

The United Kingdom's
Strategy for Countering
Chemical, Biological, Radiological
and Nuclear (CBRN) Terrorism

March 2010



**The United Kingdom's Strategy
for Countering Chemical, Biological,
Radiological and Nuclear (CBRN) Terrorism**

March 2010

© Crown Copyright 2010

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned

ISBN: 978-1-84987-201-0

Contents

The United Kingdom's Strategy for Countering Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism

Ministerial foreword: Admiral the Lord West of Spithead	3
Part 1 Strategic context	5
Part 2 Our strategy for countering CBRN terrorism	8
Part 3 Delivering the CBRN strategy	15
Part 4 Conclusion	18
Annex E Roles of Government Departments, Devolved Administrations and Agencies	19
End notes	24

Ministerial foreword

Admiral the Lord West of Spithead

Parliamentary Under-Secretary of State, Home Office



The UK and UK interests overseas continue to face a significant threat from international terrorism. The Government's strategy for responding to this threat, known as CONTEST, was updated and published in March 2009.

CONTEST explains how contemporary terrorist organisations aspire to use chemical, biological, radiological and even nuclear (CBRN) weapons. The availability of information on the internet, changing technology and the theft and smuggling of CBRN materials make this aspiration more realistic than it may have been in the past.

This document, which has been produced by the Office for Security and Counter-Terrorism in the Home Office, sets out the UK's strategy for countering the threat posed by terrorist use of CBRN materials.

Our aim is to reduce the likelihood of a CBRN attack and, if an attack should occur, respond quickly to minimise harm and restore public confidence.

This strategy paper also describes some of the significant progress which we have made in countering this threat and highlights work which we plan to do over the next three years. It rightly emphasises work with our international and private sector partners and the important contribution of scientific research and the innovative use of technology. This reflects principles set out in our CONTEST Science and Technology strategy, also published last year.

The success of all our counter terrorist work depends on collaboration across Government Departments, Devolved Administrations, the responder community and international and private sector partners. I commend the progress which has been made and believe this strategy will facilitate further progress in future.

West of Spithead

ADMIRAL the LORD WEST of SPITHEAD,
GCB, DSC, DUniv

1.01 The 2009 National Security Strategy¹ identifies international terrorism as the most significant immediate security threat to the UK.

1.02 CONTEST is the Government's counter Terrorist strategic response.

1.03 Countering chemical, biological, radiological and nuclear (CBRN) terrorism requires activity in all four CONTEST work streams:

- *Prevent* - to stop people becoming terrorists or supporting violent extremism;
- *Pursue* - to stop terrorist attacks;
- *Protect* - to strengthen our protection against terrorist attack, and;
- *Prepare* - where an attack cannot be stopped, to mitigate its impact.

1.04 CONTEST is based on a set of principles, which apply equally to this CBRN strategy. These reflect our core values, the lessons which we and others have drawn from our experiences of terrorism, and the broader security principles set out in the National Security Strategy:

- we will continue to regard the protection of human rights as central to our counter-terrorism work in this country and overseas;
- our response to terrorism is and will continue to be based upon the rule of law;
- we will always aim to prosecute those responsible for terrorist attacks in this country;
- we will tackle the causes as well as symptoms of terrorism;

- reducing support for terrorism and preventing people from becoming terrorists are vital;
- our strategy must be responsive to the threat that can be created by evolving technology;
- partnerships in this country and overseas are essential to our success; these partnerships
- depend on openness and trust; and
- the threat which we face is international in scope; we will depend on our allies as they will depend on us.

CBRN materials

1.05 Chemicals, combined with explosives, may be used as small-scale (assassination or poisonings) or large-scale (mass-casualty) weapons. Some chemical weapons have used toxic industrial compounds; others have deployed agents specifically developed for warfare. Chlorine gas, an industrial chemical, was used during the First World War to kill or debilitate troops. During and after the Second World War, more sophisticated chemicals (such as the nerve agents Sarin, Tabun and VX) were developed for use in munitions. Their deployment during the Iran-Iraq war had a devastating impact.

1.06 Biological weapons may be used to attack people or infrastructure (e.g. food and water supplies). Anthrax was developed and tested in the First World War as a means to contaminate animal feed but it can be developed to attack humans. The accidental release of anthrax spores from a military research laboratory in the former Soviet Union in 1979 is believed to have killed over 60 people. Anthrax attacks in the US in 2001 killed 5 and infected 17: the clean up costs were substantial.



1.07 Radiological material can be combined with explosives to produce a radiological dispersion device (RDD), sometimes called a 'dirty bomb', which will contaminate people and buildings. Nuclear or fissile material may be used to develop an improvised nuclear device (IND), creating a nuclear explosion. An IND remains the most devastating of all CBRN devices.

1.08 Contamination makes recovery from a CBRN attack significantly more challenging than recovery from other terrorist atrocities. The clean-up process may be protracted as well as unfamiliar and untested.

