HM Government

Countering the
terrorist threat

Ideas and
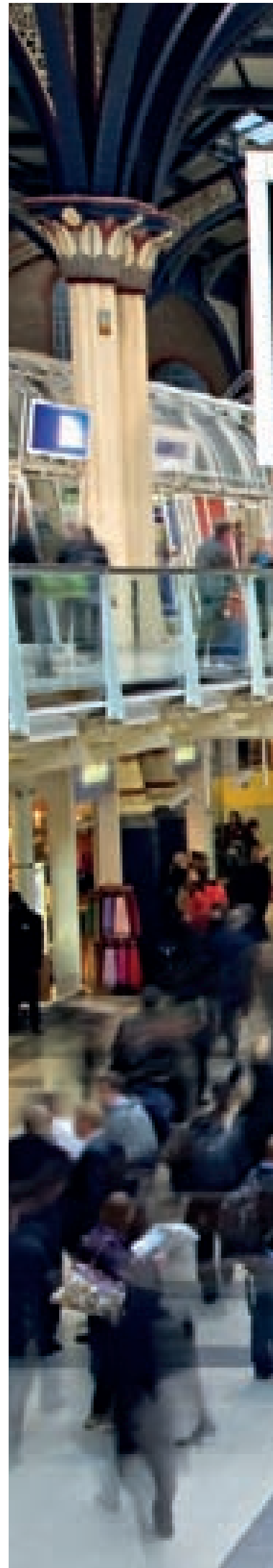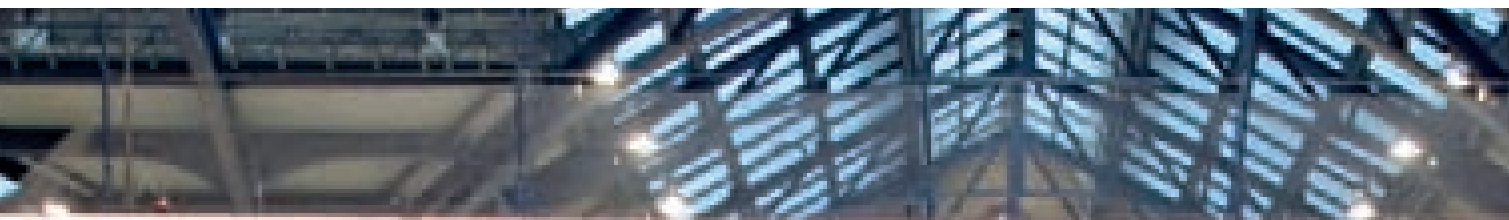# innovation

How industry
and academia
can play their part

Contents

This booklet is for everyone in industry and academia whose innovative ideas and technology could help counter the terrorist threat to the UK.

Modern technology has provided terrorists with powerful new tools and techniques.
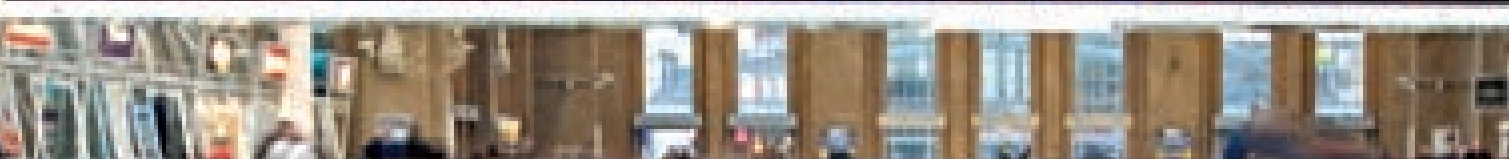
Science and technology are a key part of our response.

17:18

Key challenges

The UK Science and Technology Strategy for Countering International Terrorism sets out key challenges that we need to solve in the next few years.

There is already a great deal of work underway in Government, industry and academia to find effective solutions. But we need new ideas and fresh thinking to drive forward our counter-terrorist work.

We want industry and academia to draw on and develop:

– existing technologies now being used to support security or resilience
– existing technologies now being applied in a different way altogether
– future innovations and technologies yet to be developed.

This section highlights four of the key challenges that require innovative solutions from industry, academia and the Government working together*. We are keen to explore innovations and new ways of combining technologies to create effective solutions.

* The three key challenges outlined in the Counter-Terrorism Science and Technology Strategy that are not discussed further in this booklet are:

– understanding the causes of radicalisation
– identifying, detecting and countering novel and improvised explosives
– improving our ability to understand and counter chemical, biological, radiological, nuclear and explosive (CBRNE) threats.

