



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 27 May 2013

**6090/10
ADD 7 EXT 1**

**ENFOPOL 38
PROCIV 15**

PARTIAL DECLASSIFICATION

of document:	6090/10 ADD 7 RESTREINT UE
dated:	5 March 2010
new status:	Public
Subject:	Second Round of Peer Evaluation Preparedness and consequence management in the event of a terrorist attack

Delegations will find attached the partially declassified version of the above-mentioned document.



ANNEX

**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 5 March 2010

**6090/10
ADD 7 EXT 1 (27.05.2013)**

**ENFOPOL 38
PROCIV 15**

ADDENDUM TO THE NOTE

from : The Council General Secretariat
to : Working Party on Terrorism

Subject : Second Round of Peer Evaluation
Preparedness and consequence management in the event of a terrorist attack

Delegations will find enclosed the report of the evaluation mission in **the United Kingdom** (8-10 October 2009) in the framework of the above-mentioned round of peer evaluation.

1.	EXECUTIVE SUMMARY	3
2.	ARRANGEMENTS IN THE EVENT OF A TERRORIST ATTACK	5
2.1.	Structures and organisational framework of National Crisis Centres	5
2.2.	National arrangements in the event of a terrorist attack	10
2.3.	Competences of the national crisis centre for potential cross border targets for terrorist attacks	13
3.	TRAINING/EXERCISES FOR TESTING THE NATIONAL CRISIS CENTRE AND COMMUNICATION SYSTEMS IN CASE OF TERRORIST ATTACK.....	14
4.	SOFT TARGETS	16
5.	GOOD PRACTICES	22
6.	RECOMMENDATIONS	23
7.	ANNEX	24
7.1.	Presentations were made by the following institutions.....	24
7.2.	Speakers	24
7.3.	Expert Team	25

1. EXECUTIVE SUMMARY

- In the framework of the second round of peer evaluation covering "Preparedness and consequence management in case of a terrorist attack" an evaluation visit was made to United Kingdom from 08 to 10 October 2008.
- The UK faces a serious and sustained threat from terrorism. The national threat assessment at the time of this evaluation stood at 'severe' which means that some form of attack is highly likely. Many of those networks and individuals who are judged to pose a terrorist threat share an ambition to cause large numbers of casualties without warning. Some have aspirations to use non-conventional weapons such as chemical, biological, radiological and nuclear substances.
- The Government's counter terrorism strategy, CONTEST, is an integrated approach based on four main work streams, each with a clear objective to try and stop terrorist attacks occurring or, when they do, to mitigate their impact. The National Risk Register is focused on preparing for emergencies but the CONTEST work streams are:
 - Pursue: stopping terrorist attacks
 - Protect: strengthening our protection against attack
 - Prepare: mitigating the impact of attacks
 - Prevent: stopping people becoming terrorists or supporting violent extremism
- CONTEST is more than a simple strategy; it seeks to instil in all relevant players, from members of the armed forces to civil servants, a genuine sense of security awareness. The National Risk Register sets out an assessment of the likelihood and potential impact of a range of different risks that may directly affect the UK.
- The National Risk Register is designed to increase awareness of the kinds of risks the UK faces, and encourage individuals and organisations to think about their own preparedness. The register also includes details of what the Government and emergency services are doing to prepare for emergencies.

- The Cabinet Office Briefing Room (COBR) was established to co-ordinate the Government's response to a crisis.
The COBR structure is designed to be flexible to adapt to the circumstances at hand. In 2007, the COBR was activated more than 200 times.
- In general terms the UK is a leading country in the field of counter terrorism among the EU countries. Its national strategy is based on rich past experience and on an ongoing assessment of present risks, as well as exercises, public awareness and new practices. It is geared towards providing effective response in case of terrorism attack.
- The main recommendations resulting from this evaluation mission focus on the following areas:

NOT DECLASSIFIED

2. ARRANGEMENTS IN THE EVENT OF A TERRORIST ATTACK

2.1. Structures and organisational framework of National Crisis Centres

Counter-terrorism in the UK is the responsibility of the Home Office. The Office of Security and Counter-Terrorism (OSCT) was created in 2007. OSCT's main task is to advance and implement the UK's CT strategy (CONTEST2) at the level of the government authorities. They chair weekly meetings with all organisations responsible (defence, intelligence, police etc) to guarantee information flow and cooperation across government. While the OSCT is in charge of coordination, implementation is done in the individual areas of competence (healthcare, transport etc.)

