Protecting Crowded Places: Design and Technical Issues

Revised March 2014

HM Government

Protecting Crowded Places: Design and Technical Issues

Revised March 2014

Produced by the Home Office in partnership with the Centre for the Protection of National Infrastructure and the National Counter-Terrorism Security Office.

ISBN: 978-1-78246-387-0

Contents

Introduction

1.01 The UK faces a significant threat from international terrorism. The current assessed threat level to the UK can be found on the MI5 website[1] where more information can also be found on what threat levels mean, who decides the level of threat and how the threat level system is used. Whilst there have been attacks against well protected targets around the world, experience shows that crowded places remain an attractive target for terrorists who have demonstrated that they are likely to target places which are easily accessible, regularly available and which offer the prospect for an impact beyond the loss of life alone (for example, serious disruption or a particular economic/political impact).

Purpose of the guide

1.02 The purpose of this guide is to give advice about counter-terrorism protective security design to anyone involved in the planning, design and development of the built environment from the preparation of local planning policy to the commissioning, planning, design and management of new development schemes through to detailed building design. Whilst it draws largely on good practice examples from England and refers to legislation that applies to England, this guide will be of interest to the devolved administrations.

1.03 This guide will also be of interest to designers/architects, town planners, engineers, highway engineers and police Counter-Terrorism Security Advisers (CTSAs) and Crime Prevention Design Advisors (CPDAs). It will also be of interest to those who have responsibility for ongoing management and maintenance of public spaces and streetscapes and to conservation officers in the context of development in Conservation Areas.

1.04 The guide gives practical advice on how best to incorporate counter-terrorism protective security measures into proposed new development schemes whilst ensuring that they are of high design quality. The advice that is set out is generic and cannot address the plethora of varying circumstances and degrees of risk which apply to different facilities. Consideration should first be given to the relevance of such measures and whether or not they can be appropriately achieved through the planning system in any particular case. If so, the measures should be appropriate, proportionate and balanced with other relevant material considerations.

1.05 The aim of the guide is to equip the reader with a better understanding of the links between the counter-terrorism dimension of crime prevention and the built environment, so that reducing the vulnerability of crowded places to terrorist attack can be tackled in an imaginative and considered way. The guide is not a manual to be applied by rote or a substitute for using skilled designers.

Application of the guide

1.06 Whilst this guide is not primarily intended for those enhancing existing sites with counter-terrorism protective security measures, so called ‘retro-fitting’, the same principles apply and the document provides useful reference to the recommended approach to, and the specification of, counter-terrorism measures. Similarly, creative and innovative design will have a role when considering the integration of counter-

terrorism measures as part of new proposals in sensitive historic areas and sites which, for example, may not be able to utilise the typical solutions offered. See section entitled ‘Historic Environments’ (paragraphs 4.07 - 4.14) for specific retrofitting design advice when considering counter-terrorism measures within historic environments.

1.07 While crowded places have been identified as a particular focus for this guide, the principles can be considered and applied to a wide range of new development schemes, for example commercial and industrial sites.

1.08 In addition to this guidance there are specific requirements that need to be taken into account when considering designing-in counter-terrorism protective security measures at transport facilities, such as airports, railways and ports. It is therefore important to check that these requirements, which in some cases are legally binding, have been complied with as part of the design process. When considering designing-in counter-terrorism measures into new or existing transport facility developments, please contact the Department for Transport[2].

1.09 This guide is also only aimed at the higher and further education elements of the education sector. It does not apply to schools. Counter-terrorism issues are addressed within the broader security and emergency planning work rather than as a discrete issue in schools. It is important that schools keep pupils safe from threats to their well-being, and schools do this very well, keeping their premises secure. They are generally controlled environments, unlike universities and colleges, where any member of the public can gain access to the campus.

What is a crowded place?

1.10 As defined by the UK’s counter-terrorism strategy (CONTEST) “crowded places include shopping centres, sports stadia, bars, pubs and clubs which are easily accessible to the public and attractive to terrorists. Crowded places remain an attractive target for terrorists who have demonstrated they are likely to attack places that are easily accessible and which offer the prospect of impact beyond the loss of life alone”. Our objective as set out in CONTEST is ‘to improve protective security for crowded places’. The Government has ensured owners and operators have access to high-quality guidance, provided by the police and others, so they know what steps to take to reduce vulnerability to, and prepare for, terrorist attack. Public vigilance, the work of the police and of the security and intelligence agencies all contribute to make crowded places safer, as does other work under CONTEST such as reducing terrorist access to explosive precursors.

Terrorist methodology

Why counter-terrorism protective security measures are needed

2.01 In 2010 the Government published the *National Security Strategy*[3] and *National Security Risk Assessment*[4] which identify and prioritise the full range of risks to national security. International terrorism is shown as a Tier One Priority and experience shows that crowded places remain an attractive target for terrorists.

2.02 Attacks by international terrorists are more likely to involve the use of improvised explosive devices, of which the three main types are, person-borne (suicide devices on the person or bag carried device), vehicle-borne (which may be suicide or non-suicide devices), hand delivered or placed devices (non-suicide devices initiated typically by timer or remote control). When suicide tactics are employed they allow terrorists to deploy their device (person or vehicle-borne) at the optimum time and place to maximise the impact in locations where a non-suicide device might be discovered.

2.03 But terrorists are innovative and their methodology can be expected to change over time. Other means of terrorist attack (such as chemical, biological, radiological, or firearms) are also possible and protective security measures can help make a difference (see paragraph 2.09 below).

An explosion

2.04 An explosion is normally the sudden and violent release of energy caused by an extremely rapid chemical reaction which turns a substance (usually a solid or liquid) into a large quantity of gas (generally at high pressure and temperature). This reaction is typically measured in microseconds. The expanding gas is produced rapidly and pushes the surrounding air out in front of it creating a blast wave.

2.05 When an explosion occurs at ground level there are several effects created that cause damage and injury. The effects will be dependant on the power, quality, quantity and location of the explosive material deployed and are outlined in paragraph 2.07.

Improvised explosive devices

2.06 Improvised explosive devices (IEDs) range in size from person-borne small containers, rucksacks and suitcases to larger devices, such as those that are vehicle-borne. The latter may be borne by a variety of vehicles, ranging from bicycles and motorcycles through to large goods vehicles (LGVs).

Explosive effects

2.07 The six basic effects of an explosion are:

• blast wave: the blast wave is a very fast moving high pressure wave created by the rapidly expanding gas of the explosion. The pressure gradually diminishes with distance but can reflect and diffract around structures;

• fire ball: the fire ball is created as part of the explosion process and is local to the seat of the explosion. It is generally associated with high explosives;

• brisance: this is the shattering effect, is very local to the seat of the explosion and is generally associated with high explosives;

• primary fragments: these are parts of the device or its container (including the vehicle if vehicle-borne) which have been shattered by the brisance effect and are propelled at high velocity over great distances;

• secondary fragments: these are fragments that have been created by the blast wave. Typical secondary fragments include glass, roof slates, loose gravel, timber and metal. These can travel considerable distances; and

• ground shock: this is produced by the brisance effect of the explosion shattering the ground local to the seat of the explosion, i.e. creating a crater. The shock wave resulting from the crater's creation then continues through the ground.

Causes of fatalities, injuries and damage from blasts

2.08 The main causes of fatalities, injuries and damage as a result of an IED are:

• direct weapon effects including primary fragments, lung blast damage, thermal burns and ear drum rupture; secondary fragments such as glass, spall (flakes of material that are broken off a larger solid body) and other objects thrown by the blast;

• collapse causing crush injuries; and

• post-event falling debris (including glazing, façade, internal walls etc) damaged equipment and damaged infrastructure which can hinder the speedy evacuation of buildings.

Chemical, biological, radiological materials and firearms attack

2.09 The issues arising from chemical, biological and radiological (CBR) materials are various and complex. However, in essence, the potential problem will be less onerous the more the threat can be excluded from a facility. Key mitigation involves good access control into critical facilities and the protection of air intakes within buildings and its distribution thereafter.

2.10 Whilst attacks using firearms will be countered by armed police or the military, protective security measures such as those detailed in Annex A may help mitigate the impact of an attack, and should be considered at the design stage of a development. Although this guidance is focused specifically on building designs, tight access control involving an effective staff pass system and the regular training of staff using well-developed response/emergency plans is important in supporting technical solutions in mitigating the impact of a terrorist firearms attack.

Further information on these proposed measures are provided in Annex A.

• Project Argus and Project Griffin (see Annex F), as well as protective security advice published by NaCTSO, help raise awareness of the business community to the terrorist threat and the value of recognising those involved in hostile reconnaissance. This helps to disrupt potential attacks and to produce important intelligence leads.

2.11 Project Argus also provides guidance to the business community to help plan their response to a terrorist attack using firearms[6]. This includes;

• how you would communicate with police, staff, visitors, neighbouring premises. (including using, for example, public address systems);

• the key messages you would give them in order to keep them safe;

• how you would secure key parts of the building to hinder free movement of the terrorists (including use of enhanced doors and locks to withstand entry from armed intruders and provide cover for those caught up in an attack);

• incorporating a firearms attack scenario into your emergency planning and briefings; and

• testing the plan annually.

More detailed advice about actions people caught up in a firearms attack can take can be found on the NaCTSO website. Businesses can also obtain further information from their local police Counter-Terrorism Security Advisers.

The challenge of blending counter-terrorism protective security measures with urban design principles

3.01 When considering appropriate protection against terrorist attack, a challenge for designers and planners is the application of urban design principles (see paragraph 3.05) whilst at the same time incorporating counter-terrorism protective security measures. Meeting this challenge will involve taking account of the following:

• care to avoid an oversensitivity to risk. This can result in bland and standardised places – it is important to retain or insert positive features that attract people to spaces;

• to retain and attract people to places, which are also safe and secured against some types of terrorist threat, will always involve a combination of approaches, tailored to local conditions and special features. The design aim is a respect for locally distinctive places which involves resources to identify these characteristics, as well as sensitive responses. The result may be a combination of some standardised components, some invisibly integrated components based on conventional traffic management and streetscape designs (such as structurally enhanced bus shelters, lamp columns, benches or cycle racks) and often some elements of purpose-designed solutions, for example incorporating public art or locally important features;

• the presence of physical measures in the streetscape to prevent hostile vehicle access or proximity to a site need not preclude pedestrian access, or diminish the look and feel of an open and permeable area; and

• integrating protective security measures into a public realm that is designed to be inclusive and remains accessible to all.