1.09 The terms 'CBRN terrorism' and 'Weapons of Mass Destruction (or WMD) terrorism' are sometimes used interchangeably. This is misleading. Not all CBRN devices are weapons of mass destruction: indeed, many are not. But they do have the capability to cause significant disruption and loss of life.

The CBRN threat to the UK

1.10 Al Qa'ida is the first transnational organisation to support the use of CBRN weapons against civilian targets and to try to acquire them. During the rule of the Taliban, Al Qa'ida established facilities in Afghanistan to conduct research into CBRN weapons and to provide training. Some of the training was rudimentary and related to 'lower end', simple CBRN devices, including so-called contact poisons. Other training – and research – addressed more sophisticated weapons and materials.

In 2001, Al Qa'ida held talks with two disaffected Pakistani nuclear scientists about acquiring or developing nuclear weapons. By 2003, Al Qa'ida had developed a device to produce hydrogen cyanide gas, intended for use in crowded urban spaces². In 2004, Al Qa'ida associated cells in the UK considered the use of radiological devices³ and in 2006, the leader of Al Qa'ida in Iraq appealed for nuclear scientists to join his group and attack US bases in Iraq using non-conventional weapons⁴. In 2007, Al Qa'ida in Iraq deployed a number of explosive devices in combination with chlorine gas cylinders⁵.

1.11 Al Qai'da's aspirations have been disrupted by intelligence, military and law enforcement action and specifically by an absence of technical expertise, material, training and research facilities. Although coalition activity in Afghanistan has continued to inhibit Al Qai'da from developing CBRN programmes we believe this remains their aspiration.

1.12 Some other terrorist groups have also expressed an interest in acquiring or developing CBRN capabilities.

1.13 Four factors have increased the risk that terrorists may acquire CBRN weapons:

- **there has been a significant increase in the trafficking of material** which can be used in radiological and conceivably in nuclear weapons. This is a relatively recent phenomenon directly related to the end of the Soviet Union. Between 1993 and 2008, 1562 incidents of unauthorised activities,

Part 1

events, thefts or losses were reported to the International Atomic Energy Authority (IAEA). Their database shows that 65% of the losses over that period have never been recovered⁶;

- **the internet** has made more widely available information on the technology of CBRN devices and the materials which might be used to develop them;
- **CBRN materials are used for legitimate purposes**, notably in nuclear energy, medical science and biotechnology. The production and use of these materials significantly increases the risk that they may be diverted and exploited by terrorist organisations; and
- **security around stockpiles of decommissioned military CBRN material** is variable and sometimes inadequate, leaving materials vulnerable to theft by insiders and criminal and terrorist organisations.

2.01 CONTEST sets out for the first time the measures we have taken in recent years to deal with the threat posed by the terrorist use of CBRN. Some of the details of these programmes are reproduced here, together with priorities for work over the next 3-5 years. In all cases details have had to be omitted for reasons of security and safety.

2.02 The aim of our counter Terrorist CBRN work is to stop a CBRN attack and where that is not possible, to put in place measures to ensure that we can recover from it quickly and with minimal loss of life. In common with CONTEST in general we therefore seek to reduce the likelihood and impact of attacks and by both means to reduce the risk to this country.

2.03 In planning and prioritising our CBRN work, we take into account current intelligence, our assessment of the future threat and the Cabinet Office classified National Risk Assessment (NRA). The NRA considers the range of emergencies that might have a major impact on all, or significant parts of, the UK and, in a risk matrix, compares their likelihood and impact. The National Risk Register (NRR) is a published document based on the NRA⁷.

2.04 The Government has recently completed a review of counter Terrorist related CBRN work since 09/11, identifying both strengths and gaps. This review will remain classified but also significantly informs the detail of our forward looking programmes

2.05 In determining our priority programmes for the future within the strategic objectives set out below, we will in principle give priority to:

- completing existing programmes;
- maintaining current capabilities; and

- developing and delivering new capabilities which have significant and timely impact at low cost.

Success means that:

- those who remain intent on carrying out an attack are disrupted and brought to justice;
- CBRN materials used in any attack can be identified and attributed wherever possible;
- the material, knowledge and other resources required to deliver a CBRN attack cannot be acquired by terrorist organisations.
- the Critical National Infrastructure (CNI) and crowded places are protected against CBRN attacks; and
- should an incident occur, emergency responders can respond quickly, safely and effectively to minimise casualties and recovery time.

Strategic objectives

2.06 Our objectives cover issues relating primarily to three of the key work streams of CONTEST: Pursue, Protect and Prepare.

Objective: stop terrorists from carrying out an attack (Pursue)

2.07 The security and intelligence agencies and the police are responsible for finding those who are intent on acquiring or using CBRN material: intelligence can provide an early indication that a terrorist organisation is developing or deploying CBRN capability; that CBRN related materials or designs are being traded or sold; or that the security of state CBRN programmes around the world has been compromised.

Part 2



2.08 This work draws on the resources allocated to policing and the agencies to investigate and disrupt a conventional terrorist attack. These resources are summarised in more detail in our published CONTEST strategy.