In the event of a terrorist incident, the Home Office - as the Government Department responsible for counter-terrorist policy – would lead Central Government's response, primarily working alongside the Police Service (which has operational responsibility in a terrorist incident) and the intelligence agencies. The Operational Support Team which sits within OSCT Strategy, Planning and Change, would activate and co-ordinate the Home Office response, drawing upon expertise from across OSCT and beyond.

An immediate priority for OSCT following an incident would be to establish communication with the Police Gold Commander (the officer in overall police command). An early decision would be made as to the deployment of a Government Liaison Team, led by a Home Office Government Liaison Officer, to support the Gold Commander and provide a single channel of information between the local and central response.

OSCT in consultation with the Cabinet Office, would decide on the activation of Central Government's crisis management facilities in the Cabinet Office Briefing Rooms (COBR). COBR may meet at ministerial level (chaired by the Prime Minister, the Home Secretary (or Minister), or at official level (by a senior OSCT official). All relevant departments would be represented in COBR meetings. It is essential that COBR is kept fully up to date on developments in order to provide strategic direction. COBR has a number of responsibilities to include making decisions in relation to the adequacy of resources and national assets and determining the public information strategy.

The main task of OSCT is to pool strategic terrorism agendas and be the contact point for other authorities in CT matters. Information is supplied by the police and the intelligence services, which cooperate closely with the OSCT. OSCT has developed a “standard risk assessment methodology” which is used by the CTAs (Counter Terrorism Security Advisers) as a basis for the transmission of information on “crowded places“. One component of the OSCT is the Operational Support Team, which closely cooperates with the “resilience area” of the Cabinet Office.

Together with the National Counter Terrorism Security Office (NaCTSO), the OSCT develops programmes for reducing the impacts of terrorist attacks. The OSCT also draws up national CT exercise programmes, including the “consequence management” of other areas (Cabinet Office, NaCTSO, CLG Resilience etc).

The NaCTSO has a “multi-agency approach” and is in charge of protection measures for sensitive areas such as crowded places, critical national infrastructure, external security (border protection), CBRN and UK interests abroad. In close cooperation with the police, the best possible protection against threats to these areas is ensured on the basis of information from the intelligence services, as well as by developing technical action and other action geared towards measures. For this purpose, the NaCTSO closely cooperates with industry and trade, both as a client and as a supplier. Government entities involved in such cooperation are the DEFRA (Department for Environment, Food and Rural Affairs), the DFT (Department for Transport) and other ministries, as well as the CLG (Communities and Local Government).

NOT DECLASSIFIED. A closely cooperating network of CTAs (Counter Terrorism Security Advisers) provides consultancy to shopping centres, sports facilities etc. locally. The network is financed by the Home Office.

National Risk Assessment (NRA) is a classified cross-government document which incorporates expertise from a wide range of departments and agencies. It assesses the impact and likelihood of major risks, both hazards and threats that the country could face over a five-year period, enabling prioritisation of the UK’s planning for emergencies. An unclassified version of the NRA, The National Risk Register, can be found on www.ukresilience.info.

The Department for Communities and Local Government (DCLG) coordinates the regional resilience tier. In each region, there are Regional Resilience Fora (RRFs) whose role is to ensure that wide scale planning is undertaken across local boundaries. During emergencies, the regional tier would report on the impact of the emergency across their area or, at the request of the LGD (or Cabinet Office if the central government lead is initially unclear), to monitor the situation and provide an interface with the local Strategic Co-ordination Group. Input may also be required from the devolved administrations where this is necessary. Examples of emergencies on this scale could include prison riots and severe weather. In the case of a terrorist incident, the Home Office would deploy a Government Liaison Officer, possibly with the support of a wider Government Liaison Team (including representatives from the key government departments and the Regional Resilience Team).

In extremis a Regional Civil Contingencies Committee may be convened to co-ordinate the region's response or to advise on the prioritisation of national assets. For terrorist incidents, the **National Co-ordinator of Terrorist Investigations (NCTI)** who is the Deputy Assistant Commissioner who leads the Metropolitan Police Service's **Counter Terrorism Command (CTC)**, will co-ordinate or direct major CT investigations in England and Wales, and may provide an advisory role in Scotland.

Increasingly, there is an expectation that the NCTI can turn to the regional Counter Terrorism Units to respond following an incident or during a major operation. Whilst the CTUs are based in areas of high demand, they can be deployed flexibly as required. Regionally based **Counter Terrorism Intelligence Units (CTIUs)** and local force Special Branches can also assist.