3.02 Each site is different and there is no “one size fits all” solution. Different sites present unique challenges and considerations that will result in bespoke solutions, including those that meet the needs of the disabled.

3.03 Typical measures that help to deter, detect and delay a terrorist attack are set out in the table below. They are grouped into five key counter-terrorism design principles: better blast resistance; better building management facilities; search and screening, better traffic management and hostile vehicle mitigation measures; and better oversight. “Designing-in” counter-terrorism protective security measures from the outset will benefit those involved throughout the development process, from concept design through to planning approval, as well as those who will use and visit the places and buildings. These benefits will best be achieved through collaborative working and broad engagement with all parts of the community. The benefits include:

• it is more cost effective to “design-in” protective security measures from the outset of a scheme;

• there are aesthetic and functional benefits to designing-in counterterrorism measures at the concept stage rather than later on. The building or place should be attractive, accessible (see ‘Urban design principles’ in paragraph 3.05 below) and work for those that will use and visit it.

Counter-terrorism protective security measures should not impose upon the overall style and intention of a place;

• considering counter-terrorism protective security measures at the design stage helps ensure measures work together and do not displace vulnerabilities elsewhere in a new build;

• strengthening a building or place by designing in counter-terrorism protective security measures offers wider business continuity benefits in the event of a terrorist incident; and

• incorporating good counter-terrorism protective security measures is also good crime prevention.

Generally, good counter-terrorism protective security measures will support other measures intended to reduce other types of crime.

3.04 In seeking to deliver these benefits it is important:

• that appropriate counter-terrorism protective security measures should be proportionate to the risk of terrorist attack to which the building/place is exposed; and

• that costs for new protective security measures should fall where the responsibility for those measures lies.

Table 1: typical counter-terrorism protective security measures

Counter-terrorism design principles	Examples of measures
Better blast resistance	• External barriers or a strengthened perimeter to prevent a penetrative (ramming) or close proximity (parked or encroachment) attack; • Use of building materials which reduce the risk of fragmentation including blast resistant glazing and structural design which reduces the risk of building collapse; and • Install doors and locks which are better able to withstand entry from armed intruders and provide robust ground floor facade material, which together will help to provide cover for people caught up in a firearms attack.
Better building management facilities	• Entrance arrangements which resist hostile entry; • The separation of general heating, ventilation and air conditioning systems for entrance areas, delivery areas and mailrooms from those occupying the main occupied spaces • Air intakes that are in a secure area and above the first floor level; • Hazardous material stores that are at a safe distance from the building and; • Communications systems (e.g. public address systems) installed to pass on advice to those caught up in a firearms attack.
Better traffic management and hostile vehicle mitigation measures	• Structural measures that prevent access to, or close proximity of, unscreened vehicles to the building or space; and • Measures that reduce the speed of vehicles approaching the site or its defences, like bends or chicanes
Better oversight	• Clear lines of sight around a building • Absence of recesses on the façade or elevations of a building; • Uncluttered street furniture • Well maintained and managed litter-free building surrounds that reduce the opportunity for suspicious hidden items and suspect activity to go unnoticed; • CCTV and security guarding to provide formal oversight; • Orientating the building so that it overlooks public space and neighbouring buildings to support informal oversight by those who use and visit the location; and • Well managed access points and reception facilities that offer less opportunity for intruders to go undetected and may deter them from taking further action
Better search and screening measures	• Provision of sufficient space at vehicle entrances to allow proportionate screening of vehicles (and their occupants / loads) as and when the threat dictates; • Provision of sufficient space at pedestrian entrances to allow proportionate screening of people and their possessions as and when the threat dictates; • For higher risk sites, consider off-site screening of deliveries and mail.

Urban design principles

3.05 Good urban design creates places which maintain sustainable and attractive environments which people want to use. The principles of well-designed places and spaces can be recognised as those with:

• character - a place with its own identity;

• continuity and enclosure - a place where access for the public is clearly identified;

• quality of the public realm - a place with attractive and successful areas accessible to the public;
• ease of movement - a place that is easy to get through but where routes do not compromise security;

• legibility - a place that has clear image and is easy to understand;

• adaptability - a place that can change easily; and • diversity - a place with variety and choice. Urban design principles are described more fully on the government planning portal[7].

Public and private space: design, management and maintenance

Integrating counter-terrorism protective security measures into public realm design

4.01 Physical measures are effective in helping to prevent unscreened vehicles from getting in close proximity to a site in need of protection. The physical measures can be localised to the site or encompass a wider area and be combined with other public realm aspirations, such as environmental enhancements, pedestrian, cycle and/or public transport priority. The further that a potential Improvised Explosive Device (IED) can be separated from a building, the less critical the building's form and fabric becomes.

4.02 When considering how to achieve vehicle-free areas around sites and the installation of security infrastructure into streets and spaces, it is important to look at the transport and movement implications over a wider area or district. This is to help ensure that there is not a concentration of vehicle restrictions or displacement, and that streets and spaces are not unnecessarily congested with security infrastructure.

4.03 Where features are introduced which restrict vehicle approach, mitigation measures to address the needs of disabled people may be necessary. For instance, people with impaired mobility may find it difficult to walk even relatively short distances - the introduction of vehicle setting down points and regular resting places and seating helps to ensure that the environment remains inclusive. Accommodating the requirement to make reasonable provision for disabled people to gain access to and use the building (as described in Part M of the Building Regulations) such as vehicle setting down points, will be necessary.

4.04 Where counter-terrorism protective security measures are being integrated into predominantly residential streets, refer to *'Manual for Streets'*[7,8] and the accompanying *'Inclusive Mobility'*[9] document for further guidance on designing accessible environments. As well as setting out good principles for street design, the manual sets out a hierarchy of users and transport modes. Greater emphasis is placed on integration of pedestrian and cyclist needs in street design, with vehicular traffic being of secondary priority.

4.05 Street design that aims to limit unscreened vehicular access to vulnerable target areas or structures may not necessarily prevent normal street usage. Well designed barriers to prevent vehicle attack aspire to be unobtrusive and blend into the natural streetscape, as well as relating well to the existing landscape. For example, ensuring permeability for pedestrians may mean that the best solution is a comprehensive scheme including traffic management and footway widening as part of the integrated solution.

4.06 Counter-terrorism protective security measures that monitor public safety and provide a visible security presence need not be significantly different from measures aimed at crime prevention. Further information about good street design and designing-in counter-terrorism measures can be found at Annexes A and B of this guide and case studies at Annex C. Information about sources of advice on

counter-terrorism protective security and crime prevention can be found at Annexes D and E.

Historic environments

4.07 The advice in this section concerns incorporating counter-terrorism protective security measures into existing historic environments where there are special considerations. This means the advice is concerned with retrospective fitting of measures rather than designing measures into new developments from the outset, although common principles apply.

4.08 Counter-terrorism protective security measures have two key impacts on the historic environment: visual and physical. For temporary works, minimising physical impact is more important and reversibility is a key principle. However, for more permanent measures, both visual and physical impact are important.

4.09 In conservation areas, World Heritage Sites, sites within the setting of listed buildings or scheduled monuments and registered parks and gardens, it is necessary to consider impact on character and on historic fabric, including ground surfaces and underground archaeology. In areas where historic burials are anticipated, special precautions may be necessary and appropriate consent obtained. Works within the curtilage of a listed building or involving the building itself may require listed building consent in addition to normal planning consents.

4.10 Close liaison with the local planning authority's conservation team will be essential. In some instances, the local planning authority may also want to involve English Heritage, particularly when dealing with scheduled monuments, higher grade (II and I) listed buildings, major alterations to Grade II listed buildings and large developments in conservation areas.

4.11 When seeking advice from English Heritage, contact the relevant regional office. However, if more specialist advice is required on security issues in the historic environment, this can be provided by English Heritage.

4.12 It is often difficult to assess the blast resistance of a historic building and even more difficult to improve it by reinforcement. This is often dealt with by putting the secure boundaries as far away as possible from the building shell, a preferable option to attaching security measures to historic building fabrics.

4.13 Technology, such as CCTV cameras, needs sensitive positioning to minimise visual and physical impact. 'Technology' generally has a limited life and works to accommodate it need to be completely

reversible. Applications for planning permission and/or listed building consent will need to be accompanied by more detailed plans than usual. For example, by specifying methods of fixing where works would affect the historic fabric.

4.14 Where it is necessary to prevent vehicles from getting close to a facility, it may be possible to introduce a physical barrier into the landscape design. If there is valuable underground archaeology, shallow excavation or surface mounted/pinned barrier solutions will often be favourable. In especially sensitive locations, it may be better to prevent uncontrolled vehicular access to the surrounding streets completely, displacing the traffic management works to a less sensitive location.

Management and maintenance of public space

4.15 In considering integration of security measures into streets and spaces, the long-term management and maintenance issues could usefully be taken into account at the earliest stages. The long-term financial and administrative commitment required to keep the measures effective and attractive need to be allowed for in appropriate planning, highway and management agreements. Other key issues are:

• long-term commitment is important – in maintaining the quality of what was designed at the outset to ensure it remains both attractive and functional. It is equally important to ensure that any counter-terrorism design elements have not been compromised, for example by poor management or maintenance or by repairs and alterations. In combining these needs, it helps shape better budget planning of resources;

• formal agreements - management and maintenance plans (comparable to those for public and private buildings in terms of facilities management or estate management, and for public and private streets and spaces) can benefit from being contained in specific written documents. These can be aligned with local strategic plans and open space/public realm strategies. Where management plans contain security sensitive information,

access will need to be restricted. Having specific management and maintenance plans ensures continuity, even after initial commissions or staff appointments are replaced. Changes may also occur to the legislative frameworks of, for example, traffic orders or regulations that may require agreements to be updated;

• consult widely - local consultation has always been the key to ensure that the priorities of key interested parties and local populations (including the disabled community) as well as other user groups (e.g. tourists/nearby workers, and visitors) are taken into account. Broader engagement and collaborative working will result in better design solutions and can have significant management and maintenance of public space benefits, minimising conflict with those who use the space;

• cover costs – adequate and reliable sources of funding for maintenance are essential. Long-term management and maintenance (perhaps with replacement/refurbishment projects spanning several financial years) require consideration of long-term funding. The costs can be allowed for in appropriate Section 106 (Town and Country Planning Act 1990) and Section 278 (Highways Act 1980) agreements to ensure that the wholelife and management costs are covered by those benefiting from the implemented measures;

• high quality and well maintained space is a key strategic requirement and objective of nearby interested parties (e.g. property owners, prominent tenants, land owners);

• site staff roles. There is a strong case for putting trained staff into spaces as they can provide a range of services within the space e.g. interaction with the community using the space and carrying out of specific tasks such as locking up or checking for damage/maintenance tasks. Where this presence is onstreet, it is best if trained personnel are clearly identifiable as working for the appropriate highway authority. Where this function is being carried out by non-highway authority personnel, an appropriate contract and service level agreement needs to be agreed with the highway authority;

• continuity and training in the workforce is helpful, as is the need to ensure that staff have development opportunities; and

• there is scope to benefit from working with private and public partners, experts and interested parties. Examples include: local community groups to manage spaces long-term or possibly (with private sector partners) to provide income generation opportunities; or informal arrangements for others to use space (for example, encouraging police to use spaces to exercise their horses or to use local facilities such as cafes) to add to informal surveillance.