These are explored in the UK's Science and Technology Strategy to Counter International Terrorism, ISBN 978-1-84726-938-6, published August 2009.
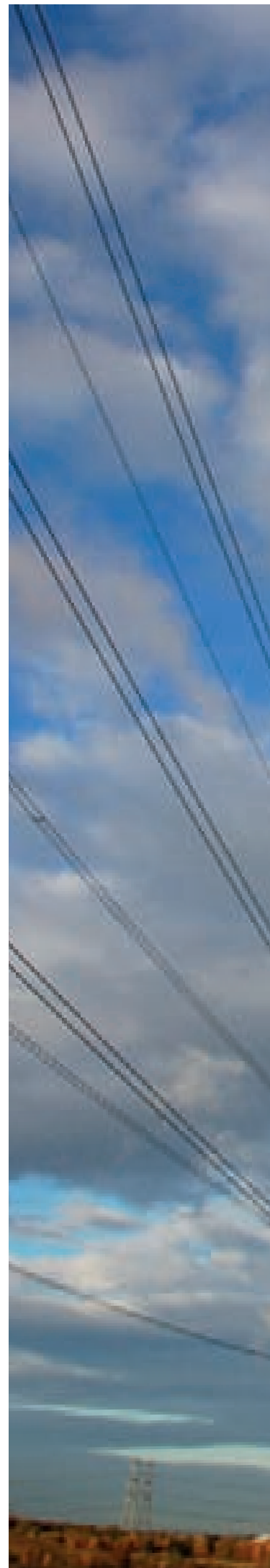
We need innovative
solutions from
industry, academia
and the Government.

Section 1

Key challenges

**Countering the terrorist
threat: ideas and innovation**

How industry and academia
can play their part

Reducing the vulnerability of crowded places

Crowded places are attractive terrorist targets. Securing these locations presents significant challenges: the threat is very difficult to detect, and some existing security methods are extremely resource intensive or have the potential to intrude unreasonably into the privacy of the general public.

Common features:
– busy, high volume movement of people
– noisy and chaotic
– open or multiple access points
– mixture of enclosed and open spaces
– large amounts of glass
– luggage, shopping bags, etc.

The challenges:
– we must make it more difficult to attack crowded places, with minimal inconvenience to the public
– we need to identify the individuals or items of luggage that are a threat among the crowd

– we have to do this with minimal intrusion
– we must also minimise injuries from flying glass or debris should a terrorist attack take place.

How can industry and academia help?
Industry and academia may be able to apply existing or new technologies to develop:

– systems to detect hidden explosives at a greater range
– systems and algorithms to detect and differentiate a wider range of materials and objects, with greater throughput and convenience for the public
– systems and algorithms to detect abnormal behaviour while minimising the intrusion on members of the public
– materials that improve the safety of the public in the event of a terrorist attack.

Reducing the vulnerability of crowded places is not a job for the Government or the police alone. We have engaged a wide range of local partners, including local authorities and businesses. The Government's recent public consultation about two draft guidance documents – 'Working Together to Protect Crowded Places' and 'Safer Places: A Counter-Terrorism Supplement'[1] – sought to develop a consensus about appropriate local interventions.

[1] www.homeoffice.gov.uk/documents/
cons-2009-crowded-places/

Protecting the national infrastructure

The national infrastructure delivers essential services, such as power, water, transport, finance and healthcare. Damage to that infrastructure can have severe economic impact or cause large-scale loss of life.

Common features:
– spread across the UK
– largely in private sector hands
– complex
– highly interdependent
– reliant on high technology
– need to maintain uninterrupted services

The challenges:
– much of our infrastructure is publicly accessible, making it vulnerable to attack
– the infrastructure is made up of essential services; an attack could affect hundreds, thousands or even millions of people in different ways
– insider knowledge (i.e. provided by someone with access to restricted information) could greatly increase the chances of a successful attack.

How can industry and academia help?
Industry and academia may be able to identify technology to help owners of the national infrastructure:

– improve protection and resilience
– mitigate potential damage in the event of an attack
– recover from an incident quickly and efficiently
– predict the impact of an attack, ensuring we are better prepared
– relay messages to the population in the event of an attack to minimise its impact.

Protecting against cyber terrorism

The UK is increasingly dependent on computers and the internet, but the very open nature of the digital network makes it vulnerable.

We expect terrorist groups to continue to favour high-profile 'conventional' or 'unconventional' operations over cyber attacks, and we must be vigilant against any future increase in their capability or change in intent. We will continue to need ways to protect ourselves from cyber attack and to find ways of recovering quickly should such an attack occur.

Common features:
– dependence upon cyberspace – even among people who do not themselves use computers
– viruses can travel around the world in minutes
– threats may come from anywhere in the world
– problems can multiply much faster than in the physical environment.

The challenges:
The advent of the internet and the ever increasing drive to join up communications systems has created new opportunities for crime and terrorism.