Within the UK, the Ministry of Defence (MOD) contributes to security through the application of specific Defence capabilities in support of the civil authorities. Military Aid to the Civil Authorities (MACA) covers the provision of military support to the civil power, other government departments and the community at large. The support is provided on an emergency basis and only provided as assistance, on the basis that the relevant civil agency retains responsibility for and control over the situation.

The Foreign and Commonwealth Office (FCO) is responsible for informing foreign missions in the UK in case of an attack. A project developed together with the police (Hermes) is to improve the provision of information to offices abroad. In addition, two FCO websites are available to embassy staff.

Contemporary terrorist organisations aspire to use chemical, biological, radiological or nuclear (CBRN) weapons. To address the CBRN threat, OSCT leads the cross-cutting CBRN Resilience Programme which seeks to build and improve the UK's ability to respond to and recover from a terrorist attack using CBRN devices.

Central Government crisis management arrangements are overseen and managed by three secretariats within the Cabinet Office: the National Security Secretariat, which supports the response to domestic and international security and terrorist incidents; the Civil Contingencies Secretariat, which leads on civil emergencies; and the Foreign and Defence Policy Secretariat which leads on other international events.

Each secretariat contributes to, and coordinates aspects of, the central Government emergency response machinery referred to as the Central Response, a set of integrated crisis management components which fall under the banner of the Cabinet Office Briefing Rooms (COBR). The Central Response comprises a Strategy Group, otherwise known as the Civil Contingencies Committee (CCC) for civil crises, the COBR Situation Cell, COBR Intelligence Cell, Scientific Advisory Group for Emergencies (SAGE), the Impact Management and Recovery Group (IMRG) and the News Coordination Centre (NCC). Each component can operate in concert with the others under the direction of the Strategy Group/CCC, to compress and accelerate Whitehall decision making and facilitate a timely and well coordinated response from Government.

Local responders, police forces or emergency medical teams are the first on the scene. Their assessment will be decisive for the amount and level of regional or national support to the area. Most incidents can be managed by those responders, in some cases supported by a lead department in Whitehall or a devolved administration. But for the most severe emergencies, such as a terrorism incident, a co-ordinate combined government response is essential.

Three broad types (or levels) of emergency require UK central government engagement (i.e. those departments and ministers directly accountable to Westminster Parliament).

The response to an emergency at levels 2 or 3 involves the activation of central government's crisis management facilities - COBR - to facilitate rapid co-ordination of the central government response and effective decision making. In practice, the actual response to a specific emergency will need to take into account the nature of the challenge and other circumstances at the time.

The levels of an emergency are:

- **Significant emergency (Level 1)** has a wider focus and requires central government involvement or support, primarily from a lead government department (LGD) or a devolved administration, alongside the work of the emergency services, local authorities and other organisations. There is however no actual or potential requirement for fast, inter-departmental/agency, decision making which might necessitate the activation of the collective central government response, although in a few cases there may be value in using the COBR complex to facilitate the briefing of senior officials and ministers on the emergency and its management. Examples of emergencies on this scale could include prison riots.
- **Serious emergency (Level 2)** is one which has, or threatens, a wide and prolonged impact requiring sustained central government co-ordination and support from a number of departments and agencies, usually including the regional tier in England and where appropriate, the devolved administrations. The central government response to such an emergency would be coordinated from the Cabinet Office Briefing Rooms (COBR), under the leadership of the lead government department. Examples of an emergency at this level could be a terrorist attack, widespread and prolonged loss of essential services, or a major emergency overseas with a significant affect on UK nationals or interests. Examples of emergencies on this scale, include the 7 July bombings in London. On 7 July, a multi-agency response was initiated at the local, regional and national levels. The local response was led by the Metropolitan Police with involvement from many other responders. At a national level, the Home Secretary was the Lead Government Minister and Ministers from other government departments and senior officials met from early on in the crisis to provide strategic guidance to the response, assess the likelihood of further attacks, consider public messages, liaise with international partners, and prioritise the use of national assets.

- **Catastrophic emergency (Level 3)** is one which has an exceptionally high and potentially widespread impact and requires immediate central government direction and support, such as a major natural disaster, 9/11 scale terrorist attack in the UK, or a Chernobyl-scale industrial accident. Characteristics might include a top-down response in circumstances where the local response had been overwhelmed, or the use of emergency powers were required to direct the response or requisition assets and resources. The Prime Minister would lead the national response from COBR. Fortunately, the UK has had no recent experience of a Level 3 emergency, but it is important to be prepared for such an event should the need arise.

