HM Government

The United Kingdom's **Science and Technology** Strategy for Countering International Terrorism

August 2009

The United Kingdom's Science and Technology Strategy for Countering International Terrorism

August 2009

© Crown Copyright 2009

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: 978-1-84726-938-6

Contents

The United Kingdom's Science and Technology Strategy for Countering International Terrorism

Part 1 Strategic context

International terrorism – the threat to the UK

Strategic factors

Planning assumptions

CONTEST: aim and principles

CONTEST: science and technology

CONTEST: governance of science and technology

The impact of future technology on counter-terrorism

Part 2 The 2009 Science and Technology Strategy

Part 3 Delivering the strategy

Horizon scanning

Identifying and sharing requirements; delivering effective solutions

International collaboration

Part 4 Key challenges in counter-terrorism

Key challenges

Case studies
Conclusion
End notes

Executive summary

The UK and UK interests overseas face a serious threat from international terrorism. The UK Government's response to the threat is set out in CONTEST, a three-year counter-terrorist strategy.

CONTEST is based on planning assumptions about the future direction of the threat and a set of core principles, notably the protection of human rights. It has four main workstreams (*Pursue, Prevent, Protect* and *Prepare*).

Science and technology play a key part in counter-terrorism, including our ability to pursue terrorists, prevent radicalisation, protect essential services and infrastructure and prepare for a terrorist attack.

This document updates the 2007 Science and Innovation Strategy for Security and Counter-terrorism. Its aim is to: *'use innovation, science and technology to reduce the risk to the UK and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence.'*

The strategy has three principle objectives:

- **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 science and technology requirements.**
- **To enhance international collaboration on counter-terrorism related science and technology.**

The strategy explains what has been achieved under each of these objectives since 2007 and the priorities for the next three years.

The strategy also identifies some of the key counter-terrorist challenges that we need to address in the next few years and where science and technology are likely to be vital. The challenges include:

- Understanding the causes of radicalisation.
- Protecting the national infrastructure.
- Reducing the vulnerability of crowded places.
- Protecting against cyber terrorism.
- Improving analytical tools.
- Identifying, detecting and countering novel and improvised explosives.
- Understanding and countering Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) threats.

International terrorism – the threat to the UK

1.01 The 2009 National Security Strategy identified international terrorism as the most significant immediate security threat to the UK[1]. The revised CONTEST strategy, published in 2009[2], sets out the nature of the threat and the Government's response. While terrorism is not new, the current threat is different from those we have faced before in its scope, capability and ambition. Contemporary international terrorist organisations have an international cause, plan and conduct attacks in and from a range of countries and aim to inflict significant civilian casualties. Many seek to recruit people in this country. Some organisations aspire to use unconventional methods, including chemical, biological, radiological and nuclear weapons.

1.02 The main terrorist threat to the UK comes from four interrelated sources: Al Qa'ida; terrorist groups affiliated to Al Qa'ida; self starting groups and individuals who identify with the ideology promoted by Al Qa'ida; and terrorist groups with a broadly similar ideology, but which have their own identity and regional agenda. All of these organisations and networks try to claim a religious justification for their actions.

1.03 Since 2001, the UK police and Security Service have disrupted over a dozen attempted terrorist plots and nearly 200 people have been successfully prosecuted for terrorist related activity. On 7 July 2005 four British terrorists attacked the London transport system, murdering 52 people and injuring hundreds more. A second planned attack two weeks later was unsuccessful. Since 2005 Al Qa'ida has continued to attempt attacks in this country.

Strategic factors

1.04 The revised CONTEST strategy identifies four factors which have facilitated the growth of contemporary terrorist groups:

- **State fragility and failure and unresolved regional disputes and conflicts** (particularly Palestine, Afghanistan, Bosnia, Chechnya, Lebanon, Kashmir and Iraq).
- A **violent extremist ideology**, often associated with Al Qa'ida, which regards most governments in Muslim majority countries as 'un-Islamic' or apostate; considers the overthrow of these governments to be the religious duty of all Muslims; and calls for attacks on western countries (and their citizens) who are perceived to offer those governments political, financial or military support.
- **Some modern technologies**, which have been used by terrorist organisations, not only to plan and conduct attacks, but also to disseminate propaganda and recruit people to their cause.
- **Radicalisation**, the process by which people actually come to support violent extremism and, in some cases, to join terrorist groups.

Planning assumptions

1.05 CONTEST outlines the likely direction of the terrorist threat over the next three years:

- Under international pressure the Al Qa'ida organisation is likely to fragment and may not survive in its current form. Networks and groups associated with Al Qa'ida will have more autonomy. They will continue to operate in fragile and failing states.

- Terrorists will have access to new technology and, as a result, may become capable of conducting more lethal operations.
- The ideology associated with Al Qa'ida will outlive changes to its structure.
- The extent to which the international community can reach out to those who are vulnerable to radicalisation will significantly determine the shape and extent of the future threat.
- As the structure of Al Qa'ida changes, the terrorist threat in and to the UK may diversify towards smaller 'self starting' organisations. Continued law enforcement, security and intelligence work will be needed to contain the threat we face.
- The ideology which sustains terrorism will be subject to greater challenge by all communities in this country, making it harder for terrorists to operate here and to recruit people to their cause.

CONTEST: aim and principles

1.06 The aim of CONTEST is:

"to reduce the risk to the United Kingdom and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence."