Our dependence on information technology makes us vulnerable. An attack could cause a major disruption, with the potential for significant economic damage through reduced productivity and damage to the UK's information assets. Alternatively an attack might permanently damage a single or many large systems or enable other crimes such as fraud.

How can industry and academia help?
Industry and academia may be able to develop technologies that could:

– protect UK citizens and UK trade from threats to the cyber environment
– help restore services/resolve issues following an attack
– provide self-help/self-healing information technologies
– protect against loss or corruption of data
– provide Information Assurance (IA)
– detect the origins of a cyber attack.

Improving analytical tools

Intelligence is vital to the detection, investigation and disruption of terrorism.

But the proliferation of information makes it increasingly difficult to identify the key facts that could provide warning of an attack on the UK. Improving intelligence and information analysis will enhance the speed and effectiveness of our counter-terrorist work.

Common features:
– data in different formats
– data from different sources
– data stored and owned by disparate organisations
– sophisticated techniques to hide information are readily available (for example steganography).

The challenges:
Terrorists may be located around the world and many may appear to be innocent citizens. Information on terrorist suspects can be hidden among masses of information about people in whom security agencies have no interest. The huge amount of raw information and the speed with which events take place makes identifying, tracking and pursuing terrorist suspects ever more difficult and complicated. The Government's analysis of this information must ensure that the privacy of innocent individuals is safeguarded.

How can industry and academia help?
Industry and academia may be able to provide new ways to:

– scan, examine, analyse and assess data and information
– detect and identify patterns, links, trends, etc
– present the most relevant and significant information to the user in the most appropriate and useful way, visually or otherwise
– safeguard the information collected by Government and, when required, ensure its secure destruction
– securely share relevant information across a wider range of stakeholders.
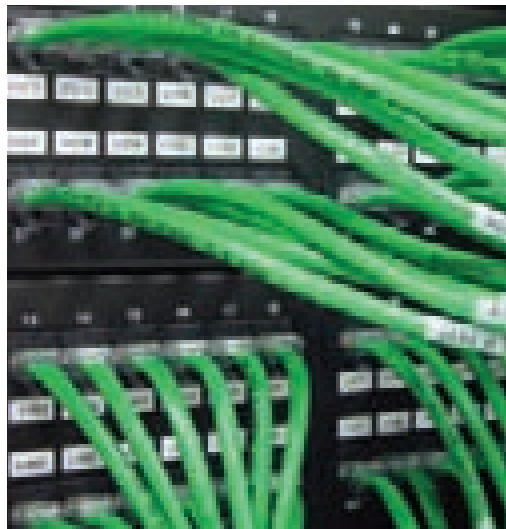
Section 1

Key challenges

London 2012 Games
Key facts

26
Olympic sports
in **34** venues

20
Paralympic sports
in **21** venues

14,000
competitors

27,500
media reps

9,800
coaches and officials

9,000,000
ticket holders

30,000
construction workers
(over several years)

70,000
volunteers

200
participating countries

Case study
The London 2012 Olympic and Paralympic Games

In 2012, London will host the Olympic and Paralympic Games – the world's biggest sporting event. They will be a celebration of sport and culture across the UK. The Government is committed to ensuring that the Games are safe and secure against all types of hazards and threats, including terrorism.

All the challenges set out in this document are relevant to the objectives of our Olympic Safety and Security Programme.

Given the complexity of the London 2012 Games, we plan to use only proven, effective and reliable technology solutions.

Earlier this year the Office for Security and Counter-Terrorism (OSCT) and the UK Security and Resilience Industry Suppliers' Community (RISC) established the Olympics Industry Advisory Group. In July the Government published an unclassified version of the London 2012 Olympics Safety and Security Strategy and a shorter explanatory pamphlet entitled 'London 2012: A Safe and Secure Games for All'[2].

Olympic Security objectives	Key challenge(s)
Protect the London 2012 Games venues, events, transport infrastructure, athletes, spectators, officials and other staff and ensure their safe enjoyment of the Games	Reducing the vulnerability of crowded places
Identify threats from terrorists or organised criminal gangs at an early stage and disrupt them before they can breach the safety and security of the Games	Improving analytical tools Protecting against cyber terrorism
Prepare for any events that might jeopardise the safe running of the Games and ensure we have the capacity to deal with them	Protecting the national infrastructure
Cooperate with international and domestic partners and communities to enhance security	All of the key challenges

[2] http://security.homeoffice.gov.uk/news-publications/publication-search/general/olympics-2012/

Key technologies

In this section we identify some of the key technologies of critical importance to solving the challenges we face. These technologies are not only useful in addressing the challenges covered in section 1 but also in responding to others across counter-terrorism.

We are already investing considerable time, effort and resources in science and technology. To make the most of this investment, we need to work closely with industry to integrate the results with existing products on the market and ensure the new products, services and technologies are widely available.

