

Counter Terrorism

Driver – Political, Social, Legal

Related Drivers – Organised Crime, Data Handling, Crime, Police Powers, Public Perceptions of the Police, Public Perceptions of Crime, Information Sharing, Collection and Storage of Personal Information

Political Context

The UK continues to face a real and serious threat from international terrorism examples being most recently, 7/7 London Bombings and the 2007 Glasgow International Airport Attack. Since 2003 the United Kingdom has had a long-term strategy for countering international terrorism known as CONTEST. Its aim is to reduce the risk from international terrorism through four strands:

- Prevent – preventing terrorism by tackling radicalisation of individuals
- Pursue – pursuing terrorists and those that sponsor them
- Protect – protecting the public, key national services and UK interests overseas
- Prepare – preparing for those consequences.¹

In March 2008, the Government published the *National Security Strategy of the United Kingdom: Security in an interdependent world* which outlines the government's response to counter terrorism built around the CONTEST strategy. The future priorities of counter-terrorism laid out in the National Security Strategy include the following:

- Delivering the Government's Public Service Agreement (PSA) – to 'reduce the risk to the United Kingdom and its interests overseas from international terrorism'
- Continuing to build our capacity to detect and disrupt terrorists, in the United Kingdom and overseas, through investment in the police and the security and intelligence agencies
- Enhancing the protection against terrorism provided by new border technology and the new UK Border Agency
- Increasing our capacity to deal with the consequences of a terrorist attack
- Delivering the improved range of projects and programmes to tackle violent extremism, including working with overseas partners
- Addressing grievances and challenging violent extremism narrative.²

The report *Cutting Crime: A new partnership* states the following regarding counter terrorism:

“to make a difference on the ground, to connect with local communities to increase confidence and to ensure that police have the sources of information to counter every level

of terrorist activity, officers at every level need to be equipped with appropriate knowledge and skills".³

In May 2009, the Prime Minister published an updated version of CONTEST which retained the Prevent, Pursue, Protect and Prepare framework.⁴ Some of the key objectives over the next three years include:

- Develop supporting intelligence, analysis, and information; and to improve strategic communications to prevent violent extremism and radicalisation within Britain (Prevent)
- Increase detection and investigation capability and capacity (Pursue).

Politically, counter terrorism is no longer being treated as a stand alone function of police forces. Sir Ronnie Flanagan has argued that neighbourhood policing can play role in supporting counter terrorism activity.⁵ The Home Affairs Select Committee points to examples where local intelligence gathered through neighbourhood policing is being used to help tackle terrorism and other serious crime. The Committee suggests that all forces should ensure that they have adequate systems in place so that intelligence can be shared easily between neighbourhood officers and specialist and response teams.⁶ This type of activity can support the four major threads for the CONTEST strategy.

Prevent

In April 2008, the Home Secretary announced the allocation of investment into ring-fenced posts, paid for by the Comprehensive Spending Review (CSR), to support the Prevent Strategy in 24 'priority' police forces.⁷ In the same month the Association of Chief Police Officers (ACPO) issued its *Prevent Strategy and Delivery Plan* that outlined how the police service would use the funding to create additional capabilities at force level and improve the sharing of intelligence and community engagement.⁸

Much work has been issued regarding the prevent stream of the counter terrorism strategy since the launch of CONTEST in 2006:

- The '*Preventing Violent Extremism: Next Steps for Communities*' report outlines the Government's priorities for tackling violent extremism.⁹ The report highlights that preventing violent extremism is core business for local authorities and police services. (DCLG)
- Upgraded guidance on shared values that can help universities and higher education colleges to tackle violent extremism on campus.¹⁰ The guidance also contains specific information engagement with the police. (DIUS)
- The Home Secretary, in conjunction with the Communities Secretary and the Secretary of State for Children, Schools and Families launched new guidance in July 2008 to help and support police, local authorities, schools, and community groups tackle violent extremism and prevent radicalisation. (Home Office, DCSF, DCLG)
- £12.5 million to schemes including:

- Extending police led multi-agency projects to identify and support those at risk of being targeted by violent extremists
- Working with young people whose previous contact with the criminal justice system has left them vulnerable to extremist views.¹¹

According to the Her Majesty's Inspectorate of Constabulary (HMIC) Inspection report '*Prevent: Progress and Prospects*' all forces have moved beyond the critical stage of planning and are in different stages of implementation:

- The majority of posts are in place – by the end of January 2009 the service had deployed 96% of the resources
- Staff are developing within their roles to deliver capabilities detailed within the ACPO strategy
- Structures are being developed – eight forces, including the West Yorkshire and Thames Valley forces (both assessed to be among the six forces with the highest vulnerability), are 'advanced' in their development of structures to support 'Prevent';
- Awareness among front-line staff is improving
- There are an increasing number of examples where the police, working with partners, intervene to disrupt radicalisers or support individuals vulnerable to violent extremist influences.¹²

Pursue

In April 2007 an integrated and national operation network was launched which included three Counter Terrorism Units (CTUs) and the Metropolitan Police Service's Counter Terrorism Command. These units work with forces and in collaboration with the Security Service bringing counter terrorism intelligence analysis and development functions together with investigations and operational activity.

Parliament's Intelligence and Security Committee (ISC) published a review of intelligence concerning the 7/7 London terrorist attacks in May 2009. The review was carried out as part of an investigation by the ISC to determine whether the attacks could have been prevented. The Committee concluded that they could not criticise the judgments made by MI5 and the police based on the information that they had and their priorities at the time.¹³ The Committee points to the need for improvements in exploiting information held by the Police and the intelligence and security agencies, and in maintaining statistics on terrorist-related convictions.¹⁴

Protect

The HMIC Inspection report '*Leading from the Frontline*' looked into the supervision and leadership of police sergeants, particularly critical incident management. Points emerging from the inspection are that although staff seemingly express confidence in their own ability to respond, many do not understand the term 'critical incident' and have received little

guidance or training. It appeared to inspectors that training in this area has not been delivered systematically across forces.

HMIC is concerned that existing preparatory processes, including training, within the police service are not equipping frontline sergeants to recognise and effectively manage critical incidents, and the risks associated with them. ACPO should therefore develop a framework to implement the NPIA 'Practice Advice on Critical Incident Management' in all forces which should be completed by October 2008.¹⁵

Economic Context

In June 2008, ACPO Terrorism and Allied Matters (TAM) planned to review the effectiveness of funded posts and utilise findings to inform the 2009/2010 Comprehensive Spending Review (CSR) allocation.

Whilst this review was not undertaken, the National 'Prevent' Delivery Team (NPDU) is considering information from the HMIC inspection '*Prevent: Progress and Prospects*', and renewed information about vulnerability, to inform the next CSR allocation. As a result, ACPO TAM has proposed that 2009/2010 CSR funding is apportioned to provide:

- One Sergeant post to the 19 forces currently unfunded (with five forces also receiving a researcher) (Total 24 posts)
- Additional Counter Terrorism Intelligence Officer / Community Engagement Officer posts in specific Basic Command Unit, based upon a reassessment of risk, within 17 forces; some of which are already in receipt of CSR funding (total 23 posts)
- 13.5 posts to support the NPDU or posts elsewhere to support 'Prevent' related activity.

The evidence from *Prevent: Progress and Prospects* suggests that supporting currently unfunded forces with dedicated 'Prevent' resources should provide a tangible benefit.

Social Context

The 'Prevent' strategy includes work to challenge the ideology behind violent extremism, disrupt those who promote violent extremism and support communities and institutions in developing strategies against it. Up until the 2005 attacks countering terrorism were mainly done by specialist units. The 2005 attacks dawned a new age, as people who felt alienated and grievous, planned and resourced their attacks in cities and towns across the UK, far away from their targets of attacks.