Private demise

4.16 The level of security and access afforded to the public when entering onto private land will usually be at the discretion of the owner. However, there will be circumstances where a Local

Planning Authority (LPA) may wish to secure a particular level of access or security provision that is appropriate for the proposed use of the land by an applicant. Such measures can be made the subject of conditions on a planning permission, or be the subject of appropriate obligations in a related Section 106 Agreement.

4.17 In the case of crowded places, it may be appropriate to ensure, through appropriate conditions on a planning permission, that the proposed layouts allow for secure entrance areas where security screening (people, vehicles and mail/deliveries) and control can be best carried out with minimal risk to the least number of people. Information on the specification and implementation of search and screening measures is available on the CPNI website. A public available standard has been developed by the Home Office Centre for Applied Science and Technology which gives guidance and recommendations for checkpoint security screening of people and their bags and possessions, for non regulated applications[19]. It will also be appropriate in other circumstances to ensure that unencumbered pedestrian public access is maintained and that the security measures proposed are proportionate to the use (i.e. the right of access by the public to areas of public realm accessible from the highway). This is particularly relevant where security measures restrict vehicular access and there are managed security measures requiring trained personnel. Appropriate obligations in a Section 106 Agreement can be used to ensure that the level of restriction is commensurate with need and that the public are not unduly

restricted in accessing important amenities such as shopping.

Personnel security

4.18 Where access control measures are incorporated into a building, or installed to control access to a wider area of streetscape, the personnel controlling those measures must be trained and trusted.

4.19 Personnel security is an important aspect of protecting crowded places. It comprises a system of policies and procedures which seek to minimise the risk of staff or contractors exploiting their legitimate access for unauthorised purposes. Those who seek to exploit their legitimate access are termed 'insiders': insider activity comprises many forms from minor theft through to terrorism.

4.20 Robust personnel security helps an organisation employ reliable people, minimises the chances of staff becoming insiders, detects suspicious behaviour by employees and resolves security concerns when they emerge.

4.21 The Centre for the Protection of National Infrastructure (CPNI) provides advice and guidance on personnel security which can be obtained from the CPNI website[10]. In particular CPNI guidance offering practical personnel security advice for HR and security managers is available[11].

4.22 Where there is a need to manage access to the public highway or security related infrastructure on the public highway, this will need to be carried out under the control of the Highway Authority. As well as carrying out this function, it may also be appropriate for the authority to contract with others to provide this highways management service. For example where an 'Access Only' Traffic Order restricting vehicular access to a shopping area is managed by security personnel employed by local businesses. This is most appropriately done through the use of a Section 278 Agreement setting out the level of training, service and monitoring required by the service provider and the financial arrangements, in order to ensure that those that benefit from the service pay the full costs.

Closed circuit television (CCTV)/ oversight

4.23 CCTV can help clarify whether a security alert is real and identify suspect activity, for example potential terrorist planning (reconnaissance) activity. It can also be vital in post-incident investigations, but only if the images are good enough to identify what happened over the timeframe and can be used evidentially in court. It must also command the confidence of the public, so it is important to consider very carefully the purpose and scale of any scheme and consult over its operation.

4.24 CCTV is most effective when provided with the following:

• good lighting;

• management support;

• continuous monitoring;

• comprehensive and full site CCTV coverage;

• adequate response; and

• good maintenance/housekeeping.

4.25 CCTV cannot replace security staff, although it may permit a reduction in their number or their redeployment to other security activities.

4.26 The Town and Country Planning (General Permitted Development) Order 1995 (as amended) ("the GPDO") includes 'permitted development rights' concerning the installation of CCTV equipment (see Part 33 of Schedule 2 to the Order). The wording of Part 33 refers to permitted development rights in the context of 'installation, alteration or replacement on a building of a closed circuit television camera to be used for security purposes.' These rights mean that, within certain limits, CCTV cameras can be installed without having to obtain planning permission. Part 38 Class B of the GPDO contains permitted development rights for CCTV and associated lighting for the Crown on Crown land for national security purposes:

4.27 Outside of these limits planning permission must be applied for in the normal way.

4.28 Use of such CCTV is also likely to be subject to the terms of the Data Protection Act 1998. The Information Commissioner's CCTV Code of Practice (2008)[12] contains a wide range of useful guidance and good practice in relation to planning, clarity of purpose, installation and operation of CCTV cameras and systems.

4.29 CCTV is not an alternative to getting the design right in the first place, for example, avoiding recesses in building elevations/facades that can offer hiding places for devices or individuals and may require monitoring /oversight. If poles for mounting CCTV cameras are being considered, careful thought will be needed to minimise the impact on the streetscape.

4.30 The intended purpose of a CCTV system will drive its design and ideally is implemented in one go rather than piecemeal at a site. Sharing CCTV between organisations can be considered as an option.

4.31 Using an Operational Requirement as the starting point for any CCTV system design allows interested parties to identify the need for such a system. It also sets out the parameters for operation, including the standard of recording, monitoring and response, as well as image quality, system access, maintenance and management[13].

4.32 A number of national police initiatives raise awareness of counter-terrorism and specifically the role that a visible security regime supported by surveillance equipment can play to deter, detect and delay suspicious terrorist activity including hostile reconnaissance. A short summary of relevant police-led initiatives is at Annex F.

4.33 The Protection of Freedoms Act 2012 received Royal Assent on 01st May 2012 and included provisions for a Surveillance Cameras Code of Practice and the appointment of a Surveillance Camera Commissioner. The first Commissioner was appointed on 13th September 2012, reporting to parliament on how CCTV and automatic number plate recognition (ANPR) systems are being used and raise any concerns through a report to

parliament. The Code of Practice[20] came into force on 12th August 2013 setting out guiding principles that should apply to all surveillance camera systems in public places. These guiding principles are designed to provide a framework for operators and users of surveillance camera systems so that there is proportionality and transparency in their use of surveillance, and systems are capable of providing good quality images and other information which are fit for purpose.

Annex A: Typical counter-terrorism design attributes - design of structures

When considering the incorporation of counter-terrorism measures into general design advice to site owners and operators is available from theNaCTSO website. Counter-Terrorism Security Advisers (CTSAs) also offer detailed security advice on a bespoke basis and will provide proportionate consideration to new build sites and redevelopments, focusing effort commensurate with the assessed attractiveness of the site and where the likelihood of return - in the form of protective security improvements - is higher. Advice is also available from the private sector on a commercial basis. If appropriate, the Centre for the Protection of National Infrastructure (CPNI), via the CTSA, may also offer bespoke advice. The CPNI website contains general security advice across a range of spheres including cyber, personnel, and physical security; as well as guidance on security planning. Further advice for designers and architects can be found using the Resilient Design Toolkit on the police Secured by Design website[21]. Engagement with the Counter Terrorism Security Advisor should be sought at the earliest opportunity in the design process to ensure the best consistent and proportionate advice, preferably at RIBA Stage 1.

The measures described below are not mandatory and the desirability of their inclusion in a development depends on a range of factors. Where the measures are appropriate, they will help to mitigate the vulnerability of buildings to terrorist attack and limit the extent to which the building might exacerbate the effects of such an attack. They are particularly relevant to buildings with significant occupancy and size and may be less realistically practicable for buildings that are modest in scale and/or have only modest levels of occupancy.

External areas

Measures that should be considered include:

• physical measures such as external barriers and/or a strengthened perimeter to prevent access to the facility for the placement of Improvised Explosive Devices (IEDs) either by forceful (i.e. suicide car bomb) or overt means (i.e. pedestrian suicide bomb). See also Annex B, (Design of hostile vehicle mitigation measures) for further information;

• measures to limit secondary fragmentation;

• avoidance of hiding places around buildings and within façade arrangements that might be used to conceal a hostile person and/or an IED;

• the value of CCTV coverage as a potential deterrent; and

• any pedestrian and vehicle gates to be compatible with the robustness of the remainder of the perimeter.

Building structure

Measures that should be considered include:

• as a minimum the measures for robustness against disproportionate collapse for Class 2B buildings described in current Building Regulation A3;

• the use of either framed reinforced concrete or framed structural steel;

• if framed reinforced concrete, use in-situ connections. Ensure beams, columns and floor are all tied continuously together using robust vertical and horizontal reinforcement details. In addition to normal gravity and environmental loads allow for load reversal (e.g. slabs being forced upwards by explosion pressure (see robustness clauses in current code of practice BS EN 1992[14] and consider the use of these clauses irrespective of building height);

• if framed structural steel, ensure that connection details will take reverse loadings. Floor slabs to be tied to beams with in-situ topping BS EN 1993[15] robustness clauses to be considered irrespective of building height);

• if unscreened vehicles are permitted to enter underground parking facilities then ensure that the structural design considers the floor/roof slabs, columns and connection details within this facility. In addition, this vulnerability needs to be clearly considered in any contingency plans, for example building evacuation plans which involve the movement of people around the building;

• the spreading of structural sway/ shear stability throughout the building, especially where expansion joints split up the structure. Concrete walls and shafts that provide stability may also provide useful protected internal spaces where occupants can take shelter from external threats;

• attaching glazed and non-glazed cladding panels directly to floor slabs rather than to perimeter columns;

• using non-glazed cladding materials that will provide protection from fragmentation and will not readily fragment or fail under blast loads and fixed to the structural frame with connections that can resist inward and outward loading;

• avoiding blast traps/containment in building elevations/façades (such as overhangs and deep recesses) or surroundings;

• protected spaces (previously known as bomb shelter areas) and the evacuation routes to them should provide effective resistance to blast and fragments. The exit routes should be duplicated. They should be in a core part of a robust building, remote from threat areas and away from a perimeter, preferably at levels above ground floor or in a basement. They should also provide good fire resistance. Overall space should be provided on a basis of at least 0.66m² per person, related to the building occupation level. Provision in protected spaces should include a means of communicating with the facility's control room and the outside world, lighting and water and, ideally, seating, toilet facilities and a back-up means of communications. Specialist advice should be sought;

• avoiding masonry buildings over two storeys, unless special masonry reinforcement is employed;

• using pre-cast framed structures where connections between components provide a comparable level of robustness to that achievable with an in-situ reinforced concrete frame;

• roof structure (and components of) over occupied spaces constructed of reinforced concrete (not less than 150mm thick) particularly if there is a mortar threat; and

• as small as practicable structural spans with regular column grid spacing and the avoidance of large spans, particularly at lower levels. Check removal of key elements if exposed to or at risk of impact explosive attack to ensure that their removal does not lead to a progressive collapse.

