

• How lockdown would be function at your site

• The circumstances in which lockdown would be instigated

• How lockdown integrity would be monitored

• Who has the authority to instigate lockdown

• The importance of telling people that lockdown has been instigated

• How to make an effective announcement about lockdown

• The procedure for cancelling lockdown

• For common scenarios.

COMMON PLANNING CONSIDERATIONS WITH LOCKDOWN

Your organisation should carefully consider how lockdown should function in applicable situations.

People running towards a building

Consider what should be done if there is a large crowd of people running towards your site, perhaps where the cause is not clear. Should the people be permitted to enter your site in order to seek shelter or should they be locked out?

An attack in the proximity of your site

Early activation of a lockdown when a nearby attack is detected can undoubtedly prevent marauding terrorists from entering your site. Given that lockdown can disrupt day-to-day business, what area is considered nearby? What level of certainty is required that an attack is underway?

An attack that starts within your site

If an attack starts within your site, consider how lockdown should function. Should attackers be locked in a zone, potentially with victims, or should people be able to flee but terrorists allowed to maraud?

When people inside a locked zone want to leave

People may want to leave a locked zone, even when their safety is at risk if they do so. Should people be allowed to leave? If not how should they be handled? Also see section Legal considerations.

A crowd attempting to leave a zone via a locked exit

Being in the midst of an attack is highly stressful. People may ignore procedures and instructions. If a crowd were to attempt to leave using a locked exit, could and should it be opened? Are crushing injuries a risk if it remains closed?

Injuries and medical emergencies during lockdown

Attacks can cause life-threatening injuries or people may have a medical emergency (such as a heart attack) whilst in a locked zone. Should these people be carried out, leaving the locked area?

Fires during lockdown

If a fire is started whilst lockdown is in effect, should lockdown be cancelled to allow people to evacuate? What if there are marauding attackers outside the locked zones?

Fire alarms during lockdown

Fire alarms may be activated by people on the site, even if there is no fire. Some fire systems unlock all doors when the fire alarm is activated. What should people do when there is a lockdown and the fire alarm starts?

People outside a locked area

People may be locked outside an area, for example outside a building or in a corridor. Should doors be opened to let these people into a locked zone? What if attackers are close by and many people are already in the locked zone?

When a lockdown cannot be instigated

If technical systems fail or doors at key access points are propped open, preventing lockdown from being as planned, what action should be taken?

When the integrity of lockdown is compromised

If the integrity of lockdown is compromised by a door being forced or an attacker gaining entry, what action should be taken?

Facilitating access to police and other emergency services

When a lockdown is in effect, how would police and other emergency services gain access to locked zones when required?

LEGAL CONSIDERATIONS

Planning lockdown procedures must include consideration of relevant legislation as well as the detail of your organisation's insurance policies.

An organisation must protect its employees, other personnel and members of the public from a marauding terrorist attack but also from other risks such as a fire within the building. The best methods used to protect people in each case may be at odds; fire safety legislation exists to ensure people they leave a building quickly, whilst protecting them from marauding terrorists may require locking doors.

Conflicts can be resolved but must be carefully managed considering immediate threats to life and whether taking a particular form of action is likely to increase or reduce the number of lives lost. Consult with your organisation's legal and safety departments as well as your local fire service.

Ensure there are well-defined governance arrangements and that records are kept of the issues, the decisions made and the reasoning behind those decisions. Records will provide evidence to any investigations, coroner's enquiries and public enquiries and assist in defending against legal action; criminal charges or civil claims.

Health and Safety at Work Act 1974

Under the Health and Safety at Work, etc. Act 1974, employers have a duty to protect the health, safety and welfare at work of all of their employees. It also requires employers to protect people other than those at work (such as members of the public, volunteers, clients and customers) from risks to their health and safety arising out of, or in connection with, their work activities.

The legislation aims to protecting people from all risks, including marauding terrorist attacks and fires. Organisations must complete a risk assessment. This should consider how lockdown may reduce the risk to people in the event of a marauding terrorist attack as well as how the risks to people caused by lockdown and make any necessary adjustments.

Duty of care under common law

Under the common law, organisations have a duty of care to people who may be affected by their activities. Individuals may sue for damages using the civil law if they are injured as a result of another person's negligence.

The injured person must show that the defendant had a duty to take reasonable care towards them, and they have suffered the injury through a breach of that duty. The injured person must also show that the injury was a foreseeable result of the breach of the duty.

Building Standards Regulations

Building standards regulations include 'Approved Documents' that provide guidance on how to comply with legislation, although are not legally binding. Different legislation and different building standards regulations apply in different parts of the UK. In practice, the fire safety requirements are similar and include provisions for means of escape, including where locks are used.

For England and Wales, Approved Document Part B sets out the requirements for Fire Safety, which includes provisions for safe means of escape and fire detection and alarm systems. Section 3.7 states "measures incorporated into the design of a building to restrict access to the building or parts of it should not adversely affect the fire safety provisions".

It is possible that there may be conflicting requirements between implementing lockdown and complying with building standards regulations. Discuss requirements with your (part of local councils, though also available privately in England and Wales).

Table 1: Legislation relating to Building Standards Regulations in the UK

COUNTRY	LEGISLATION GRANTING POWER TO MAKE BUILDING STANDARDS REGULATIONS
ENGLAND	Building Act 1984
NORTHERN IRELAND	Building Regulations (Northern Ireland) Order
SCOTLAND	Building (Scotland) Act 2003
WALES	Building Act 1984

Regulatory Reform (Fire Safety) Order 2005
The Fire Safety (Scotland) Regulations 2006
The Fire Safety Regulations (Northern Ireland) 2010

These pieces of legislation, applying in different parts of the UK, require minimum fire safety standards and risk assessments. All contain a clause stating that emergency doors "must not be locked or fastened that they cannot be easily and immediately opened by any person who may require to use them in an emergency".

Your organisation's plans for lockdown may conflict with this requirement. It is essential to discuss potential plans the Enforcement Authority (as defined in the relevant legislation) as well as the fire service.

Human Rights Act 1998

Article 5 of the Human Rights Act 1998 protects the right not to be deprived of liberty or freedom unless it is in accordance with the law.

In practice this legislation is only relevant where doors are locked such that individuals are unable to leave a building or site. Organisations may prefer one-way (also called exit-only) lockdown for this reason.

Further information

For more information contact your local police force Counter Terrorism Security Adviser (CTSA).

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
SOP	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 material. 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 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 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'.
Mag lock	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 vehicle weapons.
PA-VA	PA-VA systems are used for making announcements or providing audio 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 and 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 Police's Stay Safe campaign to advise the public how to respond if they are caught up in any 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 organisation 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.