In describing these key technologies, we want to highlight what we see as the next steps in each area and where technological innovation is most likely to offer the biggest benefit to counter-terrorism. Our challenge is to know how far and how fast industry and academia can respond.
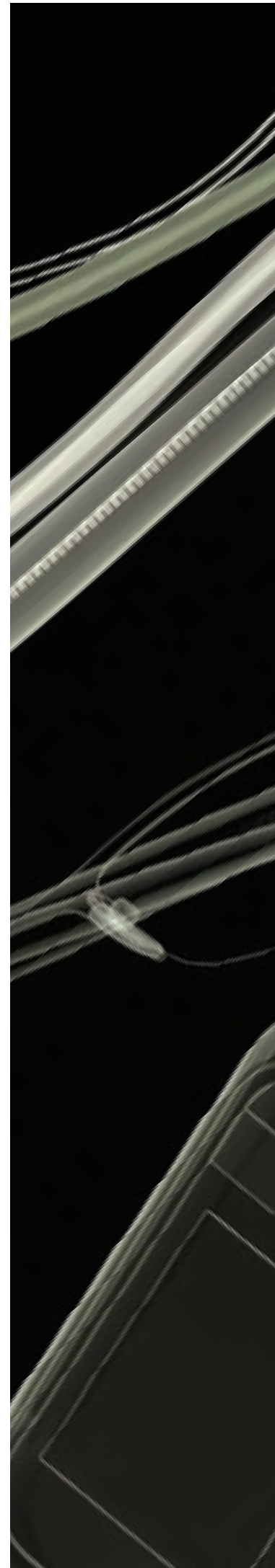
Our challenge is to
know how far and
how fast industry
and academia
can respond.

Section 2

Key technologies

**Countering the terrorist
threat: ideas and innovation**

How industry and academia
can play their part

Knowledge management

Knowledge management is about:
– connecting people who create,
  manage and exploit information
– enhancing the effectiveness and
  speed of knowledge systems
– finding ways in which IT systems
  can 'do some of the thinking'
– increasing the ways in which
  knowledge can be exploited
– developing new ways in which
  people can interact with information
  and with IT systems.

Why is Government interested?
Better knowledge management in
connection with counter-terrorism
will enable the Government to:

– use relevant data more effectively
  and more widely
– get much closer to real-time
  analysis and subsequent action
– achieve closer working and
  collaborative action across
  Government
– use our resources and IT systems
  more effectively.

Application
Departments and agencies responsible
for counter-terrorism need to derive
greater benefit from the information that
they create, hold, manage and use. They
also need to improve capabilities for
real-time analysis and support knowledge
management more effectively through
joined-up business processes.

What have we been looking at?
Government has been examining
some of the recent developments
in knowledge management, in both
industry and academia. For example,
the Ministry of Defence Counter-
Terrorism Science and Technology
Centre is, in collaboration with industry,
developing novel techniques for data
mining in unstructured data sets.

What do we need to do next?
We need to identify the next generation of
tools for information analysis, intelligence
creation, and visualisation.
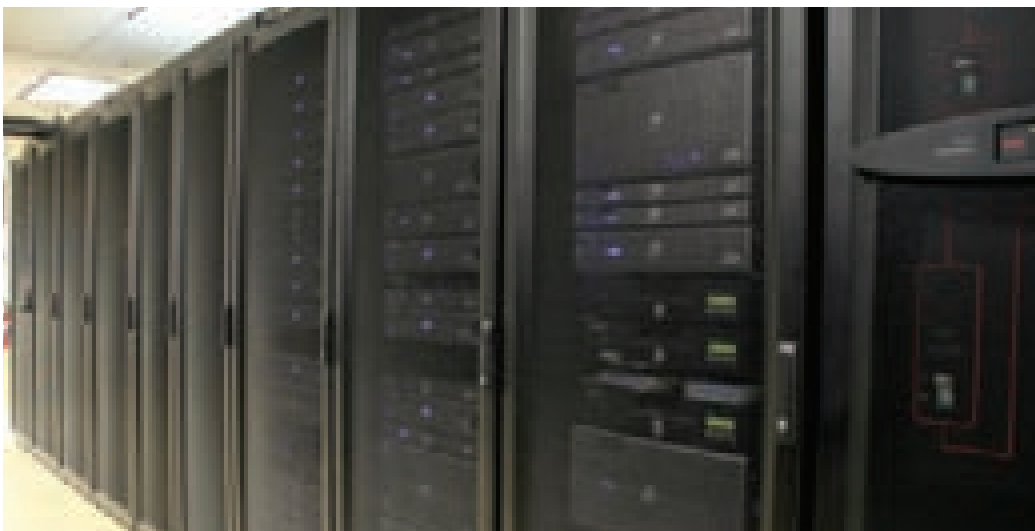
Biometrics

Biometrics include:
the secure establishment and verification of identity, and the protection of assets by restricting logical and physical access to authorised personnel.