1.07 CONTEST is based on a set of principles. These reflect our core values, the lessons we and others have drawn from our experiences of terrorism to date, and the broader security principles set out in the 2009 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 be based upon the rule of law.
- We will always aim to prosecute those responsible for terrorist attacks in this country.
- Our strategy will tackle the causes as well as symptoms of terrorism.
- Reducing support for terrorism and preventing people becoming terrorists are vital: without popular support terrorism is unsustainable.
- Our strategy must be responsive to the threat that can be created by rapidly evolving technology.
- We recognise that partnerships in this country and overseas are essential to our success and that these partnerships depend on openness and trust.
- The threat we face crosses our borders and is international in scope. We will depend upon our allies as they will depend on us.

1.08 CONTEST is based on four workstreams, each with a clear objective:

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

1.09 Work on *Pursue* and *Prevent* reduces the threat from terrorism while work on *Protect* and *Prepare* reduces the UK's vulnerability to attack. Together, they reduce the overall risk from international terrorism. The revised strategy also emphasises a number of priorities common to all the four main workstreams: one of these is science and technology.

CONTEST: science and technology

1.10 The 2009 National Security Strategy identifies technology as a key driver of threats to the UK[3]. It notes that the exploitation of advances in technology by both terrorists and organised crime groups will inevitably create challenges to our national security.

1.11 CONTEST argues that rapid technological change has had two key effects on terrorism. The communications revolution has made easier the spread of violent extremist ideology and propaganda and has facilitated fundraising, recruitment, training and operational planning. Technology has also provided terrorist groups with the means to plan operations more securely and to achieve more lethal effects. We know that some terrorists aspire to develop and use chemical, biological, radiological and even nuclear weapons and that they have tried to use the internet to locate the materials and expertise they need.

1.12 These trends are expected to continue. In the future, terrorists are very likely to have more scope to communicate with each other, sometimes with less chance of detection. Online communications will continue to enable extremist messages to reach vulnerable individuals faster than conventional media. Technology may provide improved surveillance and reconnaissance capability as well as more lethal weapons. Scientific training and expertise will itself have even greater significance for terrorist (and insurgent) organisations because technology will be able to compensate for the vulnerabilities they have.

1.13 While technology has provided powerful new tools, techniques and tactics in support of the terrorist agenda, it is also a key element in our response. Success in delivering relevant science, innovation and technology is vital to the delivery of CONTEST. Science and technology impacts every area of the strategy. Our continued ability to identify and convict people engaged in terrorism, prevent radicalisation, protect our infrastructure and prepare for an attack all depend on developments in the physical and social sciences.

1.14 Traditionally, scientific and technological support to counter-terrorism has been focused on the technical sciences. Improved communications and surveillance systems have helped the law enforcement, security and intelligence services in their work. Technology has provided systems to better protect our critical national infrastructure and crowded places and has improved detection equipment for explosive and CBRN threats. More recently, the social and behavioural sciences have provided important insights into the causes of radicalisation which have been essential to the development of the *Prevent* strategy. The Guide for Local Partners on Prevent, published in 2008, provided more detail on the growing body of knowledge informing our understanding of radicalisation[4]. Understanding the behaviours of both individuals and crowds has also formed part of our work to protect crowded places.

CONTEST: governance of science and technology

1.15 The Office for Security and Counter-Terrorism (OSCT) was established in the Home Office in March 2007. It supports the Home Secretary and other Ministers in the development, direction, implementation and governance of the UK's Counter-Terrorism Strategy (CONTEST). It also directly delivers those aspects of the counter-terrorism strategy which fall to the Home Office, manages counter-terrorism related crises through the Cabinet Office Briefing Rooms (COBR), facilitates the Home Secretary's statutory oversight of the Security Service and is responsible for the programme management and direction of the 2012 Olympic and Paralympic Security and Safety Strategy.

1.16 OSCT coordinates cross-Government Science and Technology work in support of counter-terrorism, in close conjunction with a range of Departments and agencies, and is responsible for this document. OSCT also chairs the CONTEST Science and Technology Board, which assesses progress on science and technology in the four main workstreams of CONTEST and across Departments, agencies and policing. In addition, the Government Chief Scientific Adviser sits on both the CONTEST board and the CONTEST Science and Technology board.

Part 1 The impact of future technology on counter-terrorism

In the preparation of CONTEST, OSCT worked closely with the Ministry of Defence Counter-Terrorism Science and Technology Centre (MOD CT Centre) to identify science and technology developments likely to impact on terrorism out to 2020. The full report is classified but the following are key highlights.

In very general terms the report identified three overarching issues likely to favour terrorist organisations in this period:

- The 'democratisation' of science and technology, which puts more information and capability in the hands of small groups and individuals.
- The proliferation of technology, which offers terrorists an increasing choice of weapons.
- The pace of change in many science and technology domains, which may exceed the speed with which any government can respond.

These three issues in turn reflect a number of more specific trends during this period:

- **Globalisation:** new communications technology is enabling international outsourcing of high-cost, secondary functions to suppliers, service industry and consultants, many of them located in other countries.
- **Acceleration and convergence:** the rate of change in 'Commercial Off the Shelf Technology' (COTS) and open source technology is increasing. Future technology trends will be marked not only by accelerating advances in individual technologies, but also by convergence of technologies, (eg information, biological, materials, and nanotechnologies) with the potential to revolutionise our lives.
- **Knowledge transfer:** the growing exchange of high-tech knowledge between the developing world and the West, the increasing size of the computer-literate workforce in developing countries, and efforts by global corporations to diversify their operations, will foster the spread of new technologies.
- **Knowledge loss:** the trend towards employing technology rather than human expertise may come at the expense of developing human analysis and judgement.
- **Independence and agility:** in technological development, small groups can often outperform larger counterparts. State organisations can be constrained by their decision-making processes and by security and commercial factors. Moreover, the last few years have seen the creation, adoption and exploitation of new technologies by an 'audience of amateurs' who now far outnumber those in traditional research and development roles.