2.09 A sophisticated forensic capability may be required to provide evidence in the event of a prosecution of those planning a CBRN attack. The Government has established a National Network of Laboratories (NNL), for the rapid analysis of chemical and biological material to accredited standards. Operational from 2005, the NNL is an example of the Government working across departments and with private industry.

2.10 Intelligence not only enables the disruption of a specific threat but also informs and improves the effect of interventions made under other objectives set out below.

Next steps

2.11 The Cabinet Office has led the development of a CBRN Intelligence Strategy, the aim of which is to maximise the effectiveness of the agencies' contribution to countering the global threat from CBRN terrorism through a 'single mission' approach. For security reasons this has to remain unpublished. Implementation of this strategy will be overseen by the Pursue delivery board in the CONTEST structures.

2.12 OSCT is leading work to establish further CBRN forensic capabilities, from recovery through to analysis. This work is supported by the Ministry of Defence and the Home Office Scientific Development Branch (HOSDB).

Our requirements include:

- improved techniques for at-scene CBRN sampling;
- accredited techniques for laboratory analysis of CBRN materials in a range of evidence including environmental samples, food, and body fluids; and
- detailed guidance on optimal handling and storage of clinical samples.

Objective: deny terrorist access to CBRN materials (Protect)

2.13 Many CBRN materials or precursors are widely available and are found throughout society. We need to deny terrorists access to this material, to knowledge about their use as weapons and specifically to the people with that knowledge and relevant training.

2.14 The police National Counter Terrorism Security Office (NaCTSO) and the Centre for the Protection of National Infrastructure (CPNI) jointly support the provision of specialist advice on the security of what are



often termed ‘hazardous substances’ (meaning, in this context, substances which may have a CBRN application).

2.15 Through its network of counter-terrorism security advisors (CTSAs), NaCTSO has provided security advice to almost 2000 sites where hazardous material is stored. NaCTSO ‘Know Your Customer’ campaigns have raised awareness about the “dual-use” of certain products, encouraged suppliers to be more enquiring of new customers and to report suspicious activity.

2.16 NaCTSO has developed an awareness raising programme for the academic sector, facilitated by CTSAs. NaCTSO also enforces Part 7 of the Anti Terrorism, Crime and Security Act 2001 (ATCSA) which requires laboratories holding certain pathogens and toxins to put in place specified security measures.

2.17 The policy lead on civil nuclear security matters lies with the Department of Energy and Climate Change (DECC); the Office for Civil Nuclear Security (OCNS) sets the requirements for security measures through the Nuclear Industries Security Regulations 2003; the Civil Nuclear

Constabulary is responsible for operational policing to meet the regulatory requirements. In 2009 the Office for Security and Counter Terrorism (OSCT) in the Home Office with Civil Nuclear Constabulary (CNC) and DECC, completed a classified report into nuclear security from which the recommendations are being implemented.

2.18 The Government has introduced radiological detection systems at UK borders to prevent the illegal importation of radiological materials. Freight and people, in vehicles or on foot, are screened as they pass through fixed portals or Mobile Radiation Detection Units (MRDUs). This work is now led by the UK Border Agency (UKBA).

2.19 The UK is committed to the full implementation of UN Security Council Resolution 1540 which addresses the role of non-state actors in proliferation of CBRN weapons. The UK is a leading partner in international collaboration on CBRN security, supporting work to secure nuclear materials and programmes under the Chemical Weapons Convention (CWC) and the Biological and Toxin Weapons Convention (BTWC).

Part 2

2.20 The Global Threat Reduction Programme (GTRP) plays an important role in denying terrorists access to CBRN materials. This ten-year, \$20 billion initiative was launched by the G8 at the Canadian Kananaskis Summit in 2002 and now involves more than 20 donors. The aims of the GTRP are to: improve the security of fissile materials; reduce the number of sites containing nuclear and radiological material; contribute to the destruction of chemical weapons stocks; and provide sustainable employment for former weapon scientists whose expertise could otherwise be acquired by terrorist organisations. GTRP is the UK's largest cooperative counter-proliferation assistance programme.

2.21 We are also playing a key role in the 2010 Nuclear Security Summit to be held in Washington DC.

Next steps

2.22 We will continue with programmes to reduce the possibility of terrorists gaining access to hazardous sites and substances through further work to improve security and awareness.

2.23 We will assess security arrangements at sites where CBRN materials are stored or processed.

2.24 We will continue to update the list of protected pathogens within the scope of ATCSA

2.25 We will continue to install systems to detect illicit radiological material, and improve our storage and analysis facilities for any material which is found.

2.26 We will support the EU CBRN Action plan and other international initiatives to help countries develop capabilities to stop the acquisition and use by terrorists of CBRN materials terrorists. (See para 3.18)

Objective: Reduce our vulnerability to a CBRN attack (Protect)



2.27 We can reduce our vulnerability to CBRN terrorism by ensuring that our infrastructure is resilient to an attack using CBRN materials and that, wherever possible, we "design out" weakness. The public also have an important part to play by being alert to and reporting suspicious behaviour and creating a hostile environment for terrorist operations.