Windows and glazing

Measures that should be considered include[16]:

• consider whether large windows are essential and reduce the use of glazing. Carefully consider the inclusion of atria and whether these introduce avoidable risk of falling glass;

• consider the positioning of windows. Windows that are low down in rooms reduce the distance that flying glass will travel into the room;

• where glazing is used, the inclusion of an inner layer of laminated glass with an interlayer of not less than 0.76mm polyvinylbutyral well secured into the frames. Depending on the likely size of the potential IED and its distance from the glazing, the thickness of the glazing will need to be increased if the pane size increases. Glazing frames must be well secured to the building's structural frame; and

• the use of "security rated" ground accessible external windows which are compatible with door and cladding strengths and bars, mesh, grilles and upgraded glazing to protect against forceful entry.

The effect of a blast on laminated glass - top picture, compared to toughened glass - bottom picture.

Building internal layout, facilities and building services

Measures that should be considered include:

• locating critical elements, such as essential building utilities, in the most protected parts of the facility or dispersed, duplicated and/or disguised;

• provision of entry/exit point intruder detection and CCTV;

• provision of public address (PA)/ communications for emergency announcements;

• separation of the main public/visitor entrance from the main stair/service/ lift shaft riser;

• separation of the main public/visitor/ reception area from any central internal atria;

• split floor areas up with robust internal partitions to limit penetration of possible fragmentation;

• the incorporation of at least two staircases in the layout, spaced apart but preferably with no more than 50m between them, and orientated to provide diverse, well separated escape routes;

• entrance arrangements appropriate to the likely attempted hostile entry risk (e.g. vehicle and pedestrian barriers). For example, the provision of a lockdown capability for the entrance area in an emergency, where initiation of lock-down is by local alarm and release is remote (for example from an inner security control position);

• entry control and associated barriers giving access to a building should be located at the outermost practical position possible. The further a hostile event is allowed into the main body of a structure, the greater the damage that will generally occur;

• if an entry access control system is to be provided, it is preferable that it includes PIN verification at the outer boundary;

• separation of the general heating, ventilation and air conditioning (HVAC) system from the provision for the entrance areas/foyers;

• locating air intakes for the HVAC system in a secure location and ideally at level 2 or above;

• ability for the HVAC system to be capable of rapid shut-off and the location of make-up air intakes in a secure area;

• locating essential/critical services away from vulnerable façades of the facility; and

• locating the security control centre within a protected area of the facility.

Parking of vehicles beneath buildings

The parking of vehicles and the delivery of goods beneath buildings may in some circumstances offer particular design advantages (such as preserving street frontages and using land more efficiently) which may outweigh other considerations. However such underground or subbasement parking and delivery areas can present significant challenges from the point of view of counter-terrorism protective security as they increase vulnerabilities to terrorist attack by vehicle-borne improvised explosive devices (VBIEDs) – and hence pose a risk which needs to be assessed. Where such facilities are planned and they involve access by unscreened vehicles, then it is important that those proposing the development consider the extent of the risk posed and any appropriate options for mitigating it by reducing the development's vulnerabilities. Where appropriate in the light of police CTSA advice about the assessment of risk, this includes considering introducing design mitigation measures such as a strengthened structural building design (taking account of advice from police CTSAs - see bullet points under 'Building structure' above) and improved traffic management,

including screening of vehicles (see ‘Traffic Management’ in Annex B).

Deliveries to facilities

Protection of facilities from deliveries (including post) to them could be on a rolling scale. For low risk installations, the delivery and post receipt areas could be in an isolatable part of the building where receipt of a suspicious item will not disrupt the remainder of the building. As the extent of risk increases, measures to be considered include installation of an x-ray scanning machine and local containment through to off-site receipt and processing facilities for all deliveries.

General considerations

The following should also be taken into account:

• the likely response from emergency services – How quickly can they be called and how long will they take to arrive at the facility?

• whether hazardous stores can be located at a safe distance from the facility.

Annex B: Typical counter-terrorism design attributes - design of hostile vehicle mitigation measures

Vehicle-borne threats range from vandalism through to sophisticated or aggressive attacks by determined criminals and terrorists. Methods employed to gain unauthorised entry or exit from a site can range from the surreptitious tampering with barrier systems through to vehicle-borne improvised explosive devices (VBIEDs) rammed into the site by suicide operatives.

The load carrying capacity and mobility of a vehicle offers terrorists a convenient delivery mechanism for a large explosive device. The choice of vehicle and driver by those with hostile intent can also assist if either's familiarity can help to deceive surveillance or assist in gaining entry to sites.

Clear definition of the threat and the potential attack methods to be countered helps identify the most appropriate mitigation techniques.

Types of vehicle-borne threat

There are five main types of vehicle-borne attack – all can be deployed with or without the use of suicide operatives.

• parked vehicles. Controlled and uncontrolled parking facilities for unscreened vehicles adjacent to a site can pose a significant problem in terms of blast stand-off distances against VBIEDs;

• encroachment is where a hostile vehicle negotiates through an incomplete line of defences without the need to impact. An alternative form of encroachment is the exploitation of an active/retractable barrier system at a vehicular access control point by a hostile vehicle "tailgating" a legitimate vehicle through the access control point;

• penetrative attacks use the front or rear of the attack vehicle as a ram and have historically been used for criminal activity and terrorist attack to breach target premises. The choice of threat vehicle type in terms of its structure, mass, velocity and manoeuvrability will directly affect the design of suitable counter-measures;

• deception techniques prey on human weaknesses. For vehicle-borne threats this may be by the use of a "trojan" vehicle (one whose model, cloned livery or

registration is familiar to the site) or by hostile occupants negotiating their way through on a pretence or by using stolen or cloned access control or ID passes. Alternative scenarios include an unwitting mule/delivery driver delivering an IED surreptitiously planted by an attacker or an insider threat bringing a device into their own work site; and

• duress against the occupant of a legitimate vehicle to carry a hostile payload or duress against a guard controlling an access control point.

Whereas most new-build designs in greenfield sites could accommodate either sufficient blast stand-off distances in their site layouts or build structural robustness into their building, most existing sites (often through necessity and site, building, financial or logistical constraints) risk manage the vulnerabilities and place their trust in enhanced retro-fit physical measures, procedures and the assumed legitimacy of staff, pool or routine delivery vehicles etc. Naturally this affects the risk of a site to the last two forms of vehicle-borne threat, namely “entry by deception” and “entry by duress”.

Deception, duress and the "tailgating" form of encroachment attacks can all be mitigated by negating the need for active barrier systems and only designing a site to have a security cordon comprising static/passive barriers.

Site considerations

When designing hostile vehicle countermeasures it is extremely important, where possible, to maximise blast stand-off distances from the assets that require protection. Measures which exclude or restrict vehicle access will also need to consider provision of disabled access as described in the Buildings Regulations Part M – access to and use of buildings. In particular, requirements for disabled parking and setting down points should be reviewed.

Historically, hostile vehicles were parked, often legitimately, adjacent to the intended target. The stand-off distance used as the basis of the design for blast hardening of a building must be enforceable, i.e. no unauthorised (hostile or otherwise) vehicle can gain access beyond the stand-off barrier line. By doing so, the building’s blast protective measures and associated costs may be lessened.

Costs associated with fully hardening a building due to lack of blast stand-off can be significantly greater than installing vehicle counter-measures at a suitable distance. This is particularly the case with retrofits / refurbishments. However, each site will need to be assessed on a case by- case basis as land costs, ownership, available room, planning permission, business needs and re-location costs may eliminate any cost benefit.

Site design can accommodate countermeasures to layered vehicle attack scenarios where one or more of the above threat scenarios is used – for instance one hostile vehicle to create a gap by way of penetrative attack or blast and then another to exploit the subsequent gap and get closer to the asset.

Site assessment for vehicle-borne threats

Each site will require a specific assessment before counter-measures can be recommended. Those doing the assessment will need purely to assess whether the adjoining land is traversable and if so by what vehicles, ignoring congestion, signage, road markings and "rules of the road.

Part of the assessment will be to assess maximum speeds and angles of attack achievable by a hostile vehicle undertaking a penetrative attack. This process is called a vehicle dynamics assessment and profiles all the approach routes. This allows the counter-measures to be designed to an appropriate level, preferably not over or under-engineered.

After installation of vehicle security barriers at a site, regularly review any changes to the surroundings – for instance demolition of a neighbouring building or changes in the landscape could open up an approach route that previously did not exist or could allow a fast straight approach that for certain threat vehicle types would exceed the capability of the original vehicle security barriers. Equally, monitor neighbouring site activity, security measures and ownership, in case any of these affect the vulnerability of the assets and security systems. Once a site's vulnerabilities have been assessed it is possible to assess risk and to devise mitigating counter-measures.

Traffic management

For retro-fitting a site, avoid starting from a point which tries to accommodate the existing traffic patterns of staff, deliveries and visitors as this will usually result in solutions that are less effective and more expensive than otherwise might be possible. Instead, start from a point where the aim is to manage traffic in such a way that natural blast stand-off is created and less traffic has to negotiate vehicle access control points. If pass check personnel are in-situ at an access control point then design the area so that they are not put under undue pressure or distracted by traffic management requirements.