The Police face the challenge of 'getting upstream' – tackling radicalisers who groom and exploit vulnerable people, and foster grievance and alienation. There are various sources and institutions from which radicalising influences can originate. The 'Prevent' strategy aims to recognise and tackle the causes of radicalisation and vulnerability via local authorities, police, schools, universities and prisons, all working alongside communities.

The police service is in the process of mobilising its staff and partners, beyond counter terrorism specialists, to engage in preventing violent extremism. Challenges in making this progress should not be under-estimated, particularly following the demands of building the national Counter Terrorism Network (see [Political Context](#)). Establishing 'Prevent' is being taken forward through three significant cultural shifts:

- Counter terrorism specialists within the police service, and their partner agencies, are understanding the need for sensitive information in their possession to be made available for local partnerships - a recognition that the intelligence 'need to know' principle includes the 'needs' of local authority officials, schools and others dealing with vulnerable communities
- Responsibility for preventing violent extremism and counter terrorism is being adopted within the wider policing family, and increasingly by those dealing with partnership and community policing
- The police are harnessing the significant trust and confidence, built upon the foundations of tackling crime and disorder, to agree courses of action for tackling terrorist criminality.¹²

Technology Context

An emerging issue for 2009 / 10 will be the availability and capacity of forces to undertake the analysis of material that impacts upon 'Prevent', in particular the capacity to prepare and update Counter Terrorism Local Profiles (CTLP). In February 2009, the Office for Security and Counter Terrorism (OSCT) announced that approximately £700,000 would be available to forces to provide analytical capacity to produce the first tranche of CTLPs. Bids for this money are currently being considered. However, this funding is for 2009/10 only and whilst this is welcome, the long term requirement for analytical support to support 'Prevent' needs to be reviewed. HM Inspector's recommendation concerning the review of capability and informing future capacity building should include analytical resources.¹²

Skills in computer forensic examination and other ICT skills will be needed to glean counter terrorism activity from these data transmissions received as part of the Interception Modernisation Programme (IMP) (see [Legal Context](#)). At the moment the UK law enforcement has about 300 police officers in formal High-Tech Crime unit and employs overall 500-600 specialist computer forensic examiners, a mix of police officers and civilian employees. In most police forces there are backlogs in excess of six months for "non-urgent" analysis (i.e. where there is no immediate threat to life or serious conspiracy in progress).¹⁶

Legal Context

The **Regulation of Investigatory Powers Act 2000 (RIPA)** makes provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed.¹⁷

The Prime Minister ordered a *Review of Intercept of Evidence* in September 2007 to advise on whether a regime to allow the use of intercepted material in court could be devised that would facilitate bringing cases to trial while protecting national security.

The result of this review, *Privy Council Review of Intercept as Evidence* (commonly referred to as the Chilcot Report) concluded that it would be possible to provide for the use of intercept as evidence in criminal trials in England & Wales by developing a robust legal model, based in statute and compatible with the European Council for Human Rights.

The report states any legal regime that was developed should meet nine operational recommendations.¹⁸ In a statement to Parliament, the Prime Minister announced the Government will accept the Chilcot report's recommendation to allow intercept as evidence to be used in court on the basis that the intercept was only used when it could not be gained in another way.

The Prime Minister said that an implementation plan would set out how it would be introduced but that if the nine conditions / recommendations in the report could not be met then intercept as evidence would not be allowed to be used in evidence.¹⁹

It was announced in the Queen's speech in November 2006 that a new **Counter Terrorism Bill** would be introduced.²⁰ This included provision regarding further powers to gather and share information and **provides statutory data sharing powers for the intelligence and security agencies**. It also puts the police's counterterrorist data DNA database on a similar statutory footing to the National Police Database. Additionally, police will be provided with powers to enable them to temporarily hold travel documents from individuals suspected of wanting to travel abroad or terrorism-related purposes.