The report identifies seven broad science and technology domains where future developments may have a significant impact on terrorist activities and our counter-terrorism work. These domains and some of the potential developments are set out below. The list should not be regarded as comprehensive.

Information and Communication Technology (ICT)

- Instantaneous worldwide mobile communications will become available to most people, increasing global information flows.
- There will be an exponential growth in the volume of data stored on networked computer systems; small

and inexpensive devices will store massive amounts of data as voice, video and text.

- There is likely to be an increasing trend away from producers pushing information out to the public and towards consumers pulling in only what they want, when they want it.

Biotechnology

- The costs of bioengineering will continue to fall.
- More genetic data and information about the human genome will be publicly available.
- Laboratory equipment will automate or facilitate specific bioengineering procedures, providing capability to groups which otherwise lack the necessary expertise.

Military Science

- Weapons with greater precision and higher lethality are likely to be more widely available.
- Technical change will facilitate aspects of chemical and biological weaponry.
- The ability to make explosives from commonly available ingredients will become more widespread.

Nanotechnology (the understanding and control of matter at dimensions between approximately 1 and 100 nanometers)[5]

- Nanotechnology will enable the accelerated development of novel materials and may be used to facilitate the development of possible future explosives and fissile material.
- Nanotechnology will allow the exploitation of alternative properties of materials as well as miniaturisation of existing capabilities, which will lead to enhancements in areas such as protection, communication and detection.

Robotics

- Robots that effectively mimic human appearance and movements may be used as human proxies.
- Robots may increase the performance and safety of individuals and small teams by increasingly carrying out repetitive or dangerous tasks.

Engineering and Manufacturing

- Non-traditional methods of manufacturing, such as rapid prototyping and 3D printing, will continue to develop, making available the production of sophisticated components to the non-specialist.
- A range of commercially available technologies will continue to greatly enhance human performance (speed, strength and mental agility etc.) on land and in the water.

Materials Science

- Fabrics will incorporate power sources, electronics and optical fibres; advances will significantly improve camouflage and protection and allow clothing to monitor an individual's health.
- Composite materials will possess greatly enhanced strength, toughness, wear and corrosion resistance.

METROPOLITAN
POLICE

2.01 In 2007 the Government published its first Science and Innovation Strategy for Security and Counter-Terrorism[6]. This sought to 'optimise the benefits of science and innovation to reduce the risk from terrorism so that people can go about their business freely and with confidence'. The strategy identified four key ways of meeting this aim: horizon scanning; expanded cross-Departmental operational analysis leading to clear research priorities; effective working with business and academia; and international collaboration.

2.02 This 2009 strategy builds on the earlier document. Its aim is to: *'use innovation, science and technology to reduce the risk to the UK and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence.'* It has three principal objectives:

- **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 science and technology requirements.**
- **To enhance international collaboration on counter-terrorism related science and technology.**

2.03 This strategy:

- Reflects our recognition that modern technologies, which facilitate terrorist propaganda, communications and operations, are an important long-term strategic driver of the terrorist threat.
- Places greater emphasis on identifying science and technology requirements from across Government, the police service and wider law enforcement to ensure that the right solutions are developed to counter the challenges we face.
- Seeks greater partnership and engagement with industry and academia and commits us to more openness and transparency on science, technology and counter-terrorism.

2.04 This strategy also reflects the Home Office Science and Innovation Strategy 2009–12[7]. As in that document, the definition of science used here includes physical sciences and engineering, social sciences, statistics, economics and operational research.

2.05 The remainder of this document outlines the achievements in these areas since 2007 and the next steps that we intend to take. It also details the key challenges that we believe can be addressed using science and technology.

UK/EU Passports
Including Switzerland and the European Economic Area
UK Border

3.01 This section sets out the strategy's three main areas of work, outlining achievements so far and future action.

Horizon scanning

3.02 Our objective: to use horizon scanning to understand future scientific and technical threats and opportunities and inform our decision making on counter-terrorism.

Key achievements since 2007

3.03 Horizon scanning is vital to our counter-terrorist work. We need to understand which existing terrorist groups might pose a threat to us in future and from where new groups might emerge. We also want to anticipate the technologies they may use. We need to be aware of the technologies which may be available to us and plan accordingly. New research and innovative technologies often take time to develop, so we need to identify potential threats and opportunities as early as possible. The paper on pages 10 and 11 above, is an example of collaborative horizon scanning between OSCT and MOD.

3.04 Since its formation in 2003 the Joint Terrorist Analysis Centre (JTAC), the UK centre for the analysis and assessment of the threat from terrorism, has grown by 60%. Part of the role of JTAC is to assess the current and future technological capabilities of terrorist organisations and this work has played an important part in shaping our overall counter-terrorism strategy. JTAC works closely with the Cabinet Office Assessments Staff who produce papers for consideration and approval by the Joint Intelligence Committee (JIC). The JIC also considers future scientific and technical issues likely to impact on our wider national security. In 2008 the Cabinet Office set up the Strategic Horizons Unit to coordinate Government security-related horizon scanning work, including in science and technology. This unit works alongside the National Security Forum[8], established in 2009 to provide expertise from people outside of Government on a range of issues relating to the National Security Strategy.

3.05 The Government Office for Science (GO-Science) is responsible for ensuring that Government policy and decision-making is supported by robust scientific evidence and long-term thinking[9]. The GO-Science Foresight Horizon Scanning Centre (HSC)[10] has created the Future Security and Intelligence Outlook Network (FUSION) which brings together strategic futures analysts within the Government security and intelligence community. FUSION promotes collaboration on issues that cut across Departmental interests, and encourages the use of futures techniques within Departments and Agencies. FUSION complements the HSC's Futures Analysts' Network (FAN) Club, which is open to all inside and outside Government from the UK and overseas. Both networks enable the exchange of new ideas, innovative thinking and good practice.