Options

• traffic exclusion is the starting point in terms of ambitious and effective protection. On larger self-contained sites, car parking for both visitors and staff further away from a protected building can bring extra confidence through natural stand-off – covered walkways which are not typically provided currently in car park designs, or a park and ride facility depending on relative distances, may ameliorate any staff concerns;

• traffic exclusion but with screening of any vehicles that are allowed into the cordon is the next best option. Less than 100% screening or a random screening strategy increases risk. Off-site consolidation and

screening facilities can offer multiple security benefits by reducing the number of vehicles that need to access either a secure site or underground delivery and parking facilities within a development. Such off-site screening increases the confidence of any vehicle that does arrive at a site and can release valuable space inside the development for alternative uses. Other environmental, safety and cost benefits may also ensue from off-site screening facilities;

• traffic inclusion for any vehicles within and around a large perimeter site is an option but typically would need to be coupled with individual protection schemes around critical and/or vulnerable assets thus providing reduced blast stand-off;

• although temporary vehicle security barriers at times of heightened threat are an option for some sites, they have a number of drawbacks. These are that their deployment is intelligence based; they require specialist equipment and time to deploy; unless stored locally, they would normally need to be transported to site; they may be deployed too late if in response to other attacks; temporary barrier systems are usually less effective against penetrative impact than permanent alternatives; they are often not suitable on natural or soft ground surfaces; their modular and wall-like nature does not always lend their effective use to undulating or unmade ground; their mass may preclude their use at certain sites; few temporary barrier designs incorporate integral vehicle gate systems; and effective temporary barriers tend not to lend themselves to use at sites which have less defined pedestrian lines and which need to be pedestrian permeable such as at transport interchanges or shopping centres; and

• if vehicular and/or pedestrian traffic into, or along, a road needs to be temporarily or permanently restricted for counterterrorism purposes, the Chief Officer of Police can recommend to the Traffic Authority that they introduce an Anti- Terrorism Traffic Regulation Order (ATTRO). This is made with reference to Sections 22(c) and (d) of the Road Traffic Regulation Act 1984 (as amended by the Civil Contingencies Act 2004). Further information on their applicability and selective use is available from CPNI or CTSAs. Discussion is recommended with disability user groups regarding alternative setting down or parking arrangements which may need to be considered if hostile vehicle mitigation measures to a site restrict vehicular access to certain areas.

Traffic calming measures

Slowing traffic in advance of vehicle security barriers has a number of benefits. It gives drivers the ability to better comprehend what is expected of them at a barrier system. It provides the guard force with more time to assess approaching vehicles and their occupants and affords more scope to react appropriately. In addition the vehicle approach speed will be reduced accordingly. This reduced speed can then be used to design an appropriately ‘matched’ barrier system to resist the hostile vehicle impact, thereby potentially reducing costs and infrastructural/engineering impacts as well as potentially allowing for more visually acceptable barrier solutions to be deployed.

Traffic calming can be achieved by way of horizontal deflections (typically bends or chicanes). Horizontal deflections can preclude poorer turning circle vehicles – although parts of the chicane can be designed as retractable or removable for occasional access by such vehicles.

Vehicle security barriers

Vehicle security barriers provide the hard stop for penetrative vehicle attack. They are structural in nature and can be either *Active* (powered or manual) or *Passive*. *Active* measures include hinged and sliding gates, boom barriers, retractable blockers and retractable bollards. Although bollards are often the preferred form of *passive* measure as they typically maintain maximum pedestrian permeability, other forms of *passive* barrier can also be considered. Structural elements can be imaginatively incorporated into benches, planters, landscape architecture, earthworks, walls, balustrades, cycle stands, lamp columns, shelters and information boards (these are often referred to as “street furniture”). CPNI can advise on the form and foundation requirements for such elements.

Trees of sufficient girth and rooting can be used as a vehicle security barrier but care must be taken to monitor the ongoing health and structural integrity of the tree. The tree will also need to be maintained so that limbs do not provide an easy climbing aid close to a perimeter and so that evergreen or seasonal foliage does not obscure sight lines for guard force surveillance. It is rare to be able to rely solely on trees as a vehicle security barrier due to the inability to grow sufficient strength trees close enough to each other to deny vehicle access between them.

The blast stand-off measures should be spaced so that the maximum clear distance between fixed structures is 1200mm. Seek advice for the appropriate gaps and overlaps between items that displace on impact. When the stand-off measure tapers in elevation, the 1200mm clear dimension is to be measured at a height of 600mm above the finished ground level. The 1200mm dimension has been optimised to limit the opportunity for the vehicle to extrude through the barrier line, whilst providing sufficient access for pushchairs and wheelchairs. The typical minimum height of all structural elements is 900mm but lower heights are possible depending on the form of the barrier, nature of the approaches and threat vehicle types. Cosmetic features in excess of this height may help with aesthetic aspirations, aid visually impaired road users or help to make the measures more conspicuous in areas of higher pedestrian flow.

Vehicle security barriers typically require well designed structural foundations in order for the items to perform appropriately in the event of a hostile impact. The foundations may need to accommodate underground utilities or provide for their diversion. Future maintenance access to the utility chambers will need to be considered at the design stage.

Safety, maintenance and service issues

Regardless of category or type of operable barrier, in the context of safety, operable

(*active*) barrier systems are considered to be 'machinery' and with that the system owners and designers have a duty of care to design a safe environment in which people can work and/or transit through on foot or vehicle. Operable barriers will require maintenance and servicing during their lifetime and there is therefore a need to implement a robust service level agreement to reduce or eliminate barrier downtime. Despite best efforts, there is always the possibility that an accident or collision occurs between the operable barrier and a legitimate or hostile vehicle. It is therefore very important to a have a contingency plan that allows that location to be either brought up to full operational capability very quickly or secured and an alternative location used.

Specifications and advice

The Centre for the Protection of National Infrastructure (CPNI) has published impact testing and installation guidance documents, in the form of British Standards Institution Publicly Available Specifications (PAS)[10]. The two documents are:

• PAS 68 entitled *'Specification for Vehicle Security Barriers'* which covers the manufacture and testing of vehicle security barriers. It is strongly recommended that all vehicle security barriers be specified to comply with PAS 68 at an appropriate performance level; and

• PAS 69 entitled *'Guidance for the Selection, Installation and Use of Vehicle Security Barriers'* provides guidance on the selection and installation of vehicle security barriers. CPNI also provide awareness and training on the subject of designing-out vehicle-borne terrorism to architects, engineers, planners and personnel with security, site ownership or operational responsibilities. CPNI can also provide specific advice commensurate to the attractiveness of the site, and maintain a list of appropriate, tested counter-measures derived from their extensive research and development programme. Advice is also available from the private sector on a commercial basis.

Annex C: Case studies

Effective protective security regimes draw upon the 'Deter, Detect, Delay' principles. The appearance of a site to any potential attacker, whatever the motive, can play a significant role in how they assess the vulnerability of that site.

A clear area, well maintained, with managed access points and reception facilities set in tidy grounds, presents an image of professionalism and offers less opportunity for an intruder to go unnoticed. This may well be enough to deter them from further action.

Once an attacker has decided to continue with an intrusion then robust, proportionate, well maintained and well managed protective security systems, including structured policies and procedures, that are adhered to, make it more difficult for critical assets to be accessed. As a consequence, an attacker has to evade or circumvent these measures to effect an entry. An integrated security regime will detect an intruder at an early stage and, most importantly, before any critical assets have been reached.

The attacker must then breach the physical security measures before gaining access to any assets. The right measures will provide a sufficient delay to allow time for the security response to reach the point of attack and apprehend the intruder.

Existing sites looking to improve their overall security arrangements will have to install new systems and physical measures retrospectively. It is important therefore to select the most appropriate measures applicable to that site and its security requirements to minimise the financial impact and business disruption caused by installation and implementation.

Consideration of security features is most effective for new build sites at the design/concept stage, so effective consultation with the relevant interested parties, planners, designers, police and security experts is of paramount importance. This will identify the level of security required and the most appropriate measures and systems available to meet that requirement. The procurement and installation can then be incorporated into the design and build budget, whilst the site and building design can accommodate the security measures and still achieve a welcoming, attractive, comfortable and safer environment.

The following examples show how recent projects have included good counter-terrorism design principles.

Better blast resistance

Resistance to blast can be achieved in a number of ways. A Government Department's headquarters building in central London is a good example of how measures can be combined to reduce the vulnerability to blast.

A series of bollards (impact tested to appropriate BSI PAS 68 criteria) has been installed around the building perimeter to keep potentially hostile vehicles further away. This system provides distance between the bollards and the building, referred to as 'stand-off', reducing the effects of a blast on the building.

In addition, the building incorporates laminated glass in strengthened frames to

reduce fragmentation and so reduce the number of casualties in the event of a blast.

The construction of raised beds and a water feature at the main entrance softens the appearance of the building, making it more attractive to visitors and personnel alike.

Another good example can be found in a sports stadium. The overarching requirement at stadia, which is mandated by legislation, is to ensure the safety of the many thousands of people accessing a venue for an event and departing afterwards. Hostile vehicle mitigation measures were constructed at pedestrian access points in such a way that they would be clearly visible to crowds and therefore ensure easy egress whilst reducing any potential trip hazard. In addition, these measures were designed and constructed so that, if an attack took place, as well as preventing a hostile vehicle entering the pedestrian walkways, they would be more resistant to blast, thus reducing injury to people nearby from secondary fragmentation.

A major station which undertook major refurbishment and development, has also installed a series of measures to prevent vehicle-borne improvised explosive devices accessing the concourse.

Pedestrian entrances and vulnerable areas have been protected by correctly spaced and impact tested bollards, lowering the vulnerability to vehicle-borne improvised explosive devices and extending the stand-off distance, so that blast effects are reduced. Whilst the majority of bollards are fixed in place, some demountable bollards have been included in areas where emergency services and maintenance vehicles require access. These bollards are controlled by the on-site security guard force.

Better building management facilities

All buildings require services and management facilities such as delivery areas, post rooms and storage areas. Heating, ventilation and air-conditioning systems (HVACs) and utilities all have to be located within, around or upon the building structure. These systems may carry vital data or provide energy for essential processes and critical assets. Ducting, pipework, cable management systems and other building services installations can be vulnerable to attack if inappropriately placed; and appropriate arrangements need to be in place to ensure that maintenance work is carried out by trusted personnel.

Careful consideration and design of the systems and their routes can greatly reduce the vulnerabilities they present. The need to maximise the use of space, largely driven by the cost of land, has pushed buildings upwards and designers have put building services such as HVACs on rooftop platforms to reduce building footprint size. Additionally, lift gear and water tanks have to be located at height through operational need, as do communications masts and aerials.