2.2. National arrangements in the event of a terrorist attack

COBR can be activated at one hour's notice 365 days of the year, typically at the request of the Lead Government Department (e.g. the Home Office for domestic terrorist incidents or the FCO for overseas incidents or international events). The activities of COBR are geared towards the achievement of three core objectives:

- Protect human life and, as far as possible, property and the environment. Alleviate suffering;
- Support the continuity of everyday activity and the restoration of disrupted services at the earliest opportunity; and
- Uphold the rule of law and the democratic process.

Upon activating, COBR will immediately begin providing strategic direction, based on a number of inputs, including:

- a common recognised information picture (pulled together by the Situation Cell in COBR);
- operational intelligence assessments and Joint Terrorism Analysis Centre (JTAC) threat levels in relation to terrorist threats where relevant;
- advice from the Police Gold Commander when established or ACPO/ACPO(S) in other situations and the lead Government Department;
- advice on the wider impact and longer-term recovery; and
- scientific advice provided by, or on behalf of, the Lead Government Department

In addition to setting the strategic direction, COBR is the central Government's mechanism of choice for performing a number of critical functions in support of the wider response, including:

- Taking decisions on the adequacy of existing legislation and the use of Emergency Powers at national or sub-national level;
- authorising military assistance to the civil power or a central government department;
- mobilising national assets and central Government resources and releasing them to support response and recovery efforts as appropriate;
- determining national protective security measures and other counter-measures;
- determining the public information strategy, and co-ordinating public advice in consultation with the Police Gold Commander and devolved administrations (where appropriate) and other key stakeholders;
- managing the international/diplomatic aspects of the incident;
- determining the likely development of the emergency and providing early strategic direction of preparations for the recovery phase (including the restoration of services);
- sharing information with the devolved administrations on the evolving situation; and
- advising on the relative priority to be attached to multi-site or multiple incidents and the allocation of scarce national resources.

For further information, COBR operating doctrine is set-out in more detail in the publicly available document, Central Government Emergency Response Arrangements: Concept of Operations, popularly referred to simply as the ConOps. The ConOps can be found at www.ukresilience.info.

In addition to COBR, the Cabinet Office has set up a "UK Resilience Cycle" with four steps:

- Horizon Scanning, looking up to 12 months ahead;
- Assessing Risks. The results of the Horizon Scanning feed into a wider systematic risk assessment;
- Building Resilience based on the risk assessments taking into account generic capabilities to develop specific plans for business continuity and crisis management in order to define requirements and solutions.
- The process of developing plans to cope with disruptive incidents is known as Business Continuity Management (BCM). It involves identifying critical business activities and resources and planning how to maintain them in the event of a disruptive incident.

In partnership with key stakeholders, the Cabinet Office has developed a BCM Toolkit to help commercial, public sector and voluntary organisations to develop appropriate business continuity plans. These should be exercised regularly to ensure they are workable and that adequate measures are in place to provide information to staff and key stakeholders in the event of an emergency.

Any emergency on a scale requiring a co-ordinated UK central government response will need national direction of public information from the outset. Central government will be responsible for the national communications strategy to respond to the crisis, the development of which will be co-ordinated with the lead responder locally (normally the police).

Communication is vital during the response phase of a terrorist incident and warnings, advice and information to the public will be a priority. The News Co-ordination Centre (more below) may be established by the Cabinet Office Communications Group in support of the Home Office to ensure consistent messages at all levels, and across all departments and organisations involved in the response. The Research Information and Communications Unit (RICU) may also join the NCC to provide advice on messaging and support the dissemination of messages amongst key stakeholders across government.

From the operational control at scene (“Bronze Command”), information goes via the operational co-ordination (“Silver Command”) to the integrated overall command (“Gold Command”). The “Gold Commander” is usually led by the police. This level is in contact with the COBR.

NOT DECLASSIFIED. In addition to the main meeting room with the latest communication facilities, the COBR provides offices for all institutions represented with possibilities to communicate with their “home offices” and to communicate amongst each other.

The News Co-ordination Centre (NCC) will be established in response to emergencies generating significant media interest to pull together the national media and public communications effort. Under Home Office leadership for a terrorist incident or the lead department in other cases, it will work to the policy direction of COBR. Information Officers from relevant Whitehall departments and agencies will be attached to the NCC for the duration of the emergency. Where there is a significant devolved dimension, an information officer from the relevant devolved administration will also normally join the NCC. The Welsh Assembly Government Press Office will provide 24/7 cover at its Emergency Co-ordination Centre where necessary and link into the Press Teams at the SCGs in Wales and the NCC in London.