Why is Government interested?
Biometric technologies support our counter-terrorist work because:

– they provide a means of validating individual identities, thereby reducing the opportunity for identity theft and misuse
– they are a key component in the UK Border Agency's strategy for securing our nation's borders
– they support the prevention, and investigation, of serious crime
– as part of the cross-Government identity management strategy, they promise more secure access to Government and commercial services.

Application
Biometric technology is currently being applied to:

– checking the identity of applicants for visas

– automated immigration services at major UK airports
– protect the national infrastructure.

In the future, we believe that biometrics will:

– remain essential to the secure identification of people entering and living in the UK
– offer a more secure and convenient method of controlling access to important buildings and the critical national infrastructure
– help assure the identity of individuals in high-value transactions for Government and commerce.

What have we been looking at?
Government departments continue to assess the security of biometric systems; research new system concepts for law enforcement; and work with other organisations to develop national and international standards.

What do we need to do next?
We need to:

– improve the processing of biometric data to aid reliable recognition
– secure authentication of Government users of mobile devices and online services to improve security
– develop integrated systems to make use of multiple sources of biometric data.

Section 2

Key technologies

**Countering the terrorist
threat: ideas and innovation**

How industry and academia
can play their part

Screening

Screening is:
systematic examination of people,
vehicles or cargo.

Why is Government interested?
Screening technologies allow us to:

– identify threats hidden on the body,
  in vehicles or in cargo
– discreetly identify threats in crowded
  places with minimal interference to
  innocent bystanders
– prevent threats entering high-value
  and vulnerable areas
– increase the number of materials and
  hazards that can be remotely identified
– improve the performance of the people
  operating screening equipment.

Application
Screening technology is currently
being applied across the UK, in our
ports, airports and in other high-risk
areas. Technologies must be reliable
and effective while enabling the rapid
movement of people or vehicles. We
would like to be able to screen people
and vehicles at their normal speeds of
travel – without imposing delay and with
minimal intrusion.

We anticipate that future screening
technologies will be able to achieve
current levels of security while
reducing the inconvenience to
and intrusion on the public.

What have we been looking at?
Government has been considering
the value in simultaneously exploiting
different parts of the electromagnetic
spectrum: for example, combining
measurements of radiation in different
parts of the spectrum may increase our
capabilities to detect certain materials
and to reduce the error rates involved
in detection and identification.

There has also been work on new methods
to detect and identify chemical, biological,
radiological and nuclear (CBRN) hazards.

What do we need to do next?
We need to find ways to:

– extend the range and increase the
  speed at which we can detect threats
– screen people less intrusively (for
  example scan people without requiring
  the removal of clothing or other
  belongings)
– integrate different screening
  technologies, to increase the confidence
  in both positive and negative results.

Physical protection

Physical protection means:
restricting access to improve protection, by the design and use of barriers or access controls; armouring and the development of tough new materials; and through the layout of buildings and infrastructure. This domain also includes research into the effects of explosives.

Why is Government interested?
The Government has a duty to protect citizens and the UK infrastructure. Physical protection technologies are important because they:

– reduce the threat posed by improvised explosive devices, sabotage or other hostile action
– increase public confidence in protection from attack
– enhance the resilience of the national infrastructure.

Application
Physical protection technology and knowledge are currently being applied to:

– critical areas in major UK cities to limit vehicle access/proximity to critical buildings and infrastructure
– improve the effectiveness of body armour for UK police and other personnel
– improve the design and layout of buildings, public spaces and major centres.

What have we been looking at?
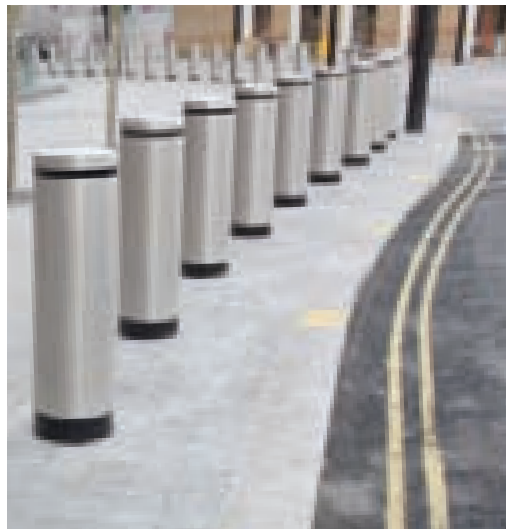Government has been looking at:

– making body armour lighter and less restrictive
– improving the cost-effectiveness of physical protection technology
– increasing use of aesthetic and/ or concealed physical protection technology.