Many public buildings have all HVACs equipment installed at rooftop height. This includes the air intakes and service

hatches. Access to these systems is regulated by the existing access control regime applied across these sites, with no requirement for additional fencing, policies or procedures. Physical circumvention of the protective regimes, although not impossible, is extremely difficult, especially if it is to be achieved undetected.

A shopping centre and precinct development has incorporated a number of features into its final design. Although this project was conceived and design commenced during the 1990s, events in the Haymarket at London and Glasgow Airport in 2007 reinforced the need to consider counter-terrorism protective security measures at an early stage in the design process. This allowed the local CTSAs, working with representatives from the Centre for the Protection of National Infrastructure (CPNI) to engage with the design team, senior management and the developers to consider vehicular access to the site and identify protective security measures that were achievable, appropriate and acceptable to all.

This city centre venue is surrounded by the local roads network, which includes primary and through routes and, as can be seen in the photograph above, an underpass. The underpass presented vulnerabilities to terrorist attack at an early stage and, due to the importance of the route and the need to maintain service access, a permanent road closure was not an option. Through consultation with the local authority a series of measures have been introduced. These include a robustly enforced parking and loading restriction and, more significantly, an Anti-Terrorism Traffic Regulation Order (ATTRO).

The ATTRO allows the local police to close the route at certain times, specified in the order, and divert vehicles away from the area.

The site also includes a substantial underground delivery and service area. There is a need to control access into this area and manage delivery arrivals and prevent hostile vehicles penetrating vulnerable or critical facilities before they can be identified and denied access. Effective measures had to be deployed which would achieve this without unduly impacting upon the day-to-day site operation.

Existing sites where rejection routes have not been considered at the design stage often face difficulties, as their service entrances do not allow room for rejected vehicles (such as large articulated goods vehicles) to turn around or manoeuvre away. Consultation with the local city council has resulted in agreement for the centre management to utilise a holding area on the approach roads, some distance from the entrance, where expected vehicles wait whilst their appointment and identity details are verified before they can be security screened and then called forward to the service area. Spontaneous arrivals also have to wait here, so that security personnel can obtain the necessary information and then confirm with the intended recipient that the delivery and/or delivery agent are bona-fide. Where that is

not confirmed then the vehicle is rejected and can easily be returned to the roads network or, if necessary, intercepted by the appropriate enforcement agency.

The service entrances are protected by a series of rising bollards, meeting BSI PAS 68 and 69 specifications, control of which sits with the site security guard force. These are integrated with the local road layout and, at other entrances around the site, augmented by additional features such as anchored stone benches, reinforced concrete walls and fixed bollards.

The selection, design and layout of these measures were directly influenced by underground service ducts and utilities infrastructure. Close liaison was necessary between designers, planners, CTSAs and utility companies to understand how the different networks and infrastructure could work in concert with each other without incurring unnecessary levels of cost or disruption whilst still maintaining the required level of protection.

Better traffic management and hostile vehicle mitigation measures

Traditionally, protective security barriers, such as bollards, planters and gates, have required deep and/or wide structural foundations which have large cost and time implications in terms of ground excavations and the relocation of existing underground utilities. CPNI has been working with industry and impact test facilities to push the boundaries of science to better understand the dynamic loadings on various types of barrier during vehicular impacts, to identify the thresholds of success/failure and to identify new materials and alternative construction methods that can better cope with both impact and potentially a subsequent blast. This work has allowed systems to be engineered with far less onerous foundations and is already paying dividends on-site for instance with the use of bollard systems requiring only 100mm of excavation.

The Cabinet Office (on behalf of Government departments) has worked with the City of Westminster and their contractors, engineers, planners and specialist consultants to install essential protective security stand-off measures within the environs of the iconic Whitehall streetscape, whilst making significant improvements to the area, such as better use of public space and improving the visitor experience by widening footways.

The structural measures comprise bollards, balustrades and walling systems sited sympathetically and appropriately with the many and varied historical structures and listed buildings in the area. Many of the security solutions were

pioneered and tested by CPNI with the help of industry and predominantly reflect the architecture of the adjoining listed buildings. They utilise shallow foundations that are designed to accommodate existing underground obstacles such as utilities and roots of mature trees. The structural core is made of a unique proprietary blast resistant system which consists of steel plates and friction welded spacers which is then filled on site with concrete. In the case of walls and balustrades on Whitehall, Portland stone cladding is then applied to the core.

The Traffic Environmental Zone (TEZ) is a security cordon surrounding the City of London. Originally installed in 1993, the primary purpose of TEZ measures is to slow and rationalise vehicular movements entering the “Square Mile”. Points of entry into the City were narrowed in order to calm traffic, 17 minor streets were closed, and 13 were converted to one-way traffic. These changes were installed over a single weekend, utilising temporary measures on an experimental basis. The TEZ was subsequently expanded to the north and west in 1998 and between Holborn and Victoria Embankment in 2003.

Initially, concrete blocks and bollards were utilised to enforce TEZ measures. Over time, these have been replaced by more permanent solutions which sought to reclaim areas of the public realm for the benefit of pedestrians. One piazza is a notable example of this. Formerly a two-way vehicular route, the area has been subject to a high quality design approach that integrates security measures alongside improvements to the public realm. The carriageway was raised to footway level and repaved using granite setts, while the footway itself was resurfaced with York stone. Stone seating and planters are used to subdivide the space, allowing adjacent restaurants to spill-out onto the footway.

Within the area-wide TEZ, further visual deterrents have been introduced to improve security in the “Square Mile”. The City encourages the use of features such as raised planters, trees, and benches as an alternative to bollards in order to provide perimeter protection for specific buildings. These may be crash-rated, providing the security of crash-rated bollards without drawing attention to their protective role. The use of an area-wide security approach together with building perimeter measures has reconciled the City’s security demands with the needs of pedestrians and businesses.

Better oversight

One major shopping centre in the UK has a large number of CCTV cameras within the site and these are monitored and controlled from a dedicated security

control room. The system also incorporates an Automatic Number Plate Reader (ANPR) that has a number of software filter measures to reduce excess data capture and keep the system more manageable. For example, during day-to-day operation it uses an internal database of vehicles known to the security management.

For specific issues or to accommodate the investigation of crime it can also have other databases added. Enforcement agencies work in partnership with the centre management, utilising the CCTV system and adding access to databases such as the Police National Computer (PNC) as necessary to facilitate particular operational need.

If the ANPR system identifies a vehicle of interest to the authorities then operators can ‘track’ it around the car parks using CCTV. If the occupant(s) alight from the vehicle they too can be tracked around the centre.

Within the Control Room they abide strictly by the Data Protection Act 1998 and the centre employs a member of staff who has responsibility for management and accountability issues.

A major station main building has a large expanse of glazing across most of the roof area. This lets in high levels of natural light and provides an excellent basis for natural surveillance. The comprehensive CCTV system has been integrated with internal lighting to provide a similar environment in low natural light conditions. This is further enhanced by the use of glazed panels in place of solid barriers to manage and separate pedestrian traffic and define security zones. As a consequence, this large, open public space and adjacent restricted zone has a comfortable, welcoming atmosphere whilst enhancing clear views of the area and limiting the opportunities for all types of crime. CCTV monitoring by the in-house security guard force is augmented by operational links to British Transport Police affording a rapid and appropriate response to incidents.

Early engagement in planning and design

A major sports stadium is an example of a private sector building with overt protective security measures designed to mitigate against a hostile vehicle attack.

It was a major project involving partnership working between the site owners, architects, Government security advisers, police CTSAs, local authorities and others.

The need for a partnership approach was identified at an early stage in the project (RIBA stage 1). A police 'Major Projects' team became involved and this team arranged for the local CTSA to advise on counterterrorism protective security measures.

A series of briefings was delivered to the stadium Safety Manager and to the Board of Directors to raise awareness about terrorism and its relevance to a crowded place venue.

The police team not only looked at design from a 'Crime Prevention Through Environmental Design' (CPTED) and counter-terrorism point of view, but also from a policing operations perspective (e.g.; 'How was the venue going to be policed during an event?'). Account was also taken of the requirements of, for example, the Fire and Rescue Service to facilitate their response and ensure site compliance with Fire Safety Regulations.

Since completion, the sports stadium has been acknowledged as a leader in its imaginative design of hostile vehicle mitigation measures and has become a favoured venue for high profile conferences. This unanticipated business opportunity has been borne out of the effectiveness of the integrated security approach.

A major project to develop a station commenced in 2000. Major interested parties were involved in the planning and design from the outset. These included, from a security point of view, British Transport Police (BTP) Counter-Terrorism Security Advisers, Crime Prevention Design Advisor, Crime Reduction Officers, experts from the Centre for the Protection of National Infrastructure (CPNI) and, because the original building was a Grade 1 listed building, representatives from English Heritage and railway heritage organisations.

The design aspirations and security requirements were agreed and incorporated into the design, planning and build programme, resulting in the current structure today. Many of these links have been maintained to cater for the day-to-day running of the site. Policing and response plans involve co-operation between BTP and the local police force, the council and the site management. On-site security guards are complemented by regular patrols from the police. A formal forum has been established and meets on a structured basis, with security issues included as a standing agenda item. A dedicated site security manager has been appointed.

Due to geographical and operational links with a nearby large busy railway station, currently being refurbished and developed, the same approach to security and design has been adopted. Through this early engagement of interested parties, the standards reached in an international station are being mirrored in a neighbouring station project, with security matters included as a contractual priority. CCTV systems including that monitored by the local authority, will be linked to provide coverage across both sites and hostile vehicle mitigation measures will be extended to provide perimeter and critical area protection.

Access control into goods yards and underground service areas

Shopping centres cannot operate without a reliable supply chain. One busy regional shopping centre has nine separate vehicle access points to the service yards which must be able to accommodate the delivery requirements of all the businesses, including the centre itself, during operating hours. It must manage these requirements whilst ensuring access is controlled. Responsibility for the policy and management of vehicular access control into and out of these nine entrances has been given to an individual member of staff. Each vehicle is logged at the Control Room upon arrival and details relating to the retail unit expecting the delivery, plus a driver contact number, recorded.

After 20 minutes the delivery driver and store are checked to certify that delivery is still taking place. This is an example of good practice in their access control and goods vehicle management.

If there is an increase in the threat and/ or response level the management will deploy guards to the goods vehicle entrances to carry out more frequent vehicle searches. If necessary all vehicle access can be denied on a temporary basis.