Various levels of support for an LGD are available depending on the seriousness of the situation. This could include:

- Producing coordinated/consolidated briefing for use by Ministers, press officers and stakeholders to ensure consistency in the messages delivered;
- Coordinating requests for interviews with Ministers, experts/ third parties
- Establishing a central press office – to work with the lead and other Government departments
- Work in conjunction with the Media Monitoring Unit and the GNN to operate an analysis and monitoring team, ensuring that coverage is monitored and assessed and, where necessary, errors corrected
- Communications forward planning
- Work with the media to facilitate coverage, where necessary
- Establishing emergency media centre;
- Organise media briefings;
- Working closely with the Government News Network in the regions;
- Working closely with the Press Offices of the devolved administrations
- Regular updating of the UK resilience website and links to related sites as well as monitoring of other external sites. Additional work can also include developing bespoke websites where necessary.
- Working with the lead government department to ensure that all relevant audiences – public and stakeholder - are targeted quickly and effectively
- Liaising closely with the Media Emergency Forum/regional MEFs;
- Arranging emergency advertising; and
- Staffing a 24/7 operation.
- **NOT DECLASSIFIED**

2.3. Competences of the national crisis centre for potential cross border targets for terrorist attacks

Diplomatic and foreign partners do not participate in meetings of COBR. “Project Hermes” is a joint initiative of the Metropolitan Police Service (MPS) and the Foreign and Commonwealth Office (FCO) to provide accurate and timely information to the diplomatic community following a Mass Casualty Incident in London.

Information from the MPS and Her Majesty's (HM) Government is directly transmitted to the Diplomatic Missions via SMS (text), e-mail messages and secured websites.

After initial notification of the incident itself, the dissemination of further information will be agreed with the NCC.

Bilateral exchange of information on foreign victims and casualties will also be carried out via the FCO which will also be a partner in the COBR in such cases.

On the basis of its experience and requirements, the UK has created a multitude of structures and organisations, some of which are part of the Home Office or the Cabinet Office.

These structures exist not only at horizontal level but also partly at vertical level and also involve regional and local entities.

The **Home Office** retains the lead for the management of terrorist incidents in Scotland and Wales. The Scottish Executive and Welsh Assembly Government are responsible for co-ordinating wider impact management and recovery issues within their territory. The **Scottish Executive** is also responsible for policing and criminal investigations in Scotland. Under existing arrangements, the **Secretary of State for Northern Ireland** has responsibility for policing and counter-terrorism within Northern Ireland. But the Home Office provides the Northern Ireland Office (NIO) with the strategic advice to address the threat from international terrorism.

NOT DECLASSIFIED

Cooperation with the EU Member States is governed by structures and obligations defined at EU level. Depending on the requirements, there is more or less intensive cooperation with the different EU Member States.

3. TRAINING/EXERCISES FOR TESTING THE NATIONAL CRISIS CENTRE AND COMMUNICATION SYSTEMS IN CASE OF TERRORIST ATTACK

Training and exercises for testing the National crisis centre and communication systems in case of terrorist attack are carried out annually. Exercises include engagement with local and regional responders as well as international partners.

The different exercises are an important element in ensuring readiness in the face of terrorist attacks. The authorities in the UK give special importance to the exercises. After each exercise an evaluation process takes place, where lessons learned are captured.

An Exercise Unit within the OSCT engages in the preparation and conduct of exercises. Six exercises were conducted in the UK in 2006 and 2007. The financial impact of these exercises was between £200,000 and £1.5 million each.

Following an ACPO review of police exercising, a new A National Counter Terrorist Exercise Programme was adopted by the competent political decision makers for the period 2008 to 2012. The new Programme provides for three exercises per year involving each of the nine regions of the UK at least once. One exercise per year is devoted to CBRN issues. The new Programme now includes a significant preparatory build towards each live play CT exercise and incorporates specific objectives relating to the Olympic Games in London in 2012. Clear policies on how to deliver the exercises as well as clear debriefing procedures are in place.

Within three months of the end of an exercise, there is an overall debriefing as well as an assessment of local and strategic lessons learned.

CT exercises are in principle focused on three different priorities which can be combined:

- Command and control structure;
- Crisis management;
- Communication;
- Five different types of exercises are in place:
 - Tier 1: COBR and Central Response;
 - Tier 2: COBR Workshop or COBR Tabletop Exercise;
 - Tier 3: Departmental Exercise;
 - Tier 4: Regional Exercise;
 - Tier 5: Local Exercise Activity.