The Bill also included provision about the detention and questioning of terrorist suspects and amends the **pre-charge detention** limit from 28 days to 42 days. This also includes changes to **post charge questioning** allowing terrorist suspects to be questioned after charge on any aspect of the offence and for adverse inferences to be drawn from silence in relation to these questions.

On 13 October 2008, the 42 day detention limit of terrorist suspects failed to pass through the House of Lords by a defeat of 309 votes to 118.²¹ The Bill continued through the House of Commons without the provision and gained Royal Assent on 26 November 2008. The Home Secretary has announced the government would not attempt to override the will of the Lords, instead a new bill to allow 42-day detention would be introduced if an emergency warranted it.

The **Communications Data Bill**²² allows for the collection and retention of communication data, including data not required for the business purposes of communications service providers, for national security purposes. Communications data plays a key role in counter-terrorism investigations. The Bill will implement the remainder of the European Union's Data Retention Directive. Additionally the Bill will potentially contain legislation underpinning the Interception Modernisation Programme (IMP). IMP is based on the model where Communications Service Providers (CSPs) collect and store the data and where public authorities have access to it.

The Government are consulting on ways to collect and retain communications data as part of IMP (until 20 July 2009) and seeks views on how to strike the balance between privacy and security. The consultation '*Protecting the public in a changing communications environment*' proposes:

- Legislation to ensure all data that public authorities might need, including third party data²³ be collected and retained by CSPs such as the fixed line, mobile and WiFi operators.
- Having CSPs process the data to enable specific requests by public authorities – such as the police and Security Service - to be processed quickly and comprehensively.²⁴

Current legislation governing surveillance - RIPA - draws a strong distinction between communications data and communications interception. Interception refers to the content of the communication in some cases, especially data from Internet Service Protocols (ISPs) content is needed to determine whether the data is relevant.

Passage of the IMP would mean large numbers of requests for what might be considered authorisations for “communications data” would need to be converted into requests for “intercepts”. As the product of interception is currently inadmissible in court, a number of new problems arise for investigators and prosecutors about what they can use in evidence and what they are required to disclose under Criminal Procedures and Investigations Act.¹⁶

A briefing by the Policy Engagement Network at the London School of Economics and Political Science (LSE) recently examined the Interception Modernisation Programme (IMP) consultation, '*Protecting the public in a changing communications environment*'. The briefing states “*for finding and identifying the fraction of users of interest to law enforcement and what exactly they are up to, we will still need the police to do policing work.*” Collecting communications data is only one aspect of the investigation. Skills in terms of what can be presented in court and linked to specific individuals are hugely significant.¹⁶

Potential Skills Needs

Analytical skills – to visualize, articulate, and solve complex problems and concepts, and make logical decisions based on available information

Collaborative working skills – working effectively with colleagues and other law enforcement agencies to protect UK borders

Communication skills – effective communication between neighbourhood policing, local partners, communications, intelligence agencies and communities

Community intelligence skills – aligning skills and experience of police officers and staff to neighbourhoods to support engagement and tackle crime

Community policing skills – to discuss and set local priorities and encourage more people to become involved in crime reduction alongside operational policing tasks

Computer forensic skills – analysis of information contained within and created with computer systems and computing devices, typically in the interest of discovering what happened, when it happened, how it happened, and who was involved

Covert surveillance skills - to use these skills to identify potential sources of radicalisation

Critical incident management skills – recognise and effectively manage critical incidents

Data collection and management skills – recording and collecting data in line with a particular system: Counter-Terrorism Local Profiles (CTLTP)

Data analysis and reporting skills – analysis of CTLTP to focus ‘Prevent’ work in the community

Intelligence gathering skills – to scan multiple data sources and follow leads

Intelligence information sharing skills between police forces, other intelligence and security agencies, communities and local partners