What do we need to do next?
We need to continue to develop smart technologies that enhance protection without obstructing daily life, and deliver value for money.

Section 2

Key technologies

**Countering the terrorist
threat: ideas and innovation**

How industry and academia
can play their part

Countering Improvised Explosive Devices

Countering Improvised Explosive Devices (IEDs) means:
detecting and neutralising improvised explosive devices, and exploiting them for forensic/evidential purposes.

Why is Government interested?
Countering IEDs is important, in order to protect:

– the general public
– UK infrastructure
– the public transport system and infrastructure
– UK and coalition Armed Forces operating overseas.

Ideally, we would be able to detect IEDs on people, in luggage, in vehicles or unattended.

Application
Technology to counter improvised explosive devices is currently used in the UK to counter IED threats and overseas by the Armed Forces. In the future, we anticipate more widespread use of detection and neutralisation technologies in both areas.

What have we been looking at?
Government has been looking at means of detecting the chemicals that are found in IEDs, and/or the physics of IEDs.

What do we need to do next?
We need to find ways to:

– improve early detection and neutralisation, either before or during manufacture or before or after devices are in place and live
– improve detection and identification of hidden/covered devices
– improve identification of IEDs from a greater distance
– improve the confidence in our detection capabilities (reduce error rates)
– improve the integration of detection techniques, such as multi-spectral integration
– widen the range of capabilities to neutralise devices.

Partnership is vital to the success of our counter-terrorism work. We need to make the most of the expertise and knowledge held by industry and academia, and to foster strong, collaborative partnerships.

In this section we explain how industry and academia can talk to Government and deliver scientific and technological solutions to the problems we face.

Section 3
How to get involved

HOW IS THE GOVERNMENT SUPPORTING PARTNERSHIP WITH INDUSTRY?

The Office for Security and Counter-Terrorism (OSCT) was set up as part of the Home Office in March 2007. It supports the development, direction, implementation and governance of CONTEST. It also delivers those aspects of CONTEST which fall to the Home Office. In relation to science and technology, its role is to coordinate and direct research and development relevant to counter-terrorism.

OSCT needs the support of industry, and is a significant customer of the UK security and resilience industry. We are working in partnership with industry to develop new technologies and new applications for existing technology.

OSCT has established an Industry Engagement Team to bridge the gap between policy makers and industry. The team will help industry access and talk to the Government 'problem owner'. If you would like to contact the team to discuss any of the challenges posed in this paper or to seek Government input or support, please email:
CONTESTscience@homeoffice.gsi.gov.uk

As we sharpen our understanding of the challenges, we will draw upon industry to help us find solutions. Examples of how we might achieve that include: mechanisms provided by RISC (the UK Security and Resilience Industry Suppliers' Community) or similar bodies, commercial relationships with preferred suppliers or 'ideas factory' style events bringing industry and academic experts together to create solutions for specific problems.

INSTINCT: INNOVATION AND FUTURES
INSTINCT (Innovative Science and Technology In Counter-Terrorism) is a cross-Government innovation project, led by the OSCT. It aims to improve the Government's ability to be an effective customer of innovation. This involves funding projects with a higher technical risk than would normally be accepted, in an effort to rapidly identify productive lines of work.

As part of the INSTINCT programme, the MOD's Centre for Defence Enterprise hosted an industry engagement event in 2009 based around the challenge of securing Crowded Places.
www.security.homeoffice.gov.uk/science-innovation/instinct

THE TECHNOLOGY DEMONSTRATOR
OSCT will work with industry to create realistic test environments. During 2009, INSTINCT plans to use a technology demonstrator to allow potential suppliers to test products and services with the potential to reduce the terrorist threat in a realistic environment.

We have started collaborating with a small number of companies to find the best way to test and demonstrate systems, products and applications. An open architecture will mean that Government is able to see how specific applications could be integrated with others for greatest benefit.

I'M IN INDUSTRY. HOW CAN I TALK TO GOVERNMENT?

The Government has a long track record of working with the science and technology industry across the military, security and intelligence markets. OSCT works with industry through a variety of routes including trade associations, exhibitions, industry primes and the Technology Strategy Board.

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, representing over 2,000 companies ranging from prime contractors and global leaders through to small and medium enterprises and start-ups.
www.riscuk.org

The trade associations are:

– the Society of British Aerospace Companies (SBAC)
www.sbac.co.uk

– the Association of Police and Public Security Suppliers (APPSS). This is part of the Defence Manufacturers' Association, DMA
www.appss.org.uk

– the British Security Industry Association (BSIA)
www.bsia.co.uk

– Intellect (the UK trade association for the technology industry).
www.intellectuk.org

(The SBAC and the DMA will merge in 2010.)

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 Communication Technology (ICT)
– Detecting suicide bombers
– Olympics.