Transnational exercises on Tier 1 and Tier 2 have not yet been conducted. However, the authorities of Kent have carried out joint exercises with the French authorities in the Channel tunnel.

4. SOFT TARGETS

Both the political and operational levels put special emphasis on the following areas:

- Crowded places;
- Critical national infrastructure;
- Hazardous sites.

The operational police unit that covers the “Protect” issues of CONTEST is the National Counter Terrorism Security Office (NaCTSO), a police unit working for the Association of Chief Police Officers (ACPO) **NOT DECLASSIFIED**. NaCTSO are responsible for tasking **NOT DECLASSIFIED** Counter-Terrorism Security Advisers throughout the country offering their services on request, including to big companies which handle high technology equipment and have access to sensitive information and technology. In addition to this, and to increase public awareness, informative books and leaflets are regularly published and distributed.

With OSCT, and a number of other national and local stakeholders, NaCTSO are responsible for implementing the recommendations of a review, undertaken by Lord West in 2007, about how best to protect crowded places. A key finding of that review was to highlight the importance of engaging with a wide range of local partners, in particular local authorities and local businesses to encourage them to implement counter-terrorist security advice. The review also recommended that protective security measures must be proportionate to the risk. Individuals and businesses must be free to carry on their normal social, economic and democratic activities. To help target this work, the UK has developed a risk based approach to the protection of crowded places. Alongside this, The UK is also doing much to promote design in counter terrorism protective security measures with planners and architects.

The UK has recently concluded a public consultation about its work on crowded places with a view to publishing two guidance documents for national and local stakeholders: “Working Together to Protect Crowded Places” and “Safer Places: A Counter Terrorism Supplement”.

Particular attention is given to possible attacks on crowded places **NOT DECLASSIFIED**. According to the UK assessment, the most likely target for a crowded places attack is one which is easily accessible, regularly available and offers the prospect for an impact beyond the loss of life alone. Additionally, a crowded place with iconic status, or which has interests that are terrorist targets in their own right, are likely to be preferred over similar venues with no such associations. Such attacks can be conducted by groups with a relatively limited level of expertise. Terrorists worldwide have for example targeted nightclubs (e.g. Bali, 2002) and hotels (e.g. Egypt, 2005 and Jordan, 2006).

Longstanding and regularly activated major incident plans and structures are in place across government. The adaptability and expertise of the emergency services provides a solid basis for handling a mass casualty incident. For example, Ambulance Trusts and other NHS organisations have an excellent track record in dealing with major incidents and regularly exercise their major incident plans. The Urban Search and Rescue20 (USAR) capability for the Fire and Rescue Service, provided through the New Dimensions programme, has now been fully rolled out across the service.

Public transport (in particular Rail, Underground and Air) is also the subject of special attention. Conventional attacks on transport systems are judged to be some of the more likely to occur,; although the likelihood of them affecting any one individual is still considered very low.

Tight security measures are applied at airports. Rail and underground networks, however are open systems, which is likely to make them attractive potential targets for terrorist attacks. As a result, there have been several successful attacks on rail networks worldwide.

On 7 July 2005 the London transport system was attacked with 4 explosions (3 on underground trains, 1 on a bus). This was followed by unsuccessful attacks against the London transport system two weeks later. There have also been a number of recent examples in other countries of successful attacks against underground systems (e.g. Moscow, 2004) and mainline rail services (e.g. Madrid, 2004).

Security for the national rail network, as well as the London Underground, the Docklands Light Railway and the Glasgow Subway, is regulated by the Department for Transport, which inspects and monitors compliances. These system are considered more vulnerable because of the large amount of passengers and goods going through. The British Transport Police are responsible for policing the UK rail networks and are closely involved in contingency planning, as well as working with industry and the Department for Transport on security issues.

The special case of Eurostar services through the Channel Tunnel are subject to a more stringent security regime similar to that which exists at airports, under which all passengers and their baggage are currently subject to screening.

For aviation security, stringent protective security measures exist at UK and EU Member State airports. Airlines and airports are required to carry out a range of specified measures. These include the following measures to mitigate the risk of attack:

- Screening of passengers and their bags, as well as of all staff working in restricted areas;
- Physical security measures including the separation of incoming international passengers from all outbound travellers; and background checks on staff in sensitive posts.
- Security measures are also in place to protect aircraft in flight, such as the compulsory locking of Cockpit doors. These security regimes are regularly inspected by the Department for Transport's
- Transport Security & Contingencies Directorate (TRANSEC) to ensure compliance. In addition, TRANSEC provides advice to UK airlines operating overseas on measures needed at their foreign stations.

