MARAUDING TERRORIST ATTACKS

Supplementary Guidance – Are you ready?
Testing and Exercising

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, manufacture, 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

INTRODUCTION

Intended audience

This document is most useful for:

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

Scope

Marauding Terrorist Attacks (MTAs) are fast-moving, violent attacks where assailants move through a location aiming to find and kill 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.* It builds on the information provided in the supplements titled:

Marauding Terrorist Attacks: Lockdown

Marauding Terrorist Attacks: Physical Barriers To Delay and Discourage Attackers

Marauding Terrorist Attacks: Active Delay Systems (ADS)

Marauding Terrorist Attacks: Announcements

Marauding Terrorist Attacks: Preparing Personnel

Marauding Terrorist Attacks: Working with the police and other emergency services

It consolidates the information provided in the other guidance documents in relation to the tasks that need to be considered and provides guidance as to how you can to establish the readiness of your organisation to deal with an MTA.

This document discusses:

- The need for a plan
- Types of readiness testing
- Internal roles and responsibilities
- Working with external stakeholders
- Assuring your plan
- Scenarios for exercising

This document does not discuss:

- Testing and Exercising of the overall site security plan

DEVELOPING A STRATEGY AND PLAN

CPNI research has shown that the majority of sites will have MTA response plans in place, but few adopt a holistic approach that requires the development of a detailed plan that sets out how the MTA plan should be Tested and Exercised. This plan should be developed in a way that builds from simple daily tasks to completing occasional complex multi-agency live exercises. The intended outcome of this plan is to confirm a site is ready to respond to an MTA.

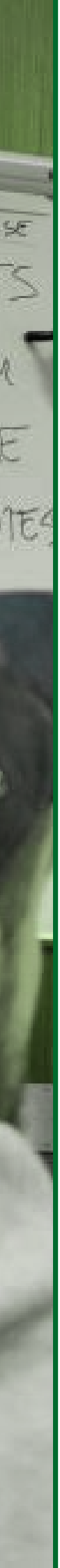
The MTA guidance document suite highlights numerous tasks to be considered or undertaken in the development of an MTA response plan. These range from simple single action tasks to major decisions on the procurement of complex security systems. It is important to establish that all aspects of delivery planning have been completed and a response plan is in place and remains ready to be activated at no notice. You can only be confident that your site is ready to respond to an MTA when you know that:

- Plans have been robustly checked and validated
- Audit processes are in place to check equipment remains in place and works
- Security staff remain competent and are present in the right numbers
- Plans and risk assessments are subject to ongoing review and repeatedly exercised.

This document will help establish that all the tasks relevant to your site have been identified and considered; and that your site is ready to meet the challenges of an MTA.

Due to the scale and complexity of the tasks that need to be completed it is unlikely that this can be achieved without the creation of:

- A site security strategy that includes the need to address the risk of an MTA
- An MTA delivery plan and
- An MTA operational response plan.



The site security strategy will set out the aims and objectives of protecting your site against security threats considered to be of high risk and should include a section on preventing and responding to MTA threats. Senior management endorsement of the strategy will provide tacit approval to the tasks that need to be completed and the commitment of the necessary resources. It will define where accountability for the delivery of the plan lies and determine the level of assurance required.

The delivery plan will set out the detail of each task to be completed and set targets as to when each task should be completed, provide an audit of planning, decisions and activity that will be available in the event of any subsequent enquiry.

The response plan will determine your organisations response to an attack. It will help determine the actions of all personnel to a number of reasonably foreseeable scenarios.

An important part of both plans will be the assessment that the site is as ready, as can be reasonably expected, to deal with an attack. CPNI recommends the use of the framework offered by the *Protective Security Management Systems Guidance and Checklists* to provide assurance that there is a viable response plan and your site is ready to implement it. The remainder of this document will provide guidance on the detailed steps your organisation must complete to make sure your site is ready.

It is important to make certain that the whole organisation buy into the security strategy and plan. The plan must become an accepted part of the way the organisation works, in the same way that fire drills are an accepted part of working in any large site. Achieving an environment where the delivery of security testing and exercising is accepted by all is likely to be evidence of a successfully embed security culture[1]. Time will need to be spent explaining to personnel the benefits of testing and exercising.

Every site will conduct testing and exercising to one degree or another. The intention of this document is to make sure that within the broader testing and exercising that is taking place, in relation to both safety and security risks, sites consider how they are able to prepare their site for an MTA. MTA testing and exercising should be in addition to other testing and exercising that is already taking place, rather than reducing the effort towards other risks. It is intended that whilst this document is focused on preparing sites for an MTA, the information set out will also improve their readiness to respond to a wide range of risks.

A regular review should be conducted of the threat and risk to your site. This assessment should consider changes in terrorist attack methods, the development of new security capabilities, changes in site operations and the profile of your organisation and neighbours. This will ensure plans are focussed on the most likely attack scenarios. CTSA's can assist with this guidance or use the ACT App.