The purpose of these five groups is to exploit government-funded research better, develop Government's counter-terrorism needs, focus private sector investment and enable Government's access to industry innovation.

The advisory groups are good examples of how industry can provide Government with expert advice without commercial prejudice. The list and membership of such groups may evolve but the central tenet of industry working with Government as a partner to deliver our CONTEST counter-terrorism strategy will remain.

We also plan to do all we can to support SMEs, many of whom have excellent records in creating innovation.

We will continue to work with industry and academia through other routes. These will include industry liaison, responding to enquiries, networking at conferences, exhibitions and events and through exploring opportunities in existing science and technology projects.

Section 3

How to get involved

**Countering the terrorist
threat: ideas and innovation**

How industry and academia
can play their part

I'M IN INDUSTRY OR ACADEMIA WITH A BRIGHT IDEA. WHO SHOULD I CONTACT?

This section helps you decide who to contact with a good idea. It describes some of the Government bodies that help develop and invest in counter-terrorism technologies.

OSCT

The Industry Engagement Team in OSCT will help industry access the relevant Government Department. Email: CONTESTscience@homeoffice.gsi.gov.uk

HOME OFFICE SCIENTIFIC DEVELOPMENT BRANCH

The Home Office Scientific Development Branch (HOSDB) helps to apply technology to reduce crime and counter-terrorism. It 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. It 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.

www.scienceandresearch.homeoffice.gov.uk/hosdb

THE CENTRE FOR DEFENCE ENTERPRISE: FUNDING PROOF OF CONCEPT

This is the first point of contact for anyone with a disruptive technology, new process or innovation that has a potential defence application. The Centre acts as a gateway between the outside world and the Ministry of Defence (MOD), bringing together innovation and investment for the defence market, ensuring that our frontline forces have the best battle-winning technologies for the future.
www.science.mod.uk/engagement/enterprise.aspx

MOD CT CENTRE

With terrorist threats becoming increasingly sophisticated and diverse, science and technology is playing an ever more important role in the planning, preparation and prosecution of military and security operations. The Counter-Terrorism Centre serves as a hub to make the most of resources in the MOD. The Centre not only represents MOD's science and technology laboratories, but works closely with academia and industry on counter-terrorism and national security projects. While the primary objective of the Centre is to focus on MOD requirements, it can also help other government departments engaged in domestic counter-terrorism.
www.ctcentre.mod.uk

CPNI

The Centre for the Protection of National Infrastructure (CPNI) is the Government body responsible for protective security advice to owners and operators of the UK's Critical National Infrastructure. CPNI provides advice on physical, personnel, and information security.
www.cpni.gov.uk

HOW IS THE GOVERNMENT COMMUNICATING WITH ACADEMIA?

The UK's universities are renowned for world-class research and innovation, and so have an important role to play in developing the technological innovation we need to protect the UK. We are actively seeking innovation from universities and encouraging dialogue so that we learn about relevant research, innovations and technologies.

AURIL

AURIL is the Association for University Research and Industry Links. Organised by university staff, its membership comprises around 1,400 academics, nearly 100 universities, and other research establishments and companies. We use AURIL as one route to the research base in UK universities. We encourage researchers who would like to contribute to counter-terrorism research to join AURIL.

www.auril.org.uk

CPNI ACADEMIC OUTREACH

CPNI runs a significant research and development programme and wants to encourage research groups to tackle issues relating to protective security.

CPNI aims to ensure researchers understand security needs in order to stimulate and give direction to future research efforts. CPNI will also identify existing research that relates to their own research interests.

CPNI works directly with individuals and research groups, supporting/funding council activities and commissioning work from university consultancies.

www.cpni.gov.uk

RESEARCH COUNCILS UK

Research Councils UK (RCUK) is a partnership between the seven UK research councils (RCs). RCUK coordinates the delivery of multi-disciplinary research in six priority areas.

One of these is *Global uncertainties: security for all in a changing world*. The RCs will work together to address five interrelated global threats to security – Poverty (and Inequality and Injustice), Conflict, Transnational Crime, Environmental Stress and Terrorism.

Government will also fund the RCs to give research funding for the technologies described earlier in this document.

www.rcuk.ac.uk/research/ccprog/security.htm

WHAT OTHER FUNDING IS AVAILABLE FOR MY RESEARCH AND PROOF OF CONCEPT?