The unit that covers the "Protect" issues of CONTEST is the National Counter Terrorism Security Office (NaCTSO), a police unit working for the Association of Chief Police Officers (ACPO) that performs a coordinating role for the police service in regard to counter-terrorism and protective security. **NOT DECLASSIFIED** advisors operate throughout the country offering their services on request, including to big companies which handle high technology equipment and have access to sensitive information and technology. In addition to this, and to increase public awareness, informative books and leaflets are regularly published and distributed.

The main criterion for the impact assessment is the potential loss of life. **NOT DECLASSIFIED**
The approach is persuasion and not legislation as well as instilling awareness of the need to take responsibility. Developing and maintaining strong links with other organisations is vital for this task.

Part of the activities of the NaCTSO is the training of **NOT DECLASSIFIED** Counter Terrorism Security Advisors (CTSA), police officers in the field who provide advice to business and the community on CT protective security measures. The CTSA receive a two-year training package which covers topics including Security Surveys, Terrorist Weapons and Explosives, Personnel Security, and IT Security.

The deployment of the CTSO is financed by the Home Office. They report back to ACPO and the Government via NaCTSO. These reports are evaluated within the CONTEST2 framework.

NOT DECLASSIFIED

Particular attention is given to possible attacks on crowded places **NOT DECLASSIFIED**. According to the UK assessment, the most likely target for a crowded places attack is one which is easily accessible, regularly available and offers the prospect for an impact beyond the loss of life alone. Additionally, a crowded place with iconic status, or which has interests that are terrorist targets in their own right, are likely to be preferred over similar venues with no such associations. Such attacks can be conducted by groups with a relatively limited level of expertise. Terrorists worldwide have for example targeted nightclubs (e.g. Bali, 2002) and hotels (e.g. Egypt, 2005 and Jordan, 2006).

Longstanding and regularly activated major incident plans and structures are in place across government. The adaptability and expertise of the emergency services provides a solid basis for handling a mass casualty incident. For example, Ambulance Trusts and other NHS organisations have an excellent track record in dealing with major incidents and regularly exercise their major incident plans. The Urban Search and Rescue20 (USAR) capability for the Fire and Rescue Service, provided through the New Dimensions programme, has now been fully rolled out across the service.

Considerable work is underway, led by the Home Office, in conjunction with the National Counter Terrorism and Security Office (NaCTSO) and local police Counter Terrorism Security Advisors (CTSAs), and with the close engagement of local partners, to put in place a consistent framework for reducing the vulnerability of crowded places across the UK. This has included establishing a standard way for CTSAs to assess vulnerability to terrorist attack of crowded places which will enable local partnerships to prioritise their work and evaluate its protective impact.

A publication entitled "Safer Places – the Planning System and Crime Prevention" ' provides guidelines on how to design counter terrorist measures, thereby extending general public resilience.

Public transport (in particular Rail, Underground and Air) is also the subject of special attention. Conventional attacks on transport systems are judged to be some of the more likely to occur,; although the likelihood of them affecting any one individual is still considered very low.

Tight security measures are applied at airports. Rail and underground networks, however are open systems, which is likely to make them attractive potential targets for terrorist attacks. As a result, there have been several successful attacks on rail networks worldwide.

On 7 July 2005 the London transport system was attacked with 4 explosions (3 on underground trains, 1 on a bus). This was followed by unsuccessful attacks against the London transport system two weeks later. There have also been a number of recent examples in other countries of successful attacks against underground systems (e.g. Moscow, 2004) and mainline rail services (e.g. Madrid, 2004).

Security for the national rail network, as well as the London Underground, the Docklands Light Railway and the Glasgow Subway, is regulated by the Department for Transport, which inspects and monitors compliances. These system are considered more vulnerable because of the large amount of passengers and goods going through. The British Transport Police are responsible for policing the UK rail networks and are closely involved in contingency planning, as well as working with industry and the Department for Transport on security issues.

The special case of Eurostar services through the Channel Tunnel are subject to a more stringent security regime similar to that which exists at airports, under which all passengers and their baggage are currently subject to screening.