3.06 The HSC's Sigma Scan[11], first published in 2006, has been expanded and updated in the past three years. It comprises a set of almost 300 papers, including over 100 involving science and technology. They explore potential future trends across the entire public policy spectrum and are drawn from more than 2000 sources and interviews with 300 leading thinkers. The Scan looks up to 50 years forward and provides a tool to help Government identify future risks and opportunities.

Next steps

3.07 OSCT will carry out horizon scanning projects based on the conclusions of the OSCT/MOD scan to 2020, to identify triggers and trends for critical areas. We will use the conclusions of these scans to adapt or develop science and technology policy and make them available across the counter-terrorism community.

3.08 OSCT will also carry out a new long-term scan within the three-year period to take account of important scientific and technological changes. The results of this scan will inform the future development of the counter-terrorism science and technology strategy.

3.09 OSCT will engage with cross-Government horizon scanning efforts on science and technology, ensuring our own work is widely distributed and used and that we are making use of relevant work elsewhere, notably in the Strategic Horizons Unit and the Joint Intelligence Committee (JIC).

Identifying and sharing requirements; delivering effective solutions

3.10 Our objective: to ensure the development and delivery of effective counter-terrorism solutions by identifying and sharing priority science and technology requirements.

3.11 Understanding and prioritising the science and technology requirements of the UK counter-terrorism community and sharing these requirements with industry and academia are at the heart of this strategy. Both industry and academia have a significant role to play in countering terrorism in the UK. The UK is a leading innovator in the design and provision of defence and security solutions and we want this expertise applied to science and technology in the counter-terrorism domain. Government is already working with industry primes, small and medium sized enterprises (SMEs) and academia to ensure that providers know what is needed and understand the route to market.

3.12 The market for counter-terrorism science and technology is more fragmented than many others, especially in comparison to the Defence market. This reflects the range of Departments, Agencies, Police forces and local delivery partners involved in this work, as well as the broad range of requirements stemming from the CONTEST strategy. Aligning these interests and developing coordinated engagement is a high priority.

3.13 Getting this right in the domestic counter-terrorism market will also help to stimulate an international market in security products for UK industry and academia. We are committed to allowing as strong a market as possible to develop in these areas, within appropriate export controls.

3.14 Testing, validation and verification of potential technological solutions is the responsibility of the Home Office Scientific Development Branch (HOSDB)[12], the Centre for the Protection of National Infrastructure (CPNI)[13], the Ministry of Defence Counter-Terrorism Science and Technology Centre (MOD CT Centre)[14] and the Transport Research Laboratories[15]. The Home Office Scientific Development Branch (HOSDB) Exhibition is an annual showcase for the latest security and counter-terrorism equipment.

Key achievements since 2007

3.15 The establishment of OSCT in 2007 has led to closer collaboration on requirements setting across Departments engaged in CONTEST. Policy leads, end-users (including the police, security and intelligence services) and scientific experts have worked together to identify cross-Government research and technological priorities under each of the CONTEST work streams, embracing both technical and social science. The Government's Chief Scientific Adviser has set up a panel of Departmental Chief Scientific Advisers to review counter-terrorism issues.

3.16 Research into methods of dealing with non-conventional chemical, biological, radiological and nuclear attacks by terrorists has been a major priority in the past five years. In 2004 the Government established a cross-department science and technology programme to strengthen the UK's ability to respond to a CBRN attack. The programme now has a budget of more than £10 million a year and has expanded to include more than 50 projects, supporting all four key CONTEST workstreams. A cross-Government board sets the programme's research priorities and the research is quality assured by an independent, external scientific advisory board. The programme has delivered new guidance and equipment, modelling tools, risk reduction, medical countermeasures and has quality assured commercial off-the-shelf products.

3.17 In 2007 the Government began to develop a revised *Prevent* strategy for stopping people becoming or supporting terrorism. The strategy was based on an improved understanding of the causes or radicalisation in this country and overseas, which in turn reflected the increase in credible research and analysis in this area. Some of this research was conducted within Government Departments, but some was commissioned externally. For example, the Association of Chief Police Officers Terrorism and Allied Matters business area (ACPO/TAM)[16] commissioned the report 'Hearts and minds and eyes and ears: Reducing radicalisation risks through reassurance-oriented policing' through their Research & Innovation Unit (RIU). The RIU feeds front-line user requirements into ACPO/TAM and facilitates research collaboration between the Police Service, Home Office and Security Service through an Interagency Co-ordinating Group.

3.18 A cross-Government Social Science Academic Advisory Board now coordinates and supports social science work under the *Prevent* workstream. The Foreign and Commonwealth Office (FCO) is responsible for a significant *Prevent* research programme on a range of overseas topics run by the Economic and Social Research Council[17].

3.19 Although not formally part of CONTEST, counter-insurgency is closely linked to our work to reduce the threat to the UK and its interests from international terrorism. Counter-insurgency requirements and solutions are often applicable in counter-terrorism. For example, the Ministry of Defence counter-terrorism science and technology programme has delivered enhanced capability to front-line troops conducting counter-insurgency operations in Afghanistan and Iraq. A new explosives detection capability has been deployed in these areas, providing a step change in capability for the detection of a range of explosive and chemical threats. MOD is also working closely with UK industry on the detection of improvised explosive devices. Small-scale trials conducted in 2009 have identified promising technologies and systems, which will be rapidly developed into full trials.