2.28 Developments in this area are dependent on and make use of other CONTEST programmes to improve protective security. Much of this work is led by NaCTSO and CTAs (para 2.15 above) who have provided protective security advice to over 500 sports stadia, 600 shopping centres and 10,000 pubs and clubs.

2.29 CPNI has advised private sector organisations, particularly those who own parts of the CNI, on specific design improvements to protect them from the effects of CBRN agents. Measures have been taken by the utility organisations, for example the water and food industries.

Part 2

Next steps

2.30 NaCTSO is devising a web-based Vulnerability Self-Assessment Tool (VSAT) designed to help those responsible for public safety at crowded places to assess security and identify protective security measures required to address any vulnerabilities. We will be working with NaCTSO to address vulnerabilities specific to CBRN.

Objective: respond promptly and effectively to a CBRN attack and recover as quickly as possible from its impact (Prepare)

Detection

2.31 Rapid response to a CBRN attack requires early detection of materials which have been released by terrorists. In its simplest form, detection may be simply based on obvious medical signs and symptoms amongst affected people. However, in most cases detection will involve the use of specialist equipment by trained personnel.

2.32 Some CBRN substances (e.g. biological agents and some radiological sources) are more difficult to detect than others. However, early detection of all agents will assist in ensuring that medical countermeasures such as antibiotics and other drugs are available in a timely and effective manner.

2.33 We have conducted a comprehensive review of detection, identification and monitoring equipment and have collaborated with industry and international partners to assess existing biological detection equipment in particular. Such systems vary from those that are portable and relatively simple in operation to those that are very sophisticated that can be operated remotely and automatically.

2.34 The police and fire and rescue services have received detection equipment to assist in the event of a CBRN incident.

2.35 We have increased the number of military and police personnel trained to search and render safe CBRN devices.

Next steps

2.36 We will work with industry and international partners to develop:

- detection techniques and equipment for a variety of applications (aerial survey, stand-off, remote, hand-held and portable) and with improved performance and ease of handling (sensitivity, specificity, false alarm rates, limit of detection, distance from source, time to detection, size, weight etc);
- improvements in bio-detector integration, i.e., integrated collection, sample processing, sensing and signal analysis;



Part 2

- aids for the identification of chemical contamination on skin, hair or clothing to assist the emergency services;
- rapid diagnostic techniques for the detection of chemical agents including in mixed samples; and
- rapid biological detection equipment which can be deployed to provide an early indication of the release of biological or other agents.

Managing the impact of an attack

2.37 Over the past five years, we have built up our resource to improving preparedness.

2.38 We have created “The Model Response to CBRN Events”, a classified document to guide responding agencies and the emergency services and provide a holistic picture of an ideal response to a CBR attack (the Model does not apply to “N” - the scale of a nuclear explosion requires a different approach.) The Model Response details the actions required, and when, where and by whom those actions would be carried out.

2.39 Initial programmes to provide capabilities to meet the Model Response are largely complete.

2.40 The Police Operational Response Programme (PORP) was established to enable the police to meet the requirements of the Model Response. A national police CBRN centre has been established which is also available to other emergency services. The centre has delivered CBRN equipment into service. Over 5,000 partners have been briefed on responding to a CBRN attack, and over 650 emergency service commanders or police responders have attended and completed specialist courses. To enhance and maintain capability, exercises have been managed or supported by the centre’s exercise team.

2.41 We have equipped 18 sites nationwide with trained officers to improve the multi-agency response to a CBRN attack and have improved Command procedures through the provision of tactical guidance, training and exercising.

2.42 The centre runs a 24/7 operations facility which has provided advice and support to over 100 incidents where suspected CBRN materials have been found. 10,000 CBRN-trained police officers have been deployed across the UK.

2.43 CBRN training on mass decontamination has been provided for 90% of fire and rescue personnel to enable them to reduce public exposure following contamination.

2.44 Hazardous Area Response Teams (HART) are being introduced in the ambulance services. These teams specialise in operating in the contaminated zone so that those affected can receive treatment as soon as possible.

Next steps

2.45 We will ensure that we maintain the levels of trained and equipped police officers, fire and rescue service decontamination units and HART to deliver the Model Response.

2.46 We will complete our work on an improved protocol for the provision of timely and reliable scientific advice in a crisis both to first responders and decision-makers.

2.47 We will explore options for enhancing the UK’s medical response through stockpiling drugs and vaccines to mitigate the effects of exposure to a CBRN attack.

2.48 We will review performance and assessment standards for equipment so that industry can make more confident decisions on future investment. We will also seek opportunities for joint procurement to reduce costs for detection equipment and improve equipment compatibility and interoperability across the emergency services.

2.49 Exercises continue to be essential. We will test response arrangements to CBRN attacks at local level by exercising the emergency services and other responding agencies and feed the lessons identified into operational training and response plans. We will also review arrangements for command and control and scene assessment.

Part 2

The recovery phase

2.50 Recovering from a CBRN incident requires: rapid removal of any residual hazard; re-occupation of domestic and business premises; return to normal function of local essential services and the provision of longer-term health care and advice. We need to plan for all of these at the earliest opportunity so that a return to normality can be achieved as rapidly as possible.