1. See https://www.cpni.gov.uk/developing-security-culture for more information on the development of a positive security culture.

TYPES OF READINESS TESTING

As described above there are two clear phases that need to be considered.

During the delivery period project management methodology will be used to confirm tasks are either on track or have been completed and technical systems evaluated to confirm their readiness for use. Additionally, Testing and Exercising will be used to:

- Validate plans and the concept of operations. Confirm policies and standard operating procedures (SOPS) are in place
- Confirm the suitability of technical security equipment before procurement decisions are made. Ensure that technical security equipment is robustly tested prior to going live and where necessary effectively integrates with other technical systems
- Confirm that staff are appropriately trained and briefed
- Test roles and responsibilities between both internal stakeholders and external partners.

The second phase is the operational response phase, during which it is necessary to introduce tests of all aspects of the plan. This will range from daily testing to ensure that equipment is working correctly and in the correct location, through to running complex multi-agency live play exercises to prove the enduring readiness of all the response capabilities.

The readiness of the site will be established through a variety of assessment processes. These will start looking at confirming the correct resources are in place and technical equipment works. They will build through a series of layers, during which the level of detail that is being tested and exercised will increase. As each layer is completed there will be an increasing level of confidence that the correct people, products and processes are in place and ready to deliver the plan.

Figure 1, below illustrates the multiple layers and the subsequent sections describe the activities and tasks that will be involved within each layer. The tasks described are intended to establish a site's readiness to respond to an MTA but will also cross over to other threat areas.

Figure 1: Multiple layers of Testing and Exercising

Checklists

The completion of checklists to ensure:

- Planning / Delivery tasks have been completed
- Operational phase:
  - That the right number of appropriately trained and qualified security staff are in place (each shift).
  - Technical equipment such as Public Address and Voice Alarm (PA-VA), CCTV cameras, ADS etc are working correctly (daily).
  - That a radio interrupt facility is available and working correctly to allow the key Security Control Room (SCR) decision maker to ensure effective command and control. Facilitating emergency messaging, without fear of blocked airwaves.
  - That security equipment such as grab bags for the emergency services are in the right location (weekly).
  - That security equipment is correctly maintained and serviced at the stipulated intervals. Making certain that contracts are in place to provide ongoing servicing and a response to equipment failures.
  - That messaging systems used to alert staff and neighbours of any incident have contact details updated as changes occur to personnel.

During the operational phase, checklists may need to be completed at the start of each shift, daily or weekly. The frequency will depend on the criticality of the function and the likelihood that its status will have changed.

A reporting process will be needed to make certain that any deficiencies are reported and quickly rectified.

Practice and rehearsal

Practice and rehearsal should be undertaken after training has been delivered and continue as required. Practice is likely to be focused on individuals, whilst rehearsals will involve a team or multiple teams working together.

It is important that the use of technical security equipment is practised and then the use of the full capability rehearsed. For example, SCR staff should practice how to use the PA-VA system. This will allow them to practice using the equipment by:

- Switching the equipment on
- Delivering announcements
- Practicing switching automated announcements off and cutting in with a live announcement.

Practice would also allow operators to consider how they would use automated announcements, pre-scripted announcements or compose their own announcements to meet different circumstance or multi-hazard threats.

Teams, working together, should then rehearse the full use of the system. This could involve being presented with a short scenario that would run through all of the functions of the equipment and test their ability to compose and deliver suitable announcements. The announcements would need to be monitored to make certain they were audible, easily understood and relevant to the scenario they were dealing with.

Depending on the equipment and SOPs being practised and rehearsed they could be delivered:

- During silent hours when the site is empty
- On a system that does not interfere with live operations of the site but can still be monitored by a supervisor or
- During live operations but with careful monitoring in place to bring the incident to an end if a live incident is identified.

Walkthroughs

These can be used in a number of ways. During the planning phase they can be used to validate proposals for the use of technology or introduce specific processes. For example, if the use of security fog is being considered as an active delay system then at an early stage a small group of key functional leads could be pulled together to consider how an activation would impact on their areas of responsibility.

They could be run on a weekly basis as a short group discussion for SCR staff on a single aspect of different MTA related scenarios. For example, this could be scripted to involve a radio call from a member of the security team, who has spotted a group of suspects arriving wearing large coats in warm weather and suspected of carrying weapons. The discussion would involve the identification of the immediate tasks required and who is responsible for completing each one. Alternatively, it could involve a discussion on the immediate actions required if a Gunshot Detection System (GDS) is activated.

Walkthroughs are part of continual training for team members and are designed to check team members familiarity with plans and SOPs.

They should be used to prepare senior decision makers for their role in either tabletop exercises or live exercises. A walkthrough will provide a more comfortable environment for them to initially run through plans.

Finally, they can be used in a similar way to bring together members of different organisations to discuss how they would work together to respond to a scenario. It is particularly important that they should include the police, allowing them to discover how a site operates. A walkthrough could become part of a familiarisation visit for police firearms teams.