3.20 In March 2007, the Security and Resilience Industry Suppliers' Community (RISC)[18] was formed to provide a focal point for Government to liaise with industry on counter-terrorism requirements. Through RISC, five joint Industry Advisory Groups have been established in areas of particular importance to this strategy:

- Chemical, Biological, Radiological and Nuclear (CBRN)
- The Critical National Infrastructure (CNI)
- Information and Communications Technology (ICT)
- Detecting suicide bombers
- Olympics

3.21 The purpose of these five groups is to exploit Government-funded research, develop Government requirements, focus private sector investment and enable access to innovation.

3.22 RISC completed two reviews on behalf of Government during 2008. The first gave an outline of the UK's 'world class' security capabilities and identified areas where new security capabilities are being developed by industry. The second review informed Government about the current challenges, opportunities and realities of dealing with Departments and agencies on counter-terrorism from an industry perspective. Their recommendations are being implemented in cooperation with RISC.

3.23 OSCT has also investigated the use of venture capital-style techniques to encourage innovation in the counter-terrorism arena. This included using regional searches, competitions and investor networks to access innovative ideas to protect crowded places and developments in Information and Communication Technology (ICT). The findings were used to inform the approach used in the new innovation programme, INSTINCT[19].

RISC

The UK Security and Resilience Industry Suppliers' Community (RISC) provides a focal point for the Government to communicate with industry about its counter-terrorism needs. RISC is an alliance of suppliers, trade associations and academics, and includes over 2,000 companies ranging from prime contractors and global leaders through to small and medium enterprises and start-ups.

The trade associations are: the Society of British Aerospace Companies (SBAC)[20], the Defence Manufacturers' Association (DMA, including the Association of Police and Public Security Suppliers – APPSS[21]), the British Security Industry Association (BSIA)[22], and Intellect (the UK trade association for the technology industry)[23].

The IDEAS factory

The Engineering and Physical Sciences Research Council (EPSRC)[24] has devised a unique way of bringing together organisations with technical challenges and academics with relevant skills to enable the development of research solutions.

EPSRC invites academics to 'IDEAS factory' events via the Research Council websites with the incentive that funding is allocated to research proposals that come out of the process. About 25 people work together on a challenge, for about a week. The Centre for the Protection of the National Infrastructure (CPNI) has run two of these events, including work on public behaviour in public spaces. This has facilitated contacts with a wide range of academics and, subsequently, six new counter-terrorism research projects.

INSTINCT (Innovative Science and Technology in Counter-Terrorism)

INSTINCT is a cross-Government programme led by OSCT that seeks innovative solutions to support our counter-terrorism strategy. Its aim is to enable Government to make the most of innovative projects and ideas in counter-terrorism by providing a greater understanding of the innovation community, smarter influence over external innovation and better coordination of investments in new ideas and solutions. Organisations involved in INSTINCT include OSCT, the Home Office Scientific Development Branch (HOSDB), the Ministry of Defence, the Centre for the Protection of National Infrastructure (CPNI) and the Association for Chief Police Officers (ACPO).

The INSTINCT programme will include calls for proposals on a variety of topics relevant to counter-terrorism. The first of these was an industry day that focused on 'Intent in Crowded Places' held in collaboration with the Ministry of Defence's Centre for Defence Enterprise (CDE)[25]. The CDE is the first point of contact for anyone with a disruptive technology, new process or innovation that has a potential defence application. This event was the first time the CDE had been used to address a (non-MOD) counter-terrorism challenge.

Next steps

3.24 OSCT will use a scenario-based approach to identify where and how science and technology can improve the UK's counter-terrorism capability. Experts, policy makers and front-line staff will participate in the process. Subject experts will be included in a counter-terrorism science and technology advisory group which will report to the National Security Forum. Front-line expertise will be drawn from the police, security and intelligence services. OSCT will also use organisational learning, operational reviews and the results of inspection activity to inform conclusions.

3.25 Science commissioned by Government through the CONTEST Science & Technology Programme will be subject to independent academic review. The counter-terrorism science and technology advisory group (see 3.24) will propose a panel of security-cleared academics for this purpose.

3.26 OSCT will produce a series of brochures for industry and academia outlining counter-terrorism related science and technology requirements and possible exploitation routes. The first of these brochures, published alongside this strategy, outlines four challenges where new developments could significantly enhance counter-terrorism work. These are summarised in Part 4 of this document. The brochure also explains in more detail how industry and academia can get involved in this counter-terrorism work[26]. Later brochures in this series will deal with a variety of priority and emerging topics, including social sciences in counter-terrorism.

3.27 Government will undertake a programme of engagement beyond the security and intelligence sphere to include industries not normally associated with counter-terrorism.

3.28 Government will continue to work with Research Councils UK (RCUK)[27] to improve the Government's engagement with academia, Research Councils and public sector research establishments in counter-terrorism. It will also continue to encourage innovation through the Technology Strategy Board[28].

3.29 Government will use the INSTINCT programme to enable greater understanding of the innovation community, smarter influence over external innovation and better coordination of investments in innovative ideas and solutions.

3.30 OSCT will work with Government Departments and agencies to improve the efficiency of the market place and coordinate our counter-terrorist requirements. Given the range of interests involved (over 50 police forces across the UK, more than 30 Government departments and agencies and the Devolved Administrations) it is neither feasible nor desirable to create a single market. However, the Home Office will be working with key sectors and in particular, with the National Police Improvement Agency (NPIA)[29] and the Association of Chief Police Officers (ACPO) to establish a more coordinated approach to the purchase of counter-terrorism equipment by police forces.

The Interception Modernisation Programme

Governed by strict rules, data about communications services is routinely used to investigate terrorist plots, convict those guilty of serious crimes, seize illegal drugs and protect the vulnerable in our society. However, the highly competitive and innovative communications environment in the UK has led to rapid changes in how communications technologies are provided and used. New ways of communicating are becoming available, for example using VOIP (Voice Over Internet Protocol) and other internet-based services. These changes have implications for how communications data is collected and the extent to which public authorities are able to lawfully obtain it.