2.51 We have established, through the Government Decontamination Service, a contractor framework of specialist companies, enabling expert advice and decontamination expertise to be brought to bear as quickly as possible following CBRN attacks.

2.52 We are the first Government anywhere in the world to have produced guidance on the tolerability of residual hazards^{8,9}. This classified guidance enables rapid, sound decisions to be made on when previously contaminated areas can be safely reoccupied by the public.

2.53 We are one of the first countries to have carried out a national CBRN recovery exercise, involving national and local government and the emergency services, to help identify issues that might arise if there was an actual attack.

Next steps

2.54 Our aim is to further minimise and contain the hazard associated with a CBRN release. We will do this in collaboration with industry and International partners. In particular we will address:

- containment of CBRN materials either pre- or post-release to limit the impact of an attack;
- reducing the amount of CBRN waste produced as a result of the decontamination process (especially for radiological releases);
- decontamination of extended areas, individuals and personal effects;

- use of expedient, non-specialist, methods for the urgent reduction of levels of contamination at scene;
- environmental sampling capability required to measure the extent of contamination; and
- practical exercises to test recovery capability.

3.01 The published CONTEST strategy concludes with a section on delivery, describing performance management, governance, funding, resources and key partnerships. This section considers the more specific issue of CBRN delivery.

Performance management

3.02 Performance on counter-terrorism is addressed in Public Service Agreement (PSA) 26. The PSA is based on the four main work streams of CONTEST. Under each one, there are a number of anticipated outcomes, progress towards which is measured using specific indicators.

3.03 CBRN features significantly in the outcomes we are seeking under the *Prepare* work stream. Our progress in reaching those outcomes is therefore assessed in part with reference to the progress of programmes summarised here. CBRN work also features in the objectives of key agencies and departments.

Governance

3.04 In the National Security and International Development (NSID) structure responsibility for matters regarding protective security and resilience against the terrorist use of CBRN weapons lies with NSID PSR chaired by the Home Secretary.

3.05 At official level the CONTEST Board provides direction for cross Government counter-terrorism CBRN work. The programmes are co-ordinated by a CBRN oversight board. Working level groups deal with more detailed issues (for example, Programme Cyclamen and Hazardous Substances).

Departments and agencies: roles and responsibilities

3.06 Annex A to this document summarises the roles of the key UK departments and agencies in the delivery of this counter-terrorism CBRN strategy.

Science and technology (S&T)

3.07 The Home Office-funded CBRN S&T Programme was established in 2004 to support the emerging civilian-based CBRN capability. Its aim is to address S&T requirements that are not part of departments' existing work, either because the requirements are broader than any one department's remit or because they fall between responsibilities. The S&T Programme is supported by a CBRN S&T board which is made up of the departments which manage the projects within the Programme.

3.08 In August 2009, the Government published the UK Science and Technology Strategy for Countering International Terrorism. The strategy outlines how science and technology can support all aspects of CONTEST. It also sets out objectives for the next three years:

- to use horizon scanning to understand future scientific and technical threats and opportunities, and inform our decision making on counter-terrorism;
- to ensure the development and delivery of effective counter-terrorism solutions by identifying and sharing priority S&T requirements; and
- to enhance international collaboration on counter-terrorism related S&T.

Part 3

3.09 Investment in S&T will be used to develop:

- technologies that could form the basis of future counter-terrorism CBRN capability;
- new knowledge or to exploit existing knowledge to inform future policy development, operational capability and science-based advice; and
- specialist facilities for the analysis of CBRN materials.

The key CBRN research topics include:

- detection of CBRN materials pre and post-release;
- modelling techniques to improve our ability to predict the behaviour of CBRN materials once released.
- initial treatment and long-term medical care for the largest number of people affected by an incident; and
- decontamination of people, materials and the environment.

Academia

3.10 A CBRN advisory sub-group under the Home Office Science Advisory Committee (HOSAC) provides advice on the quality of CBRN work commissioned and completed through the Home Office-funded S&T programme. The subgroup is drawn from academia and Government.

We intend to extend engagement with academia, through Research Councils, ‘think-tanks’ and learned societies to secure their help in the further scrutiny and development of our work.

Industry

3.11 The UK Security and Resilience Industry Suppliers Community (RISC) is an alliance of trade associations, companies, and “think-tanks” established in March 2007 to coordinate a dialogue on counter-

terrorism and security with Government. RISC has developed a close engagement with OSCT on counter Terrorism in particular.

3.12 Through RISC five joint industry Advisory Groups have been established in areas of particular importance to CONTEST:

- CBRN;
- CNI;
- information and Communication Technology;
- detection of attacks conducted by ‘suicide bombers’; and
- Olympic security.

3.13 The CBRN group, in common with the others, considers how to exploit Government-funded research, develop Government requirements, focus private sector investment and enable access to innovation. As a result each side has developed a deeper understanding of the other’s processes and expectations. Current work includes the creation of performance and test standards to help establish common goals for future industrial development of CBRN detection equipment and to improve the exploitation of novel developments arising from research.