Tabletop exercises (TTX)

At a strategic level TTXs will increase the awareness amongst senior leaders for the need for the very rapid making of decisions in the event an attack is discovered. They should be used to emphasise the need for decision making to be delegated to the SCR supervisor. Security policies should then reflect the need and reasons why decision making has been delegated.

In relation to specific actions TTXs will be particularly useful to validate MTA response plans. It is likely that a range of scenarios would need to be discussed to cover likely situations that a site could face. For example, the scenarios can be used to consider:

- When either evacuation or lockdown should or should not be instigated and the importance of actively monitoring their progress.
- The impact of different types of ADS being activated.
- The impact of MTA planning on fire safety plans.

They should be used for bringing together representatives from different organisations to examine how they will work together to deal with an attack and show how their plans are able to effectively work together. They are likely to be particularly useful to consider how responsibilities shift as an attack moves through different sites or from the grey space between sites, into a single site. There is a need for organisations to make certain their plans are tested against those of neighbouring sites, exploring and exposing the role of the police to those unfamiliar with working with them will be fundamental. Scenarios should move through all phases of an attack. They should include exercising the need for a coordinated approach to crisis communications and the post incident investigation when a site could remain closed down as a crime scene for an extended period.

Live exercises (LiveX)

A live exercise is likely to take many months to plan, be expensive, resource heavy and involve considerable disruption. It should be run as the culmination of a period of testing. It should be used as the final level of testing and validation of plans. They could be used to focus on a particular theme within a plan or test the complete plan. This would include the initial discovery of an attack, making the initial call to the police and handing over a site to them and cover both crisis and consequence management and through into the recovery phase.

It is likely that a LiveX would only be held on an annual basis. Consideration should be given to the involvement of the emergency services in the exercise. However, where they are unable to provide resources it is recommended that exercises are still conducted.

Each organisation involved should set out and agree their objectives in running such an exercise. It is important that each organisation has the potential of getting an equal benefit out of the exercise.

It will also provide an opportunity to test how crisis communications should be managed. This could include how social media is used by organisations to communicate both internally and externally, and also monitor the impact of an attack on the site, neighbours and the wider surrounding area.

Frequency

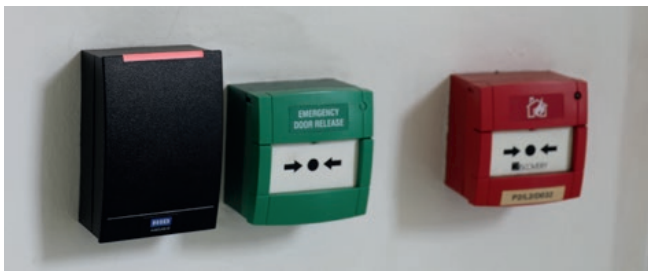
During live operations all types of testing should be used. Building from simple checklists through to Live Exercises, they should all be part of a continuing cycle of exercising that will help develop staff competence and provide ongoing opportunities to practice their roles. They will allow for the ongoing testing of well-established procedures.

At sites such as international airports, major sporting stadia or oil refineries there are a number of licencing and regulatory requirements to conduct exercises. Whilst there is no requirement for the exercising to cover an MTA, these events can be used to provide opportunities to exercise the MTA response plan.

There is likely to be significant interest in live exercises. They create an opportunity to use the overt emergency services capabilities present for the exercise as the focus of deterrence communications. They will provide a highly visual illustration of the significant planning and combined resource capability that will be bought to bare against potential attackers.

Crossover with fire evacuation drills and other emergency planning

There is a considerable crossover with the requirement to undertake fire evacuation drills that prepare personnel to respond to a fire and the need to involve personnel in rehearsing their response to an MTA. The routes used and how people are managed are likely to be fundamentally the same. It is important that all personnel are encouraged to respond to any drill or exercise in an energetic manner and not consider it to be an unnecessary activity. Time should be spent considering how the learning from each drill or rehearsal can benefit other areas of planning and how internal communications can be used to explain the importance of all staff involvement.



During the response to an MTA consideration should be given as to the need to evacuate occupants away from the site. This is likely to mean that the assembly points used in a fire evacuation drill are unsuitable, due to their proximity to the site, for use as part of the evacuation from an MTA. Personnel should be advised to disperse right away from the site. This could be to pre-arranged locations some distance from the site, with each team in a building having its own location to go to, so preventing the creation of secondary targets. People should only return to the site when it is declared safe to do so by the police.

It is important that evacuation plans are as simple as possible and consideration should be given to minimising the number of options for each site.

If the police require witnesses to gather to provide statements, this will be at a location that they have declared safe.

Learning and review.

At the end of every type of test or exercise time should be spent identifying the lessons that have been learnt and then deciding how the plan could be improved and then tracking the delivery of tasks that have been identified. A full record should be kept of all the issues raised, progress tracked, and how each is eventually closed down.