The cross-Government Interception Modernisation Programme (IMP) is concerned with maintaining our capability to use communications data in the face of the challenges posed by new communications technologies. The programme has been researching the challenges caused by advances in technology and the impact of any potential capability gaps. IMP is one of the most important and urgent examples of Government *identifying* a requirement and *sharing* that requirement with industry and many others. A recent public consultation proposed possible solutions on how we continue to collect, access and safeguard this important data to protect the public in the future[30].

International collaboration

3.31 Our objective: to enhance international collaboration on counter-terrorism related science and technology.

3.32 International collaboration is the cornerstone of all our counter-terrorist work. Terrorist incidents here usually have an international connection; international terrorist networks threaten the UK's interests overseas and people from this country have participated in attacks and insurgencies in other countries. An international response is vital to the success of CONTEST. Agencies in the UK collaborate closely with their counterparts overseas. We work with other countries and with multilateral organisations to develop policy responses to the threats we each face. We also need to coordinate closely with like-minded overseas partners in developing and sharing science and technology relevant to our counter-terrorism work.

Key achievements since 2007

3.33 In the past two years we have continued to strengthen our relationships with international partners. In Europe, our main engagement on science and technology for counter-terrorism has been through the European Union and the European Commission's Framework Programme 7 (FP7)[31]. One of the ten FP7 themes is Security, which includes counter-terrorism. Under FP7, the European Commission awards research funding to investigate a range of security questions. FP7 encourages collaboration between industry, including small and medium-sized enterprises (SMEs), academia, public sector research establishments, and international partners. The UK is actively engaged in the process to set the FP7 Security programme of research requirements. The FP7 Security programme budget for 2009 was €117 million, rising to over €200 million in 2010. UK projects currently funded by FP7 are ongoing and will deliver in the next few years. They include work on physical security, crisis management simulation and training, and supply chain security.

3.34 The UK Government is also represented on the European Security Research and Innovation Forum (ESRIF)[32], which will shortly present its report to the European Commission on counter-terrorism, mid- to long-term requirements for security research and innovation (up to 20 years ahead).

3.35 The UK has played a role in shaping the EU CBRN Action Plan[33] through expert-level participation in the preceding scoping exercise (the CBRN Task Force) and by close engagement with the EU Commission. The recently published Plan aims to support the ongoing efforts of the Member States and provides a framework for better cooperation. This is one of the Commission's priorities on counter-terrorism for the coming years and is a substantial dossier for the current Swedish Presidency. Work on the Action Plan is being coordinated within the EU Commission by the Directorate-General for Justice, Freedom and Security (DG JLS) and is built around three strategic themes:

- **Prevention** – reducing unauthorised access to CBRN materials.
- **Detection** – improving the capability to detect CBRN materials.
- **Preparedness and Response** – improving the speed and effectiveness of our response to and recovery from CBRN events.

3.36 The Plan is undergoing a further round of consultation within EU Member States and discussion at the Civil Protection Working Group before final adoption by the EU Council in December 2009. It should facilitate access to EU research funding by clarifying priorities and linking into other programmes. For example, there are plans for DG JLS to allocate up to €100 million from existing financial programmes to support implementation of the plan over the period 2010–2013. Other Commission funding programmes such as FP7 will also contribute. If successfully implemented, the Plan should coordinate activity on CBRN across a number of EU areas (health, environment etc), assist with identifying overlaps and reduce the potential for duplication of effort.

3.37 OSCT is developing a working relationship with the CBRNE Centre based at the University of Umeå in Sweden[34], established in 2008 to be a European centre of excellence in CBRNE research and training. Amongst its current work, the Centre is leading a consortium of academia, industry and end-users to bid for a major EU project under FP7 to determine baseline CBRNE requirements for Europe: the UK is involved as a potential end-user via the Police National CBRN Centre which coordinates police work in this area.

3.38 The UK has collaborated closely with EU partners to take forward the work of the Enhancing the Security of Explosives action plan[35] (published in November 2007) which recommended steps to control precursor chemicals and improve the storage, transport and audit of explosives and explosive detection capabilities.

3.39 The Government has a very wide ranging scientific and technical dialogue on counter-terrorism related issues with the US, notably the Department for Homeland Security (DHS)[36] and the Department of Defense. Joint work is taking place in particularly complex areas, including detection and identification of CBRNE material, and the longer-term recovery from CBRN attack. The UK has benefited from the US's experience in the clean-up and management of contamination resulting from the anthrax letters in 2001. Information-sharing and collaboration between the Home Office and the Department of Homeland Security has led to the Biological Autonomous Networked Detector Project (BAND) to jointly trial a prototype biological detection system. The results will inform future improvements in the UK's resilience to terrorist attacks with biological weapons.

3.40 The Ministry of Defence collaborates closely with the US Department of Defense and other US Government departments. Through a Memorandum of Understanding (MoU) the UK and US have shared standards and protocols relating to imaging, intruder detection systems and software. This has enhanced interoperability and spread good practice in both countries.

3.41 The MOD Counter-Terriorism Science and Technology Centre is collaborating with the Australian Counter-Terrorism and Security Technology Centre, which acts as a focal point for counter-terrorism and security science and technology advice, support and solutions across Australia's agencies.

3.42 Led by CPNI, the UK has also signed a new Memorandum of Understanding with Canada covering the use of Science and Technology in Public Security and Safety. This agreement will allow us to share existing knowledge and experience, develop new joint programmes of work, and share personnel. The MoU covers a range of themes including information management and security, assessment of risk, informing policy with science and technology, and CBRNE.