3.14 OSCT has also established an industry engagement team to facilitate dialogue between policy makers and industry. The team will help industry access and talk to the Government ‘problem owners’ on security issues.

International collaboration

3.15 We will continue to support the development of a truly effective global effort to counter CBRN terrorism. This work is coordinated by the Foreign and Commonwealth Office (FCO). The FCO oversees closely related international work on counter-proliferation, counter-terrorism and organised crime. Its work is being

Part 3

delivered through diplomatic missions overseas and with the security and intelligence agencies.

3.16 The Overseas CONTEST Group (OCG) prioritises and coordinates counter terrorism work overseas under the FCO lead. The OCG also monitors implementation of international CBRN work.

International collaboration enables us to:

- share intelligence about terrorist CBRN capabilities and intentions and to disrupt terrorist CBRN operations;
 - identify and remedy poor security at nuclear (and other) sites;
 - disrupt trafficking of radiological and nuclear material;
 - restrict availability of chemical and/or biological precursor materials and equipment;
 - monitor the spread of sensitive information on the internet;
 - pool capabilities and share best practice which will facilitate recovery from a CBRN incident, and
 - leverage other countries' programmes of work.
- Prevention: reducing unauthorised access to CBRN materials;
 - Detection: improving the capability to detect CBRN materials; and
 - Preparedness and Response: improving the speed and effectiveness of our response to, and recovery from, CBRN events.

3.17 Some multilateral treaty based work is described above (para 2.19). But the UK CBRN community also has a range of international relationships to promote shared investments, mutual assistance, joint research and information exchange. These include quadrilateral arrangements with Australia, Canada and the US, bilateral arrangements with France and with the US, and other such partnerships. In particular, our relationship with the US is very productive and strong links are in place with the US's Department of Homeland Security, Department of Defense and Department of Energy.

3.18 The UK has played a major role in the development of an EU CBRN Action Plan which is fully aligned with the UK's priorities. The Plan aims to support the efforts of individual Member States to counter CBRN terrorism, and provides a framework for better co-operation. Delivery through this Plan is one of the Commission's priorities on counter-terrorism. Work is co-ordinated within the EU Commission by the Directorate-General for Justice, Freedom and Security (DG JLS) around three strategic themes, reflecting the objectives set out in this strategy:

4.01 The Government's commitment to addressing the challenges posed by international terrorism is set out in CONTEST.

4.02 The CBRN threat is complex and poses significant challenges for the UK, its people and its interests overseas.

4.03 Significant progress has been made in developing capabilities to deal with terrorist-related incidents involving CBRN materials but challenges remain. Given the complexity of the CBRN threat and its probable evolution we need a shared understanding of future objectives and priorities; we also need to create a broad community, in and outside Government, in this country and overseas, to ensure those objectives can be met. That is the purpose of this strategy.

Any further enquiries about this document can be addressed to OSCT in the Home Office at:

cbrnenquiries@homeoffice.gsi.gov.uk

Annex A: Roles of Government Departments, Devolved Administrations and Agencies

Cabinet Office

The Cabinet Office provides direct counter Terrorism advice to the Prime Minister, and the secretariat for the Ministerial Committee on National Security, International Relations and Development, and facilitates the coordination of the Government's crisis response via the Cabinet Office Briefing Rooms (COBR). The Cabinet Office oversees the Single Intelligence Account and also services the Joint Intelligence Committee, which sets strategic intelligence gathering priorities and delivers strategic intelligence assessments.

The Civil Contingencies Secretariat of the Cabinet Office coordinates the national Capabilities Programme for dealing with civil emergencies, including terrorism. The Capabilities Programme is designed to improve our ability to respond to both threats and other non-malicious hazards; the response to a terrorist attack would, in many instances, be applicable to other CBRN incidents such as an industrial accident.

www.cabinetoffice.gov.uk/ukresilience.aspx

Centre for the Protection of National Infrastructure (CPNI)

CPNI is the Government body responsible for protective security advice to owners and operators of the CNI. This includes sites that produce materials which might be used in CBRN attacks and sites which might be the target for CBRN attacks. The CPNI works closely with NaCTSO, which coordinates a nationwide network of specialist police CTsAs.

www.cpni.gov.uk

Department for Business, Innovation and Skills (BIS)

BIS has responsibility for certain import licences and export controls and works closely with Department of Energy and Climate Change (DECC) on fulfilling the UK's obligations on counter-proliferation.

www.bis.gov.uk

Department of Communities and Local Government (CLG)

CLG is the central government sponsor of local authorities and the local delivery framework (Government Offices [GOs], Local Strategic Partnerships [LSPs] and Local Area Agreements [LAAs]). CLG is also the sponsoring Department for the fire and rescue service (owned by the 46 local Fire and Rescue Authorities). Through its Resilience Programme, CLG provides the fire and rescue service with capabilities to respond to national scale emergencies including equipment provided under the New Dimensions programme. CLG coordinates the work of the regional GOs on preparing for major emergencies through the Regional Resilience Teams, working in partnership with Regional Resilience Forums and responder organisations. CLG works closely with Department for Environment Food and Rural Affairs (Defra) and the Environment Agency in connection with decontamination and the disposal of contaminated waste.

www.communities.gov.uk

Department of Energy and Climate Change (DECC)

DECC is responsible for ensuring that the UK continues to meet its obligations under the Chemical Weapons Convention (CWC) and the Biological and Toxin Weapons Convention (BTWC). CWC has legal effect in the UK through the Chemical Weapons Act 1996. The CWC and the Act place obligations on companies, universities, other bodies and individuals working with toxic chemicals in the UK.