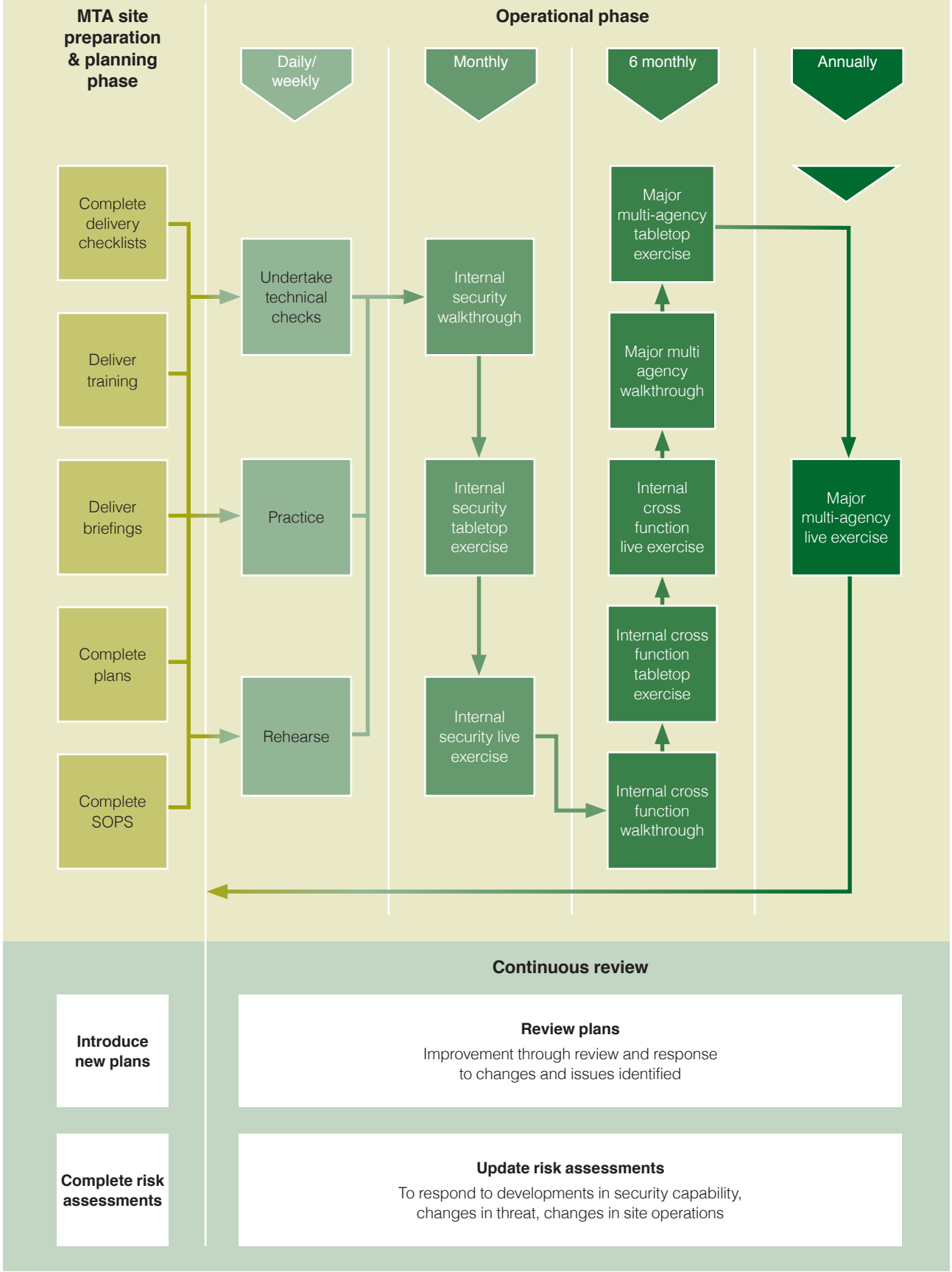
The outcome

The outcome of the “bottom-up” approach that is described is that as each element of the plan is being developed its viability is being proved and then accumulatively tested with every other element. This approach will increase the likelihood of the overall plan working and each element being fully integrated. The overall concept is illustrated in the diagram overleaf.

Each site should consider how they can use the information provided in this document and the detailed testing and exercising structure provided in the diagram. This should link into other aspects of site safety and security testing and exercising that the site be undertaking. The effort put into testing and exercising against any security threat should be determined by the site safety and security risk assessments, with the focus of the majority of testing and exercising undertaken against the threat scenarios that have been identified by the risk assessments as being of the greatest risk to the site.

Testing and exercise

MTA testing and exercising cycle of continuous review



ROLES AND RESPONSIBILITIES WITHIN THE ORGANISATION

Staff at every level should be aware of the importance of using all types of testing and exercising to develop their own skills. They must understand that the testing and exercising opportunities provide a safe environment for them to make mistakes and learn. The main objective of testing and exercising will generally be to test the plan rather than the individual. However, individuals will be put under pressure as they are faced with different and unexpected scenarios to deal with. For this reason, all those involved as "players" in responding to scenarios should be prepared and have been provided with the necessary training or familiarisation with the plan being tested before they participate. This will increase the likelihood that they will succeed in their part and focus the scrutiny on the plan and not the individuals involved.