Inter-agency working skills – to work effectively with two or more governmental agencies

Interviewing skills in post charge questioning of terror suspects in relation to the Counter Terrorism Bill

IT skills – general awareness and understanding of current ICT environment and changing landscape

Multi-agency working skills – to work with other agencies to protect the UK

Partnership working skills – to work effectively with other agencies to a common goal and standards

Relationship building skills – to engage with the community and young people and maintain public confidence

¹ [HM Government \(2006\) *Countering International Terrorism: The United Kingdom's Strategy*. Cm 6888, London: The Stationery Office Ltd.](#)

² [Cabinet Office \(2008\) *National Security Strategy of the United Kingdom: Security in an interdependent world*. Cm 7291, London: The Stationery Office.](#)

³ [Home Office \(2007\) *Cutting Crime: A new partnership 2008-2011*. London: Home Office.](#)

⁴ [HM Government \(2009\) *The United Kingdom's Strategy for Countering International Terrorism*. Cm 7547, London: The Stationery Office.](#)

⁵ [Flanagan, Sir Ronnie \(2008\) *The Review of Policing: Final Report*. London: Home Office.](#)

⁶ [House of Commons Home Affairs Select Committee \(2008\) *Policing in the 21st Century*. Seventh Report of the 2007-08 Session. HC 364-I, London: The Stationery Office Ltd.](#)

⁷ [Home Office Press Release, 3 June 2008, '£12.5 million to tackle radicalisation and help prevent violent extremism in communities'.](#)

⁸ [ACPO \(2008\) *Prevent: The Policing Response to the Prevention of Terrorism and Violent Extremism: Strategy and Delivery Plan*. London: ACPO.](#)

⁹ [Department for Communities and Local Government \(2008\) *Preventing Violent Extremism: Next Steps for Communities*. London: Department for Communities and Local Government.](#)

¹⁰ [Department for Innovation, Universities and Skills \(2008\) *Promoting Good Campus Relations, Fostering Shared Values and Preventing Violent Extremism in Universities and Higher Education Colleges*.](#)

¹¹ [Home Office Press Release, 3 June 2008, '£12.5 million to tackle radicalisation and help prevent violent extremism in communities'.](#)

¹² [HMIC \(2009\) *Prevent: Progress and Prospects*. London: HMIC.](#)

¹³ [Intelligence and Security Committee \(2009\) *Could 7/7 have been prevented? Review of the intelligence on the London Terrorist Attacks on 7 July 2005*. Cm 7617, London: The Stationery Office Ltd.](#)

¹⁴ [Prime Minister Written Ministerial Statement, 19 May 2009, 'Intelligence and Security Committee's review of the intelligence on the London terrorist attacks in July 2005'.](#)

¹⁵ [HMIC \(2008\) *Leading from the Frontline: Thematic inspection of frontline supervision and leadership at the rank of sergeant in the Police Service of England & Wales*. London: Home Office](#)

¹⁶ [Policy Engagement Network \(2009\) *Briefing on the Interception Modernisation Programme*. London: London School of Economics and Political Science.](#)

¹⁷ [Regulation of Investigatory Powers Act 2000 \(UK\)](#)

¹⁸ [Privy Council \(2008\) *Privy Council Review of Intercept of Evidence*. London: HM Government](#)

¹⁹ [Prime Minister statement, 6 February 2008, 'Intercept as evidence is permissible'.](#)

²⁰ [BBC News Online, 15 November 2006, 'Queen's Speech'](#)

²¹ [BBC News Online, 13 October 2008, 'A tactical retreat on 42 days'](#)

²² [Communications Data Bill \(UK\)](#)

²³ Third party data is data generated by communications services based overseas but crossing the networks in the UK.

²⁴ [Home Office \(2009\) Consultation: *Protecting the public in a changing communications world*. Start date: 27 April 2009, End date: 20 July 2009.](#)