3.43 The UK is also heavily involved in international social science research relating to the *Prevent* stream of CONTEST, sharing and receiving data in a range of bilateral and multilateral fora. UK Government social and behavioural scientists are in close contact with their counterparts in the Human Factors Division of the Department of Homeland Security and are linked into the DHS-sponsored Studies in Terrorism and Responses to Terrorism (START) research programme at the University of Maryland[37]. Collaboration has included joint academic workshops on radicalisation, sponsoring research on radicalisation in prisons and joint seminars on the internet. In Europe, UK social scientists are actively exchanging research ideas through the European Network of Experts in Radicalisation run by the European Commission through the Change Institute in London[38]. UK scientists are also involved in the radicalisation working group of the European Security Research and Innovation Forum, and in expert practitioners groups set up by the EU CT Coordinator.

Next steps

3.44 We will work with our international partners to identify areas of best practice and expertise. Our work with the US and the EU will continue to be the most significant but we will look to address our requirements wherever we believe a shared approach to counter-terrorism science and technology would be productive. We will build on the FP7 and ESRIF work by identifying and engaging with other multilateral organisations to facilitate international opportunities for UK industry and academia. Collaboration on social science will remain a high priority. This work will be covered in more detail in a future brochure.

The United Kingdom's Science and Technology Strategy for Countering International Terrorism

4.01 The latest version of the Government's counter-terrorism strategy, CONTEST, explicitly identifies a number of 'future challenges' that we shall face in implementing the strategy successfully over the next three years[39]. The challenges are set out in relation to each of the four main workstreams (ie *Pursue, Prevent, Protect* and *Prepare*) and in connection with our management of the threat from terrorist use of chemical, biological, radiological and nuclear weapons and explosives. Addressing these challenges will require significant scientific and technological inputs.

4.02 This section sets out seven challenges. Some of these, along with some of the related science and technology areas* are explained in more detail in the first of a series of brochures[26] which is published alongside this document**.

Understanding the causes of radicalisation

4.03 Radicalisation (the process by which people come to support violent extremism and terrorism and, in some cases, then to participate in terrorist groups) is one of the four drivers of the terrorist threat we face today. We need to continue to improve our understanding of the causes of radicalisation in this country and overseas. Whilst there is a growing body of research relating to the process of radicalisation to violent extremism, more must be done to improve the evidence base and develop robust models. In particular, we need to improve our understanding of the relative importance of political, ideological, social and psychological factors, and how and when these operate in individuals or groups. This will better enable us to develop the most effective counter-radicalisation policies and measure the impact of existing and future Government programmes.

Protecting the national infrastructure

4.04 The national infrastructure delivers essential services to the public (such as power, water, transport, finance and healthcare). Damage to this infrastructure can have severe economic impact or cause large-scale loss of life. Intelligence shows that terrorists are interested in attacking national infrastructure targets and recognise the potential impact such attacks can have. The Government will wish to maintain appropriate measures for detection and protection.

Reducing the vulnerability of crowded places

4.05 Crowded places are attractive terrorist targets. Their protection presents significant challenges as threats can be difficult to detect and deter, particularly without impeding the ability of the public to go about their normal day to day business.

Protecting against cyber terrorism

4.06 The UK is increasingly reliant on networked communication, but the very open nature of our digital infrastructure makes it vulnerable to attack. In response to this the Government has recently published the first Cyber Security Strategy for the United Kingdom[40], which sets out the UK's strategic cyber security objectives and incorporates a cyber security industrial strategy. In the next three years we continue to expect terrorist groups to favour high-profile 'conventional' or 'unconventional' operations over cyber attacks, but we

* These areas are: knowledge management, biometrics, screening, physical protection and countering improvised explosive devices.

** The challenges included in the brochure are: protecting the national infrastructure; reducing the vulnerability of crowded places; protecting against cyber terrorism; and improving analytical tools

must be vigilant against any increase in capability or change in intent. We will continue to require ways to protect ourselves from an attack and ways of recovering quickly should such an attack occur.

Improving analytical tools

4.07 Terrorists operate in secret. Detecting their activities requires the ability to exploit new data analysis and information sharing methods, sophisticated technical collection and exploitation systems, and the very latest means of information sharing and management.

4.08 One of the major challenges is to develop new methods of identifying patterns or trends from large quantities of raw data that could alert us to suspicious activity.

4.09 Because surveillance, interception and the collection of data have the potential to intrude on privacy, it is vital that there are strict rules governing the use of these techniques and strong independent oversight of how these rules are applied.

Identifying, detecting and countering novel and improvised explosives

4.10 Many contemporary terrorist groups have demonstrated an intent to experiment with novel explosives to maximise the lethal capability and, in some cases, deliberately evade protective security measures. We need to constantly update and improve understanding of and ability to detect explosive compounds of all kinds, while reducing disruption and inconvenience to the travelling public. We also need methods to render improvised explosive devices safe should they be detected.

Understanding and countering Chemical, Biological, Radiological, Nuclear and Explosive threats (CBRNE)

4.11 The CBRNE threat (chemical, biological, radiological and nuclear weapons and explosives) from terrorists is complex and poses significant challenges. In addition to a deeper understanding of how the threat is evolving and how we can disrupt it, we require measures to protect ourselves and respond effectively in the event of a CBRNE attack. This includes improved detection, identification and counter-measures. Looking to the future, Al Qa'ida and other terrorist organisations may be developing new technologies to use in an attack and we must keep ahead of this evolving threat.

Case studies

Aesthetic barriers deployed in central London

Barriers: effective physical protection with minimal architectural impact

Barriers already have a well-established role in protecting important targets from vehicle born explosives. The Centre for the Protection of National Infrastructure (CPNI) is the Government authority in this area, providing security advice to the businesses and organisations responsible for essential services. CPNI has worked closely with industry to develop barriers that are highly resistant to impact.