Time should be spent considering how all staff involved in a responding to an MTA are provided with the opportunities to test and exercise their part. The level of involvement will depend on their role. All staff should be provided with the appropriate training and opportunities to practise. It may be difficult to involve all those deployed in key roles in large scale exercises. For example, a site may have a number of control room teams and duty managers. It will be difficult to involve all the individuals concerned in a major exercise due to the shifts they work. Opportunities to participate in major exercises should be allocated across teams and individuals in a way that maximises the available opportunities and the numbers involved. Learning from such events should then be shared between teams.

Consideration should be given as to how the following groups are included:

Security personnel and key front line staff that are deployed in vulnerable areas taking immediate action to respond to an immediate threat.

SCR staff responding to the information they are presented with. They will be responsible for assessing information coming into the control room, prioritising the tasks and taking action. This will include operating CCTV, detection systems, making radio and telephone calls and making announcements.

SCR supervisors who will need to gather all the information available to them, make decisions and direct the actions of their team in the SCR and out on the site. They will need to be continually developing their situational awareness, making certain they are assessing the information available to them and reviewing their decisions

in response to the situation that unfolds in front of them. Where appropriate, they should be in no doubt that they have been empowered to make important decisions that require immediate decisions to be made.

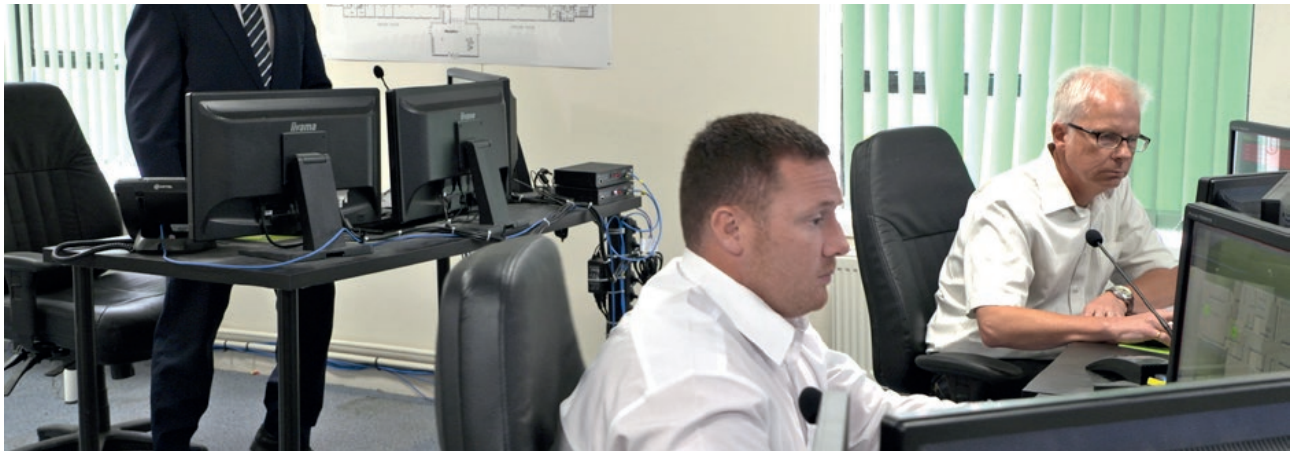
Duty managers may have cross functional responsibilities for all aspects of site management which are likely to include both the safety and security of those within the site, their day to day role may not be within security. It is therefore important that they are fully aware of all the security capabilities available to them and have a clear understanding of how important rapid decision making will be within the SCR and the need for the SCR supervisor to be empowered to make the necessary decisions.

Senior managers are unlikely to be readily available to take a direct role in the response to an incident. Their role should be focused on supporting those making fast-time tactical decisions and considering what additional resources could be used to assist them and focusing on the strategic level decisions they need to make, directing their energy on the recovery from the incident. **They should avoid stepping in and involving themselves in operational decision making, unless their support has been sought or is clearly required.** This should include considering the welfare of their staff and others involved, protecting the interests of the organisation, overseeing the use of crisis communications with the media and others and launching a recovery plan in response to the specific incident that is being dealt with.

ALL STAFF should be provided with opportunities to get involved in exercising their response to an MTA. This may involve exercising both evacuation plans and putting a building into lockdown or practising their response to announcements made from the SCR. Organisations are encouraged to consider using security exercising for all personnel in the same way that they should undertake at least one fire drill per year.

Consideration should also be given as to how other internal departments/functions need to be involved in all aspects of testing and exercising. For example, this may include those responsible for:

- Internal and external communications
- Human resources
- Fire evacuation planning
- Facilities management



WORKING WITH STAKEHOLDERS

The need to identify and work with external stakeholders is fundamental to the validation of plans and proving the overall readiness of the site and all the organisations involved.