Another shopping centre has employed a system whereby all deliveries and contractor visits need to be notified to the control room in advance. This is achieved through the issue of user names and passwords to contractors and unit retailers only when the appropriate documentation has been submitted, checked and authorised. Any vehicle arriving without appointment is refused entry to the site.

Such a policy may present difficulties at entrance gates where large goods vehicles are denied access and have to be turned around. Discussions with those responsible for the design and operation of the site, such as local authorities, highways authorities, planners, architects and police help to identify how this can be achieved without causing unnecessary disruption or danger to traffic and pedestrian movement.

The major station example used above also represents a good example of how underground service areas can be protected. The underground coach drop-off area, where substantial numbers of people arrive and depart from the station, has had vehicle blockers installed at the entrance and exit points and is covered by an extensive CCTV system. These areas are constantly manned by a uniformed security guard who validates the authenticity of a vehicle arriving at the entry point. If the vehicle is allowed to enter then the blockers are lowered remotely by the security control room personnel. Operating the blockers in this manner further reduces the possibility of the security guard being coerced or overcome in order to afford access to a hostile vehicle.

Access control and searching regimes

A national stadium illustrates good practice in ensuring there is an efficient searching regime for spectators entering the site. Sufficient numbers of well trained searchers are present to reduce as far as possible any queuing outside access gates. Those spectators who do not have bags with them can be fast tracked to further optimise access procedures.

The stadium encourages people not to arrive with bags through ticketing and website communication and will randomly search identified spectators who arrive with bags/rucksacks.

A Government Department headquarters building operates an access control regime where all personnel are subject to a security pass system and government vetting protocols to achieve a minimum level of security clearance.

This facility is equipped with airport security standard scanning systems. All visitors with baggage items are screened. There is an on-site security guard force, enhanced by regular armed patrols from the local police. Specialist police dogs are also utilised.

At a major city station the whole station facility has been separated into security zones. The Restricted Zone (RZ) encloses the departure and arrival lounges, platforms and trains and access is limited to ticketed passengers and authorised personnel. Passengers must pass through a security area operating airport standard screening systems.

Searches of venues and locations where the public have access is best conducted as part of daily good housekeeping before, during and after opening hours.

Sites should have a sectorised, systematic and thorough search plan in place and if a suspicious item is found follow the general "Golden Rules" guidance[18].

Site security staff, including door supervisors, are key personnel in this process. Proper training and support empowers them to recognise suspicious activity or objects and encourages them to report and deal with it effectively.

Within the night-time economy sector, one city centre based nightclub venue has employed a series of policies and procedures to reduce its vulnerability. This site has a maximum capacity of approximately 3000 people and, at peak times on Friday and Saturday nights, this capacity is often achieved. The club management has engaged with the local authority and business sector to address several issues.

City centre roads around the venue are subject to the use of temporary road barriers, restricting and deterring general access to vehicular traffic on peak evenings but allowing pedestrian access and known taxis. The purchase of the temporary road barriers and the costs of using a private contracted security guard force are met by a consortium of interested parties from within the city centre, principally other night-time economy venues, all of whom benefit from the measures. The restriction of free vehicular access into the most crowded areas at peak times significantly reduces the vulnerability to clientele from vehicle-borne improvised explosive devices and can allow early identification of suspicious vehicles.

Queues outside the venue are closely monitored and as they increase in size so more security personnel are deployed, keeping the ratio to clientele numbers relatively constant and not placing excessive burdens on individuals. All security personnel are equipped with 'headcams', a digital camera mounted on headgear, giving an 'eye view' of the scenes they are confronted with. The image and audio feeds are recorded to a personal hard drive which is downloaded to a centrally controlled database at the end of each shift. This system provides essential protection to the security personnel from spurious allegations

through a fully auditable record of events. It also establishes an invaluable database for the investigation of instances of suspicious activity such as hostile reconnaissance and is an obvious deterrent to potential intruders/attackers who would be wary of their appearance and activity being recorded, even in background scenes.

This venue operates during daytime hours as a bar and restaurant and there are several different access points. Prior to the nightclub opening times, these additional access points are closed down and secured, leaving just the main club entrance available. Security measures are concentrated here, with security personnel patrolling in high visibility jackets. Within the foyer are various signs displaying information about partnership working with the local authority, police and nearby venues, searching regimes and tolerance levels. Disruptive individuals are ejected in full view of those waiting to enter. All clientele are required to pass through an archway metal detector before entry and any suspicious items identified are removed. No bags are permitted inside the club.

This is a good example of rule setting immediately outside a single entry point. It very effectively advertises that there is a well-managed and stringent security regime in place and is a potential deterrent to a large amount of criminal activity, including hostile reconnaissance and attempts to deliver improvised explosive devices.

Club management has introduced a policy of planned searches. These are implemented across the entire site by sector teams just prior to nightclub opening times and soon after nightclub closing times. Each defined area is searched for suspicious items, insecurities or other security related anomalies, which are resolved before the club is opened for business. This activity deals with the possibility that devices may have been planted, or preparations made for some other activity, by paying customers, out of hours contractors/visitors, or persons who may have managed to circumvent existing access control measures.

Radio links to security personnel at other venues in the city, and the local police force, allow information about suspicious activity to be spread quickly and this affords valuable extra time for reaction to potential hazards and, if necessary, implementation of emergency plans.

Many sites, regardless of which sector they are operating in, face restrictions and limitations on the physical security measures they can deploy. This may be due to a number of issues including planning constraints, heritage considerations, building construction, local infrastructure and services, environmental impact, or a combination of effects from some or all of these. In these instances options for site operators are constrained, so security has to be addressed through policies and procedures designed to reduce vulnerability.

However, it is important to remember that sites that do not install physical barriers will remain vulnerable to a determined attack, such as that from a vehicle-borne improvised explosive device. Any physical measure installed, temporarily or permanently, must be managed by an appropriate policy and procedure to ensure that it is operated correctly, maintained according to manufacturer's specifications and addresses the relevant security issues to the required level. Where the hostile vehicle mitigation measure installed is active rather than passive (e.g. retractable barriers or swing

gates) it will be most effective where site security personnel are trained to keep the barriers in the secure position and only open them when they are content that the vehicle, load and occupants seeking entry have been satisfactorily screened.

Annex D: Sources of counter-terrorism protective security advice

Advice on how best to integrate proportionate counter-terrorism protective security measures as part of good urban design is available to site owners and operators from:

The National Counter Terrorism Security Office (NaCTSO)

The National Counter-Terrorism Security Office (NaCTSO)[5] is a police unit colocated with CPNI. It is funded by and reports to the National Counter Terrorism Policing HQ, supporting the ACPO (TAM) CT policing network.

NaCTSO contributes to the UK Government's counter-terrorism strategy (CONTEST) by supporting the *Protect* and *Prepare* strands of that strategy. NaCTSO counter-terrorism protective security work is divided into three areas:

• protection of crowded places;

• protection of hazardous sites and dangerous substances; and

• assisting the CPNI to protect the Critical National Infrastructure.

NaCTSO staff can offer specialist advice regarding counter-terrorism protective security and business continuity.

It also provides guidance in relation to the security of explosives and pre-cursor chemicals (including fertilisers) pathogens and toxins, radiological sources and other toxic chemicals.

Counter-Terrorism Security Advisers (CTSAs)

NaCTSO trains, tasks and coordinates a nationwide network of specialist police advisers known as Counter-Terrorism Security Advisers (CTSAs).

CTSAs provide detailed professional, independent protective security advice that is free to owners and operators of crowded places sites on a bespoke basis. Their work is primarily focussed on sites assessed as being more attractive to attack. CTSAs help sites to assess their vulnerabilities and enhance their security arrangements to an appropriate level through the implementation of proportionate measures to protect sites from and prepare for terrorist attack. Additionally, CTSAs help raise awareness of the terrorist threat and appropriate actions that might be taken to mitigate it by developing positive relationships with key interested parties. Further details of police led initiatives to raise awareness of counter-terrorism protective security can be found at Annex F.

CTSAs also work with other departments within the police as well as partner agencies to encourage a coordinated approach to all aspects of security; for example, they work closely with representatives of trade organisations and professional bodies to ensure counter-terrorism protective security advice is incorporated in general crime prevention regimes.

CTSAs have regular access to current terrorism threat assessments and related intelligence as well as other classified material.

As well as undertaking initial training covering physical and personnel security, site surveying and counter-terrorism, CTSAs undertake additional mandatory training over two years covering hostile vehicle mitigation, specialised physical security and operational requirement training, leading to the successful submission of a Licentiateship in Counter-Terrorism Security Management. To ensure the high standard of training is maintained, refresher training is delivered on the various disciplines relevant to counter-terrorism. In addition, quality assurance inspections are carried out by NaCTSO on an annual basis of all police forces throughout the UK. This includes the inspection of CTSA surveys to ensure that the advice follows a nationally consistent standard.

A CTSA can be contacted in the first instance via the local police website or switchboard. In case of difficulty, CTSA contact details can be found on the NaCTSO website or through contact with NaCTSO via email: nactso@cpni.gsi.gov.uk

Centre for the Protection of National Infrastructure

CPNI[10] is the Government's national technical authority which provides protective security advice to businesses and organisations across the national infrastructure. CPNI advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services (delivered by the communications, emergency services, energy, finance, food, government, health, transport and water sectors) safer.

CPNI runs a research and development programme devising effective countermeasures to evolving threats. Additionally CPNI provide awareness briefings and training courses on the subject of designing-out vehicle-borne terrorism to architects, engineers, planners and personnel with security, site ownership or operational responsibilities.

CPNI provides integrated security advice (combining information, personnel, cyber and physical) to organisations which make up the national infrastructure. This advice helps to reduce the vulnerability of the national infrastructure (primarily the critical national infrastructure) to terrorism and other threats to national security.

CPNI is an interdepartmental organisation, with resources from industry, academia and a number of government departments and agencies (including the Security Service, CESG and departments responsible for national infrastructure sectors). CPNI draws on expertise, knowledge and information from the range of organisations that contribute to its work. It sponsors research and work in partnership with academia, government partners, research institutions and the private sector to develop applications that can reduce vulnerability to terrorist and other attacks and lessen the impact if an attack does take place.

Private Sector Advice:

The Register of Security Engineers and Specialists (RSES)

Specialist counter-terrorism design advice can also be obtained from members of the Register of Security Engineers and Specialists. This Register is maintained by the Institution of Civil Engineers and is sponsored by CPNI.