Barriers are also being developed which provide protection with minimum architectural impact and require minimal excavation during installation. One example is the CPNI-tested protective balustrades and walls in Whitehall, which were designed by the City Council to reflect the listed buildings in the area.

Improving transport security

Security systems such as passenger screening at airports are complex, typically involving multiple channels, different detectors and numerous processes, which work together in complex ways. The Department for Transport (DfT)[41] has created innovative computer software that allows the modelling and testing of these complex security systems to make transport safer.

One of the challenges DfT faces is to understand how changing any aspect of a security system will affect its performance, particularly when changes may affect queues and waiting times. With help from the Defence Science and Technology Laboratory (Dstl)[42], DfT has used operational analysis – a branch of mathematics – to develop software that can simulate changes to a system's design and measure the effect on performance. The effects of these changes can now be predicted before putting them into practice in the real world.

The model has been used to provide advice to Eurostar on the design of passenger screening systems at St Pancras International and to analyse the impact on passenger flow of relaxing the hand luggage restrictions at UK airports.

Case studies

Home Office Scientific Development Branch testing equipment for stopping rogue vessels

Stopping rogue vessels: developing an effective defence against maritime attacks

For some time, police have been able to stop suspect or fugitive vehicles on the road. The Home Office Scientific Development Branch (HOSDB) has collaborated with industry to develop a new defensive system designed to stop terrorists or criminals in small boats without resorting to lethal force. The system works by disabling the propulsion system of a small vessel.

HOSDB has built on its good industrial relationships with the companies working in this area to develop a practical solution that meets the Government's needs. It trialled systems and fed back results to industry for further development. In parallel, the Smith Institute[43] reviewed HOSDB's experiments to ensure the development of good-quality science, as well as enhanced operational capability for the police.

Detecting the illicit movement of radioactive materials

Some terrorist organisations aspire to use unconventional weapons, including nuclear or radiological materials. Innovative systems designed to detect the radiation from such materials are being installed across the UK. Programme Cyclamen[44] is introducing fixed portals and mobile detection units to entry points to detect the illicit movement of nuclear or radioactive materials into the UK.

The system screens freight and people in vehicles or on foot as they pass through the fixed portals or the Mobile Radiation Detection Units (MRDUs). These monitors have the advantage of detecting radiation emitted by radioactive materials in a passive manner. Unlike X-ray machines, they do not emit any rays, but detect radiation only by receiving it. As a result, the system is not harmful to either the load being screened, or people in the immediate area.

We have already successfully piloted fixed radiation portals, which are now being installed across the UK, and the fleet of MRDUs is fully operational.

Conclusion

International terrorism is a threat to the security of the UK and to our interests overseas. The use of technology by terrorist groups is a feature of the threat we face.

CONTEST sets out the programmes which Government has developed to address this threat and some of the challenges which remain. Science and technology have an important part to play in responding to these challenges now and in the future.

The Government is committed to sharing counter-terrorist science and technology requirements and engaging with industry and academia. This strategy and subsequent publications will indicate how we intend to do that in the future, building on the very significant progress that has been made in the past three years.

End notes

1. www.cabinetoffice.gov.uk/reports/national_security.aspx
2. security.homeoffice.gov.uk/counter-terrorism-strategy
3. Page 40, www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf
4. The Prevent Strategy: A Guide for Local Partners in England; security.homeofffice.gov.uk/news-publications/publication-search/prevent-strategy
5. www.nano.gov/html/facts/whatIsNano.html
6. security.homeoffice.gov.uk/news-publications/publication-search/general/science-innovation-strategy1?view=Binary
7. www.homeoffice.gov.uk/documents/science-strategy
8. www.number10.gov.uk/Page18541
9. www.dius.gov.uk/partner_organisations/office_for_science
10. www.foresight.gov.uk/Horizon%20Scanning%20Centre
11. www.sigmascan.org
12. scienceandresearch.homeoffice.gov.uk/hosdb
13. www.cpni.gov.uk
14. www.ctcentre.mod.uk
15. www.trl.co.uk
16. www.acpo.police.uk
17. www.esrc.ac.uk
18. www.riscuk.org
19. security.homeoffice.gov.uk/science-innovation/instinct
20. www.sbac.co.uk
21. www.appss.org.uk
22. www.bsia.co.uk
23. www.intellectuk.org
24. www.epsrc.ac.uk/default.htm
25. www.science.mod.uk/engagement/enterprise.aspx
26. Countering the terrorist threat: Ideas and Innovation. How industry and academia can play their part. HM Government, August 2009, ISBN 978-1-84726-940-9
27. www.rcuk.ac.uk
28. www.innovateuk.org
29. www.npia.police.uk
30. www.homeoffice.gov.uk/documents/cons-2009-communications-data
31. cordis.europa.eu/fp7
32. www.esrif.eu
33. register.consilium.europa.eu/pdf/en/09/st11/st11480.en09.pdf
34. www.cbrnecenter.eu/
35. www.eubusiness.com/Living_in_EU/explosives-guide/
36. www.dhs.gov
37. www.start.umd.edu/start/
38. www.changeinstitute.co.uk/index.php?option=com_content&task=view&id=83
39. Pages 78, 99, 116/7, 124/5, 131, security.homeoffice.gov.uk/counter-terrorism-strategy
40. www.cabinetoffice.gov.uk/reports/cyber_security.aspx
41. www.dft.gov.uk
42. www.dstl.gov.uk
43. www.smithinst.ac.uk
44. security.homeoffice.gov.uk/science-innovation/radiation-screening1

Published by the Home Office, August 2009
ISBN: 978-1-84726-938-6
© Crown copyright