Emergency Services

Sites will have different levels of engagement with the emergency services. Some sites forming part of the Critical National Infrastructure (CNI) or requiring a regular police presence, e.g. a shopping centre or football stadium may have a formal agreement with the police about the provision of services paid for by the site. Where this is the case it is likely that the police will be more directly involved on a day to day basis on a wide range of policing and security issues. There may also be a statutory or regulatory requirement for joint emergency planning. If this is not the case engagement should take place with the emergency services and other responders. Your Local Resilience Forum (LRF)[1] will be able to support the creation of links to key responder groups but also provide links to other sites where MTA testing is taking place. Sharing of plans with LRF sub-groups or Police Civil Contingencies or local Police Planning Offices will create better opportunities for joined up working and collaboration.

The level of participation of the emergency services for each site in supporting testing and exercising will be a local decision for each of the emergency services organisations involved.

They will need to prioritise their availability to support each organisation. This is as a consequence of their capacity and commitment to multiple other tasks.

Each organisation is likely to share the same high level objective of making certain they can work effectively together to respond to an MTA. It is important that each organisation has an opportunity to achieve their own organisations specific objectives, these may not be the same as the other organisations involved. For example, for site security managers it may be important to spend as much time dealing with the period of the exercise prior to the emergency services arriving as it is once they arrive at the scene and take the lead for managing the response.

1. https://www.gov.uk/government/publications/the-role-of-local-resilience-forums-a-reference-document

Grey space and sites of multiple occupancy

Many attacks will be launched from and may first come to notice in the grey space.

The grey space may be described as:

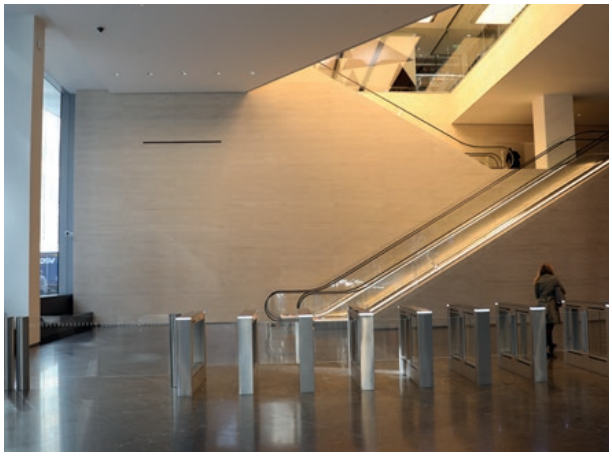
- The area outside a site and may be either a public or private space.

For areas outside a site, it is likely that they will be undefended and potentially only covered by limited CCTV monitoring. Security personnel are unlikely to deploy into this area. However, there is a reasonable likelihood that attacks may be discovered within this space.

In contrast sites of multi-occupancy may have a number of security regimes operating in isolation within the same site. This could mean that there is more than one SCR and security team operating within the same site. This could easily cause confusion for the emergency services who may receive calls from more than one.

Sites of multi-occupancy may be described as:

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



This issue will become more complex where different security providers or facilities companies need to work together, and their existing security contracts may not permit the tasks that are now required.

Testing and exercising should be used to bring together those who have an interest in their local grey space or operate within a site of multi occupancy. This will allow them to consider how they would work together to identify and respond to an attack. It will be important that this looks to develop the roles and responsibilities between each of the organisations involved. Where possible one site, with the agreement of the others, should take control of the grey space or common areas in a multi-occupancy site, this should be based on thorough discussions and practical analysis of which site can most effectively monitor that space. This should include understanding how each site uses both CCTV and security patrols in these areas. Consideration may need to be given to the legal issues associated with one organisation leading the response and determining the actions staff of another organisation should take.

Each organisation must consider the impact their actions may have on the occupants of adjacent sites and how they should work together to respond to an attack. This may include considering how an evacuation ordered at one site may impact on the flow of people already evacuating from a neighbouring site.

Detailed consideration will need to be given to how adjacent organisations communicate between each other and the emergency services. Establishing how they can use a common radio channel or other mass communication methods, such as texting. It will be important that announcements that are made from one site to another are coordinated and compatible.

It will be important to spend time developing relationships with neighbouring organisations and to consider how they can work together to develop coordinated plans. Once joint plans are developed, they should be tested by running multiple scenarios, this will establish they are viable and that staff from different organisations are able to work effectively together. This will need to be done in relation to many aspects of emergency planning, be it for fire, an MTA or another contingency plan where an evacuation may be required.

EVALUATION AND ASSURANCE

Once an MTA response plan has been developed and decisions made as to how it should be tested and exercised, consideration should be given as to the need for additional assurance that will confirm:

- The plan is viable
- The methods for establishing overall readiness are thorough
- The actions and decisions taken by those involved in testing and exercising are appropriate.