DECC has the Departmental lead on civil nuclear security; the Civil Nuclear Constabulary (CNC) operates under its authority and is a predominantly armed police service dedicated to the protection of the nuclear industry with operational and support units based at nuclear sites in England, Scotland and Wales. DECC is accountable for the formulation of UK Government international policy on nuclear safeguards and other related nuclear non-proliferation issues in the context of the nuclear Non-Proliferation Treaty and the work of the IAEA.

www.decc.gov.uk

Department for Environment, Food and Rural Affairs (Defra)

The lead Government department for the recovery phase of a CBRN incident is Defra. Defra works closely with the Government Decontamination Service (GDS) [see below].

Defra is responsible for policies on the health and welfare of animals, food supplies, waste, and disruption to the water supply and sewerage system that might occur as a result of a terrorist attack. Through the Drinking Water Inspectorate (DWI) and Water Supply Regulation Division, Defra is responsible for notifying other stakeholders of actual/potential water supply emergencies and providing advice/support as necessary to Ministers, water companies and responders. The DWI maintains a call-off contract for 24/7 testing of water

samples collected by the water companies to identify contamination by chemical or biological agents. Local authorities are responsible for the testing of private water supplies.

www.defra.gov.uk

www.dwi.gov.uk

Department for Transport (DfT)

DfT aims to protect the travelling public, transport facilities and those employed in the transport industry from acts of terrorism through its Transport Security and Contingencies Directorate (TRANSEC).

www.dft.gov.uk

Department of Health (DH)

DH provides medical services in the event of a terrorist attack and will take control of NHS resources in England in the event of a complex and significant emergency – including those on a national and international scale – through its Emergency Preparedness Division coordinating centre. It will provide the coordination and focal point for the NHS in England and will coordinate as necessary with the health departments in the Devolved Administrations.

www.dh.gov.uk

Devolved Administrations

The Home Office retains the lead department role for the management of terrorist incidents across the UK, with the exception of Northern Ireland.

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. The NIO has lead Government Department responsibility for CBRN

Annexes

terrorism. However, the responsibility for consequence management falls to the Devolved Administration. Arrangements are in place to facilitate multi-agency coordination of the planning for, response to, and recovery from, such events. These arrangements are consistent with those in place to deal with incidents which affect all of the UK.

The Scottish Government and Welsh Assembly Government are responsible for coordinating wider impact management and recovery issues within their territory. The Scottish Government is also responsible for policing and criminal investigations in Scotland and a wide range of activity necessary for the delivery of an effective CBRN response in Scotland, for example fire and rescue services.

In Wales, the Welsh Assembly Government takes forward CBRN-related work through the Wales Resilience Forum where the planning for the consequences of a CBRN attack is overseen.

www.northernireland.gov.uk

www.scotland.gov.uk

www.wales.gov.uk

Environment Agency (EA)

The EA is responsible for protecting the environment from ground pollution and atmospheric pollution. It is also responsible for regulating and providing advice and support on waste disposal issues. The EA will provide a monitoring capability for chemical incidents whenever it has the corresponding sampling and analysis capability.

www.environment-agency.gov.uk

Food and Environment Research Agency - Government Decontamination Service (GDS):

In 2009, the GDS merged with a number of other Defra Agencies and assets to form the Food and Environment Research Agency (Fera) – an Executive Agency of Defra. Fera's purpose is to support and develop a sustainable food chain, a health natural environment and to protect the global community from biological and chemical risks; its role is to provide robust evidence, rigorous analysis and professional advice to Government, international organisations and the private sector. As part of Fera, the GDS has three main functions; the provision of high-quality advice and guidance to those who will be responsible for decontamination of a CBRN or significant HAZMAT incident; assessing the ability of specialist companies in the private sector to carry out decontamination operations; and ensuring that responsible authorities have ready access to those services if the need arises. Where required, the GDS will also help coordinate decontamination operations.

www.gds.gov.uk

Food Standards Agency (FSA)

The FSA has a statutory responsibility for ensuring the safety of the food chain (excluding tap water) and advising the public on food safety matters. The FSA may undertake testing, sampling and analysis of an area affected by potentially hazardous substances to determine the consequences for the food chain and take any necessary actions to protect public health.

www.food.gov.uk

Foreign & Commonwealth Office (FCO)

The FCO has overall responsibility for the delivery of CONTEST overseas, with other Departments and agencies across Government. The FCO leads the Overseas CONTEST Group (OCG), which

Annexes

is responsible for agreeing and keeping under review work in the priority countries and regions which pose the greatest terrorist threat to the UK and UK interests overseas.

www.fco.gov.uk

Government Communications Headquarters (GCHQ)

GCHQ leads on the collection of signals intelligence and provides information security advice and equipment to help protect Government information.

www.gchq.gov.uk

The Health Protection Agency (HPA)

HPA is an agency of DH, with a statutory duty to:

- protect the community against infectious disease and other dangers to health; and
- prevent the spread of infectious disease; and provide assistance on public health issues to the NHS, other responders, the devolved administrations and the wider general public.