THE TECHNOLOGY STRATEGY BOARD – DRIVING INNOVATION

In 2007 the Government established the Technology Strategy Board (TSB) to stimulate technology-enabled innovation in the areas that offer the greatest scope for boosting UK growth. It promotes, supports and invests in technology research, development and commercialisation. It advises Government on how to remove barriers to innovation and accelerate the exploitation of new technologies. The TSB works in areas where there is a clear potential business benefit, helping today's emerging technologies become the growth sectors of tomorrow.
www.innovateuk.org

TSB SBRI

The Technology Strategy Board's Small Business Research Initiative (SBRI) is a procurement programme helping to bring new technologies to market. SBRI is aimed at businesses working on the development of an innovative process, material, device, product or service. Government departments fund research and development services, leading to the possibility of future commercial procurement in the public sector.
www.innovateuk.org/deliveringinnovation/ smallbusinessresearchinitiative.ashx

EU RESEARCH FUNDING

The EU invests in several research programmes in security and resilience. These include:

– Framework Programme 7 (FP7)
  ec.europa.eu/research/fp7/index_ en.cfm?pg=security
– European Security Research and Innovation Forum (ESRIF)
  www.esrif.eu

– the European Research Area
  cordis.europa.eu/era/home_en.html
– European Technology Platforms (ETPs)
  cordis.europa.eu/technology-platforms

EU: FRAMEWORK PROGRAMME 7

Of the above EU research programmes, FP7 has in the past awarded most funding to UK organisations. Security is one of the 10 FP7 themes.

The Security theme awards about €120 million annually for research related to a set of security topics defined by the EU. This is expected to rise to €200 million in the next round. The topics are usually announced formally in September, inviting responses by December. Most bids are from consortia; consortium members may come from the private sector, the public sector or academia.

The bids submitted in December 2008 have led to the provisional award of around €14 million to UK organisations.

The UK Government contributes to the debate that leads to the selection of topics, but plays no part in determining which proposals are selected for funding. We encourage you to participate in bidding for this funding.
www.dius.gov.uk/dius_international/science_ and_innovation/eu_framework_programme

cordis.europa.eu/fp7

HOW CAN I BECOME A SUPPLIER TO THE GOVERNMENT?

WHAT SHOULD I DO NEXT?

OSCT is trying to increase the access of industry and academia to Government, to look for ever more ways to develop new capability.

The demands and urgency of CONTEST mean that the Government increasingly needs to take considered risks in our commercial approach. The Government will also adopt new approaches aimed at making the market more accessible to SMEs and those who have not traditionally operated in the security and resilience arena.

Government will continue to place our procurement needs on the open market, using our existing online portals:

Supply2.gov.uk
The Office of Government Commerce (OGC) operates the www.supply2.gov.uk web portal. This is the only official Government portal offering lower-value contracts and aims to provide small businesses with access to contracts typically below £100,000. The potential market is expected to exceed £175 billion this year within the UK alone.
www.supply2.gov.uk

Bluelight.gov.uk
This website was launched in November 2004 to provide an e-tendering solution that is available to all emergency services. Many police authorities and fire and rescue services use it to procure goods and services.
www.bluelight.gov.uk

We have set out in this booklet how we intend to stimulate and encourage a very wide range of innovation to support counter-terrorism efforts and keep the UK, its people and interests safe.

Some innovations will come from breaking new ground, while others will come from applying existing technologies to new situations, new environments or new purposes.

If you are in industry or academia and have a good idea with the potential to support our security and counter-terrorism work, we want to hear from you.

If you are unsure about which is the best department or body for you to contact in the first instance, please get in touch with the CONTEST Portfolio Office in the OSCT. We will be happy to advise you. Email: CONTESTscience@homeoffice.gsi.gov.uk

Glossary

Abbreviation	Meaning
APPSS	Association of Police and Public Security Suppliers
AURIL	Association for University Research and Industry Links
BSIA	British Security Industry Association
CBRN	Chemical, Biological, Radiological, Nuclear
CDE	Centre for Defence Enterprise
CNI	Critical National Infrastructure
CONTEST	The United Kingdom's Strategy for Countering International Terrorism
CPNI	Centre for the Protection of National Infrastructure
CSS	Cyber Security Strategy
CT	Counter-Terrorism
DMA	Defence Manufacturers Association
Dstl	Defence Science and Technology Laboratory
EPCIP	European Programme for Critical Infrastructure Protection
ESRIF	European Security Research and Innovation Forum
ETP	European Technology Platform
FP7	Framework Programme 7 (an EU programme)
HOSDB	Home Office Scientific Development Branch
IA	Information Assurance
IAG	Industry Advisory Group
IED	Improvised Explosive Device
INSTINCT	INnovative Science and Technology IN Counter-Terrorism
MOD	Ministry of Defence
OGC	Office of Government Commerce
OSCT	Office for Security and Counter-Terrorism
RC	Research Council
RCUK	Research Councils UK
RISC	UK Security and Resilience Industry Suppliers Community
S&T	Science and Technology
SBAC	Society of British Aerospace Companies
SBRI	Small Business Research Initiative (organised by the TSB)
SITC	Security Innovation and Technology Consortium
SME	Small or Medium Enterprise
TSB	Technology Strategy Board