The CPNI Protective Security Management Systems Guidance and Checklists provides a framework for the assurance of protective security planning and delivery.

Assurance can be obtained by using internal peer review of the plans as they are developed. As outside agencies are involved, they may also provide an independent assessment of the plan's viability. Local police and other representatives of the Local Resilience Forum (LRF) engaged in the planning may be able to provide assurance as a result of their training and experience of dealing with other sites.

Colleagues responsible for the security of other sites within your own organisation will be able to provide assurance of all elements of the plan and the actions of site security staff. They are also likely to benefit from considering how they can improve their own plans as a result of examining your plans.

Heads of security from neighbouring sites should consider the benefit of working together to ensure that each other's plans are integrated. This will also provide an opportunity to share good practice and provide an assurance capability against each other's plans.

Consideration should be given as to how other forms of independent review could assist in providing assurance that the plan is sound, the assessment of readiness is thorough, and the people involved are well prepared. This could be provided by introducing an independent review by a security specialist who has not previously been involved in developing the plans. Suitable specialists should be an accredited security professional who is either a Registered Security Engineer and Specialist (RSES) or a Chartered Security Professional (CSyP).

Consideration could also be given to the use of covert penetration testing or red teaming. Such testing is likely to fall more broadly against the overall security plan. It could be used to test against:

- Hostile reconnaissance
- Search and screening
- Access control arrangements
- The availability of information to support attack planning.

SCENARIOS

The site security risk assessment should be used to identify the most reasonably foreseeable attack methods that are likely to be used if their site was attacked. Scenarios should then be developed around each attack method and these then used to test and exercise the plans that have been made. The risk assessment should also be used to identify the most likely types of layered attack, this may involve a variety of different attack types that all come together in one single attack, such as a vehicle as a weapon (VAW) attack taking place outside the site and developing into an MTA. They should also consider how an attack could lead to multiple hazards manifesting themselves as part of the attack. This could include fire alarms sounding, a fire being confirmed or areas becoming overcrowded as people respond to the developing situation.

A list of potential scenarios that should be developed for your site is provided at table1 below.

Table 1 - Potential Scenarios to be developed

- Response to hostile reconnaissance
- Response to a firearms, knife, fire as a weapon or multi layered attack
- An accident outside a site which transpires to be a VAW and develops into an MTA
- Response to a gunshot detection system alert
- Suspects being identified by security personnel – using CCTV to track their movements
- Attack detected in neighbouring building/area
- Making announcements in response to an attack being discovered
- Evacuating building occupants, including limiting the available routes due to the location of the attack or initiation of ADS
- Staff told to hide (including a staff member in a wheelchair who needs to hide)
- Initiation of lockdown and then a decision to release lockdown
- An entrance route that, for an unknown reason, becomes overcrowded due to people running from an adjacent site and trying to enter your site
- Deployment of ADS
- Calling the police
- Police deploy
- SCR needs evacuating
- Post incident requirement to establish staff are accounted for
- Test business continuity if site not available
- Mass messaging system tested with suitable test messages.

Examples of detailed scenarios

There are multiple scenarios that can be developed. They should consider a range of different types of MTA and responses. The scenarios should be developed from the site risk assessment and initially focus on the scenarios considered to be of highest risk.

The following sets out two examples of scenarios that could be developed for you site. They focus on the use of the PA-VA system and making announcements, and communication between the site of the attack, the emergency services, tenants and neighbouring businesses.

Multiple other scenarios should be developed to support the specific circumstance of your site.

Scenario 1

The first scenario focuses on the use of the PA-VA system and making announcements. The attack is initially identified by use of a GDS. If a GDS is not available at your site, the scenario should be adapted to your site. The initial identification could be changed to be by either a member of the security team calling the SCR or a crowd rush detected on the CCTV.

This scenario is intended for an office block or other site that can be easily locked down and the personnel working there are familiar with the options for responding to an MTA.

A site has a PA-VA system that is controlled from the SCR. There are three SCR operators deployed to each shift in the SCR.

On the given day three operators were on duty and present in the SCR.

It is during the time the site is open for normal business on a weekday.

A GDS system activates and an automated announcement is made telling occupants the location of the gunshot and that the building is under armed attack.

- *What are the actions of the SCR?*

Next inject – 1 minute later

Three suspects have been seen on CCTV to enter the front of the site and start firing automatic weapons towards the reception desk.

The attack is tracked on CCTV and the SCR supervisor makes the decision to go into lockdown.

- *What announcements would the SCR now make?*
- *What other actions would they take?*

Next inject – 2 minutes later

The attackers are still seen in the reception area and are shooting at anyone in the area and trying to force the security doors into the main site.

- *What announcements would now be made?*

Next inject – 2 minutes later

A fire alarm sounds and a fire is confirmed to have broken out and seen to have taken hold in the front reception area. The attackers can still be seen in the reception area.

- What announcements would now be made?

Next inject – 5 minutes later

The police arrive on site and enter the SCR. They ask for all remaining occupants to be told to stop moving through the building and lie on the floor with their hands on their heads.