For aviation security, stringent protective security measures exist at UK and EU Member State airports. Airlines and airports are required to carry out a range of specified measures. These include the following measures to mitigate the risk of attack:

- Screening of passengers and their bags, as well as of all staff working in restricted areas;
- Physical security measures including the separation of incoming international passengers from all outbound travellers; and background checks on staff in sensitive posts.

- Security measures are also in place to protect aircraft in flight, such as the compulsory locking of Cockpit doors. These security regimes are regularly inspected by the Department for Transport's
- Transport Security & Contingencies Directorate (TRANSEC) to ensure compliance. In addition, TRANSEC provides advice to UK airlines operating overseas on measures needed at their foreign stations.

Non-conventional attacks (CBNR attacks)

There is a well developed capability amongst the emergency services and other responder agencies to deal with industrial accidents involving hazardous materials. The emergency services are also well versed in dealing with terrorist incidents involving conventional explosives. When dealing with a potential terrorist incident involving unconventional materials, many of the same procedures and equipment can therefore be applied.

The emergency services receive specialist training and are provided with protective equipment and the relevant supplies in order to enable them to operate in hazardous environments and to rescue and treat any casualties. The Ambulance and Fire and Rescue Services have means to decontaminate people affected by such an incident.

Accordingly, there is planning for such events at national, regional, and local level and regular testing of the plans through exercises.

Where necessary, decontamination of the area of any incident, so that it can be returned to normal use, can be undertaken by contractors drawn from a framework established by the Government Decontamination Service.

Local authorities have plans in place to open reception centres for those caught up in incidents or displaced from their homes.

5. GOOD PRACTICES

- The basic principle – namely keeping responsibility at the most local level possible and having support and strategic consultancy provided by the government – is a useful way of sharing competencies, and avoids complex and long decision-making processes.
- The UK Counter Terrorism Strategy (CONTEST2) is foundation for all work on terrorist threats. All competent authorities have to follow 4 points, the so-called 4Ps (prevent, pursue, protect, prepare) and thus ensure consistency in the implementation of the existing programmes and action plans.
- The Government Liaison Teams (GLTs) support and advise the local authorities, as well as an important communication and information channel.
- The CT strategy (prepare, prevent, protect, pursue) is the basis for all areas and thus ensures consistency.
- Government entities and private companies (trade and industry) closely cooperate in the development of technologies for the protection of sensitive areas (crowded places, critical infrastructures).
- As for preparedness for crisis and crisis management, the structure of the police authorities, from the Association of Chief Police Officers (ACPO) to the regional and local headquarters (Gold, Silver and Bronze Commands) provides the ideal basis for optimal planning and carrying out of operations.
- Transparent information management by government entities (register accessible on the Internet, threat level, leaflets for different scenarios etc) raises the awareness of the general public and increases understanding of measures to increase security.

- Regular exercises at different levels (national, regional, local) in different regions under different scenarios and also involving other countries, including post-exercise debriefing on the basis of the procedure matrix, permit a continuous improvement of reaction capacities.
- The close cooperation between the OSCT, the NaCTSO and the competent government agencies guarantees a balanced set of programmes and measures.
- The implementation of the HERMIS plan aims towards the valid and timely briefing of all diplomatic missions in London in cases of incidents with massive losses or other serious events that could happen in the country. This is rightly considered best practice because all embassies are kept informed about the events, leaving the police free to do their job without distractions.
- A National Counter Terrorist Exercise Programme has been adopted by the responsible political decision makers and covers the period from 2008 to 2012.

6. RECOMMENDATIONS

NOT DECLASSIFIED

7. ANNEX

7.1. Presentations were made by the following institutions

- Office for Security and Counter terrorism (OSCT)
- Foreign and Commonwealth Office
- National Counter terrorism Security Office (NACTSO)
- Fire Services
- Department for environment Food and Rural Affairs (DEFRA)
- Ministry of Defence (MOD)
- National Communication Centre Office
- Cabinet Office
- Civil Contingencies Secretariat Cabinet Office
- Home Office

7.2. Speakers

NOT DECLASSIFIED

7.3. Expert Team
Council General Secretariat

NOT DECLASSIFIED

Police and Customs Cooperation Unit - DG Justice and Home Affairs

European Commission

NOT DECLASSIFIED

Directorate General, Justice, Freedom and Security

Cyprus

NOT DECLASSIFIED

Chief Inspector - Ministry of Interior

Austria

NOT DECLASSIFIED

Federal Ministry of Interior - International relations

Europol

NOT DECLASSIFIED

Serious Crime Department – Counter Terrorism