The RSES[17] is managed and organised by the Institution of Civil Engineers and

provides a professional competence standard for potential clients and insurers through its code of ethics, demanding peer review and strict continuing professional development requirements.

Suitably qualified and independent security engineers and specialists can be engaged by sites, local authorities or third parties to provide costed protective security advice or to develop or comment on other advice received from CTSAs.

Secured By Design – Design Guides

All the information on making a development Secured by Design is in the design guides. Each type of development has its own document which can be downloaded for free. Developments which meet all the criteria are applicable for a Secured by Design award. For advice, information or to apply for a Secured by Design Developer award please contact the local CPDA to the development.

Annex E: Role of Crime Prevention Design Advisers (CPDAs)

CPDAs exist in almost all police areas. Where they do not exist, their counter terrorism "filtering" function is managed by CTSAs (see below).

Designing-out crime (including terrorism) at the earliest stages in the planning process can be extremely effective in developing safer and more secure environments in which people can live and work. CPDA's monitor the Local Authority Planning Registers, and develop a relationship with local planners to discuss relevant projects. They will offer security advice to applicants (developer and the design team) on appropriate applications, and will be asked for their opinion as part of the planner's official consultation. CPDAs refer relevant applications onwards for Counter Terrorist (CT) advice from CTSAs. The CPDA and CTSA then work together to deliver appropriate conventional security and CT advice on these filtered projects, although the level of CTSA engagement will depend on the assessed attractiveness of the site.

Some projects elect to work to Secured by Design standards (SBD) and the CPDA will support this process. They:

- offer risk-commensurate crime reduction advice and actively promote 'Secured by Design', 'Safer Parking' and other relevant security award schemes;
- promote effective community safety practice and encourage the development of safer environments that reduce risk and mitigate the impact of crime;
- establish effective local and national partnerships in order to develop the built environment in ways that reduce opportunities for crime and disorder;
- establish strong and effective lines of communication with the local planning authority and develop links into the planning process to ensure that where security advice is sought on new or existing planning projects, police advice is able to be offered as early as possible;
- influence and encourage planners, designers and developers to incorporate crime reduction, including counter-terrorism protective security measures into their development projects.

CPDAs can be contacted through the police force in the relevant area by ringing 101. Further information can be found on the Secured by Design website[21].

Annex F: Police led initiatives raising awareness of counter-terrorism protective security

Project Argus

Project Argus is a counter-terrorism tabletop exercise produced by the National Counter-Terrorism Security Office (NaCTSO) and delivered by the national network of police CTSAs.

The exercise scenario comprises a coordinated terrorist attack targeting a 'crowded place'. It specifically aims to provide valuable counter-terrorism advice on protective security, (including how to deal with a firearms attack), resilience and hostile reconnaissance in light of the current terrorist threat. It does this by taking businesses through a simulated terrorist attack. The simulation provides a realistic scenario prompting open discussion to identify the measures for preventing, handling and recovering from a terrorist attack and explores their expectations against reality.

Delegates are split into small syndicate groups and asked to work through a number of questions and scenarios prompted by the simulated sequence of events and the CTSA facilitators are supported by a panel of experts.

These events have been successfully run since January 2007 and have been developed to target different business sectors. Examples include retail, night-time economy, hotels, health and major events, for example, those related to the Olympics but separate from Olympic venues. Project Argus will continue to be developed as required. Events are facilitated by CTSAs free of charge - details of how to access a Project Argus event can be obtained from the NaCTSO website[6].

Argus Professional and Argus Planners

Architects, designers and planners can play a significant role in delivering improved counter-terrorism protective security. Argus Professional was launched in 2008 to target built environment professionals including architects and designers, with a modified version (Argus Planners) for an audience consisting of planners from both the private and public sectors. They both aim to demonstrate that counter-terrorism protective security measures can be designed into structures and spaces to create safer crowded places.

Project Griffin

Project Griffin is a police-private industry initiative to accredit security personnel in identified locations by their attendance at a one day course in order to improve their skills and knowledge in relation to counterterrorism activity.

Project Griffin aims to encourage members of the community to work in partnership with the police to deter and detect terrorist activity and crime. This will be achieved by working with the community to:

• raise awareness of current terrorist and crime issues;

• share and gather intelligence and information;

• build and maintain effective working relationships;

• maintain trust and confidence in the police and other authorities; and

• empower people to report suspicious activity and behaviour.

The main strand of Project Griffin is very much about the police sharing information with key trusted partners in the community, by providing input through an 'Awareness Day'. The Awareness Day is delivered in a structured way, covering topics such as the current threat level, hostile reconnaissance, recognising the components of an explosive device and person/vehicle-borne devices, all of which help to galvanise and motivate participants to want to work with the police.

The Project Griffin Awareness Day also serves to help people think about their own local procedures and processes for dealing with certain types of incident during times of emergency.

Operation Lightning

A police coordinated hostile reconnaissance operation to identify those who might be involved in terrorist activity and/or domestic extremism.

This helps to gather intelligence by recording, investigating and analysing suspicious sightings or activity near to or at prominent or vulnerable structures or buildings.

Annex G: Useful publications

NaCTSO guidance

NaCTSO counter-terrorism protective security advice publications are available at the NaCTSO website[5].

CPNI guidance '*Protecting Against Terrorism*' - available at the CPNI website[10].

Cabinet Office guidance on *'Public Safety in Complex and Built Environments'* (Capstone guidance on integrated safety management) published in 2007.

Department for Transport and Department for Communities and Local Government document: *'Manual for Streets'* and the associated *'Inclusive Mobility'* guidance.

British Standard BS8300 Design of Buildings and their Approaches to Meet the Needs of Disabled People – Code of Practice.

NHS Estates Health Building Notes (HBNs)

'Streets for All: Guidance for Practitioners' was produced in 2005 by English Heritage, in conjunction with the Department for Transport. These regional manuals are aimed at all those involved in the design and management of streets. A summary Streets for All (2004) document is also available.

British Council for Offices Security Guide published in 2009 (available to members only).

Contact

The National Counter-Terrorism Security Office can be contacted via its website[5] or by email: nactso@cpni.gsi.gov.uk

Glossary and definitions

Accessibility – The ability of people to move round an area and to reach places and facilities, including elderly and disabled people, those with young children and those encumbered with luggage or shopping.

CONTEST - the Government's overarching counter-terrorism strategy. It was most recently published in July 2011, with the aim of reducing the risk to the UK from international terrorism.

Context – The setting of a site or area, including factors such as traffic, activities and land use as well as landscape and built form.

Counter-Terrorism Security Adviser (CTSA) - Located within each police force to provide specialist advice about counterterrorism protective security. See Annex D.

CPDA – Crime Prevention Design Adviser. Provide advice to planners and applicants on addressing crime prevention issues at the design/planning phase. See Annex E.

CPNI - the Centre for the Protection of National Infrastructure offers advice aiming to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services (delivered by the communications, emergency services, energy, finance, food, government, health, transport and water sectors) safer. See Annex D.

CPTED – Crime Prevention Through Environmental Design. The main thrust of this approach is that the physical environment can be designed to produce behavioural effects that will reduce crime and anti social behaviour and reduce fear of crime, thereby improving the quality of life. These behavioural effects can be accomplished by using design to reduce those features that support criminal behaviour.

Crowded place - The working definition of "crowded places" is widely drawn: crowded places are regarded as locations or environments to which members of the public have access that, on the basis of intelligence, credible threat or terrorist methodology, may be considered potentially liable to terrorist attack by virtue of their crowd density. Examples include:

• bars, pubs and nightclubs;

• shopping centres; and

• sports and entertainment stadia.

Curtilage –The boundary of a property.

IED - Improvised Explosive Device. Most terrorist bombs are improvised and so are known as improvised explosive devices or IEDs. They can be categorised by their means of delivery, for example a person-borne IED is known as a PBIED. Similarly a vehicle-borne IED is known as a VBIED. They can also be categorised by content, for example chemical, biological, radiological, nuclear, incendiary or conventional IED.

National Counter-Terrorism Security Office (NaCTSO) – Police unit responsible for raising awareness of the terrorist threat and the protective security measures that can be taken to reduce risks and mitigate the effects of a terrorist attack. See Annex D.

Public space/realm/domain – The parts of a village, town or city (whether publicly or privately owned) that are available, without charge, for everyone to use or see, including streets, squares and parks.

Retro-fitting – Enhancing existing sites retrospectively with the recommended approach to, and required specification of, counter-terrorism protective security measures.

Streetscape – The street patterns, furnishings and landscaping that form the built environment.

Stand-off – The minimum distance between an IED/VBIED and its target.

Urban design – The art of making places. Urban design involves the design of buildings, groups of buildings, spaces and landscapes, in villages, towns and cities, and the establishment of framework and processes which facilitate successful development.

VBIED – see IED.

End notes

1) https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels.html

2) https://www.gov.uk/government/organisations/department-for-transport

3) https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty

4) Fact Sheet2: National Security Risk Assessment can be found at https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty

5) http://www.nactso.gov.uk

6) http://www.nactso.gov.uk/our-services

7) http://planningguidance.planningportal.gov.uk/blog/guidance/design/

8) https://www.gov.uk/government/publications/manual-for-streets

9) https://www.gov.uk/government/publications/inclusive-mobility

10) http://www.cpni.gov.uk/

11) https://www.cpni.gov.uk/advice/Personnel-security1/

12) http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx

13) 12) Further advice on CCTV is available from the CPNI website www.cpni.gov.uk; from the Centre for Applied Science and Technology website https://www.gov.uk/government/publications/cctv-supporting-small-businesses ; and in NaCTSO guidance booklets available on the NaCTSO website www.nactso.gov.uk

14) BS EN 1992 has replaced BSI8110 although it is currently still in practical use.

15) BS EN 1993 has replaced BSI5950 although it is currently still in practical use.

16) More information about glazing can be found on the CPNI website http://www.cpni.gov.uk/advice/Physical-security/ebp/

17) Further advice on RSES are also available from the Institute for Civil Engineers (see website: www.ice.org.uk) and ICE details can also be found on www.cpni.gov.uk and www.nactso.gov.uk

18) http://www.cpni.gov.uk/Security-Planning/Staff-training-and-communications/workplace-security/

19) PAS 127: http://shop.bsigroup.com/ProductDetail/?pid=000000000030263559

20) https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

21) www.securedbydesign.com/ www.britishparking.co.uk/Park-Mark---The-Safer-Parking-Scheme

Published by the Home Office

ISBN: 978-1-78246-387-0