- *What announcements would be made?*

Consider if the following have been achieved

For this example, when considering the quality of the response, reference should be made to the MTA Supplementary Guidance: Announcements

Checks of the usability of the system

1. Does the location of PA-VA equipment in the SCR support use by all operators?
2. Can it transmit both live and automated announcements?
3. Can automated announcements be triggered by an SCR operator?
4. Can automated announcements be overridden?
5. Can fire alarms be turned off to allow voice announcements to be made?
6. Check that messages can be heard in common parts of the site and adjacent to entrance points
7. Are there different zones that announcements can be made to? Is there a local approach or a whole building approach?

Checks on operator capability

8. Do SCR operators know how to turn on automated announcements to announce that venue is under attack by armed attackers?
9. Do SCR operators know how to turn off fire alarms and make voice announcements?
10. Do SCR operators know how to turn off automated announcements and make voice announcements?
11. Do SCR operators know how to override/ turn off GDS automated announcement

Automated announcements

12. Were automated messages switched off after a suitable time?
13. Were the correct automated announcements used?
14. Did the automated announcements meet the circumstance given?
15. Are the right automated announcements in place to inform:
    - Lockdown
    - Evacuation
    - Triggering of GDS
    - Activation of ADS

Actions of front line security staff

16. How did front line staff respond to the announcements?
17. Did their actions reinforce the messages made in the announcements?

Response to given scenarios

18. Did SCR operator instruct site occupants that attackers are in a particular part of the site in a format that occupants will recognise the part of the site concerned?
19. Did SCR operators give specific instructions around a scenario and instruct site occupants to move out of a specific part of the building and either evacuate or hide?
20. Did the SCR operator make ongoing announcements, providing updates on situation to building occupants?
21. Did the SCR operator provide announcements to support the implementation of lockdown?
22. Did the SCR operator update on the lockdown situation and consider if an evacuation was required? Did they provide the building occupants with clear instructions?
23. Were announcements made about the police having been called?
24. Did the SCR Operator follow instructions given by the police as to what announcements to make?
25. Were messages repeated at the right frequency?

Outcome

26. Did the equipment work?
27. Was an operator assigned to deliver the tasks?
28. Were the SCR personnel able to make a rapid assessment of the situation and decide what announcements to make?
29. Were messages clear?
30. Was the content of announcements easily understandable?
31. Did messages deliver the intended outcome?
32. Did those listening understand the threat they face?
33. Was it clear how many attackers are involved?
34. Was it clear where the attack is taking place?
35. Were announcements:
    - Authoritative
    - Concise
    - Specific
    - Repeated
    - Frequent
    - Reassuring
36. Make sure they are not:
    - Rambling
    - Vague or confusing
    - Including the word firearm or phrase security incident
    - Helpful to attackers
    - Announcing arrival of the police
    - Instructing exit through a specific exit
    - Using unnecessary words
    - Making continuous announcements

Scenario 2

The focus of the second scenario is to check communication with the emergency services, shops/businesses within the centre and neighbours. It is based on a crowded place, with a knife used as the weapon.

The site is a large shopping centre in an inner city area. In the immediate surrounding area are further shops, offices and hospitality and leisure venues.

On the given day three operators were on duty and present in the SCR.

Its early evening, the centre is open and busy. There is a multiplex cinema immediately next door to the centre, which is currently in the middle of a number of screenings.

A radio call is received into the site control room from a member of the site security team saying that there are a large number of people running through the centre towards him/her, but they don't know why.

- *What are the initial actions of the SCR?*
- *Did they contact anyone at this stage?*
- *What were the messages?*

Next inject – 1 minute later

A suspect is seen on CCTV waving a knife towards a group of people who are watching him. A person is lying on floor, apparently injured.

- *What initial announcements would SCR make (consideration being given to the size of centre and where incident is taking place)?*
- *Who would they communicate with?*
- *How would they communicate?*
- *What are the key messages?*
- *What other actions would SCR Take?*

Next inject – 1 minute later

The suspect is seen on CCTV to charge towards members of the public who are between him and the doors out to the street. They rapidly move out of the way and he continues to run into the street stabbing out at members of the public. Some have clearly been stabbed.

- *What are the priority messages from the SCR now?*

Next inject 2 minutes later

Police and ambulance teams arrive at the scene. The police halt the attack

- *What are the key messages from the SCR now?*

Consider if the following have been achieved

Check who, how and when communications were made to:

1. The shopping centre tenants
2. The police and other emergency services
3. The public in the shopping centre
4. The cinema
5. The public outside the shopping centre
6. Other neighbouring businesses
7. Site staff

How did communications change as the attack developed?

How did they change as the attack was stopped?

8. Were communications clear?
9. Was sufficient information passed to each group?
10. Were images shared with any stakeholders?
11. Were announcements clear and correct information given
12. Were mass communication systems used?
13. Was social media used?

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 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.