The HPA will give advice on public health threats, including those associated with CBRN materials and may, where appropriate, make this advice public. HPA works closely with its counterparts in the devolved administrations.

www.hpa.org.uk

Health and Safety Executive (HSE)

HSE is the national regulatory body responsible for promoting the cause of better health and safety at work within Great Britain. HSE has been closely involved in the establishment of standards for decontamination to safe levels.

www.hse.gov.uk

Home Office Scientific Development Branch (HOSDB)

HOSDB provides expert advice and support to the Home Office and its partners on any issue relating to science and technology, creating new and innovative technical solutions. HOSDB helps the Home Office meet its strategic objectives in policing, crime reduction, counter-terrorism, border security and identity management. Examples of HOSDB's work include:

- providing technical know-how to improve video and CCTV operations
- developing techniques for identifying and detecting chemical and biological material
- developing techniques for ensuring the physical safety of government and other key buildings
- developing techniques for detecting hidden weapons and explosives
- evaluating methods of passenger screening
- evaluating CBRN detection and protective equipment.

www.scienceandresearch.homeoffice.gov.uk/hosdb

Joint Terrorism Analysis Centre (JTAC)

JTAC is the UK centre for the all source analysis and assessment of international terrorism. JTAC sets threat levels and issues analytical reporting to Government Departments and agencies.

www.mi5.gov.uk/output/joint-terrorism-analysis-centre.html

Annexes

Ministry of Defence (MOD)

The MOD contributes to all workstreams of CONTEST using its military capability. In the event of an attack that exceeds the capability or immediate capacity of the UK civilian response, the MOD can provide support through Military Aid to the Civil Authorities.

The Counter Terrorism Centre (CT Centre) serves as a hub to make the most of S&T resources in the MOD. While the primary objective of the CT Centre is to focus on MOD requirements, it can also help other Government Departments engaged in domestic counter Terrorism.

MOD, through the Defence Science and Technology Laboratories (dstl) provides scientific advice in connection with CBRN.

www.mod.uk

www.ctcentre.mod.uk

www.dstl.gov.uk

Ministry of Justice - HM Coroners

The Ministry of Justice oversees HM Coroners. The role of the coroner is defined by statute. In an emergency, the coroners will be responsible for establishing the identity of fatalities and the cause and circumstances of death: they will determine who has died, how and when and where the death came about. If an emergency spans more than one district, a lead coroner will be established to deal with all fatalities. OSCT has been working closely with HM Coroners in planning for contaminated fatalities.

www.justice.gov.uk

Office for Security and Counter Terrorism (OSCT)

OSCT was set up as part of the Home Office in March 2007. It supports the development, direction, implementation and governance of CONTEST the UK's strategy for countering international terrorism. The CBRNE Oversight Board, chaired by OSCT, ensures that CBRN related work under CONTEST is coordinated across Government Departments and agencies. A CBRN team in OSCT provides day-to-day direction, oversees progress and identifies CBRN capability gaps and requirements through the four main CONTEST workstreams.

<http://security.homeoffice.gov.uk>.

The CBRNE unit may be contacted at cbrnenquiries@homeoffice.gsi.gov.uk.

Secret Intelligence Service (SIS)

SIS collects intelligence overseas to promote and defend the national security and economic well-being of the UK. It supports Security Service work in the UK.

www.sis.gov.uk

Security Service

The Security Service leads on the investigation of terrorism in the UK.

www.mi5.gov.uk

End notes

1. National Security Strategy 2009:
www.cabinetoffice.gov.uk/reports/national_security.aspx
2. <http://news.bbc.co.uk/1/hi/world/americas/5092228.stm>
3. <http://news.bbc.co.uk/1/hi/uk/6123236.stm>
4. The Middle East Media Research Institute (MEMRI), Special Dispatch 1309, (2006) available at:
www.memri.org/bin/articles.cgi?Page=subjects&Area=iwmp&ID=SP130906
5. http://news.bbc.co.uk/1/hi/world/middle_east/6461757.stm
6. Source: www-ns.iaea.org/downloads/security/itdb-fact-sheet-2009.pdf
7. The National Risk Register:
www.cabinetoffice.gov.uk/reports/National_Risk_Register.aspx
8. Tolerability of Residual Hazards Section A: Chemical, July 2008
9. Tolerability of Residual Hazards Section B: Radiological, July 2008

Published by the Home Office, March 2010
© Crown Copyright

ISBN: 978-1-84987-201-0

HO_01490_G