Australian Government
Department of Defence
Defence Science and
Technology Organisation

Science and Technology Support for National Security: An International Review

Rick Nunes-Vaz and Leung Chim

Counter Terrorism and Security Technology Centre
Defence Science and Technology Organisation

DSTO-TN-0888

ABSTRACT

A critical review of open source literature enables comparison of the US, UK and Canadian approaches to the development, coordination and harnessing of science and technology for national (or homeland) security, and the relative roles of Defence and non-Defence S&T providers. The review was undertaken to inform the S&T Companion Review to the Defence White Paper, and to provide insights relevant to Australian arrangements.

The analysis shows that there is: increasing effort to improve the alignment and consistency of policies and strategies relating to national security and related science and technology; growing acknowledgement of the critical national role of niche Defence S&T capabilities; greater strategic coordination of national security capability management supported by national security S&T providers, including Defence; growing recognition of the need to overcome departmental stovepipes, particularly the military/civilian divide; growing use of programmatic (or problem-based) approaches to funding, development, management and exploitation of S&T in national security; and an increasing focus on cross-Departmental collaboration, information sharing, and the promotion of enduring S&T 'communities of practice'.

Published by

DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-014-513
May 2009

APPROVED FOR PUBLIC RELEASE

Sicence and Technology Support for National Security: An International Review

Executive Summary

This paper documents the findings of a critical review of open source literature to compare US, UK and Canadian approaches to: the development of national security[1] capability; the mechanisms by which science and technology (S&T) support is harnessed; and the relative roles of Defence and non-Defence S&T providers.

The review was undertaken to inform the S&T Companion Review to the Defence White Paper, by contextualising Defence S&T contributions to national security goals outside strict support of Defence objectives. Its purpose was to inform attempts to improve Australian national security arrangements, based on lessons learned overseas, and to help generate a longer-term vision for S&T support to whole-of-nation strategic challenges, such as national security.

The analysis shows that Canada and the UK and, from a low base, the US, are all moving to increase the application and integration of niche Defence S&T capability into national S&T programs for counter-terrorism and national (or homeland) security. Defence S&T is seen increasingly as a unique, and critical component of the national response, and one that should not be quarantined for Defence needs alone.

Primary insights indicate that there is:

- increasing effort to improve the alignment and consistency of policies and strategies for national (or homeland) security, national science, technology and innovation, and Defence science and technology;
- growing acknowledgement of the critical national role of niche Defence S&T capabilities;
- greater strategic coordination of national security capability management supported by national security S&T providers, including Defence;
- growing recognition of the need to overcome departmental stovepipes, particularly the military/civilian divide;
- growing use of programmatic (or problem-based) approaches to funding, development, management and exploitation of S&T in national security; and
- an increasing focus on cross-Departmental collaboration, information sharing, and the promotion of enduring S&T "communities of practice".

[1] While the term 'homeland security' will be used when referring to US approaches, the term 'national security' should be taken to mean 'security of the nation, its people and its territories'.

Authors

Rick Nunes-Vaz

Counter Terrorism and Security Technology Centre

Dr Rick Nunes-Vaz has a BSc in physics (Imperial College, London) and MSc and PhD in physical oceanography (University of Wales). He also holds postgraduate qualifications in systems engineering (University of South Australia) and tertiary education (University of New South Wales). Rick held post-doctoral (Flinders University), lecturer and senior lecturer (University of New South Wales) positions conducting research in coastal oceanography, producing nearly 50 publications including founding a new multi-disciplinary marine science journal as its first editor, published by Elsevier/Pergamon in 1999. Rick joined the Land Operations Division of DSTO in 2000, supporting enhancement of the methodology of defence experimentation, which included co-authorship of the five-nation (TTCP) Guide for Understanding and Implementing Defense Experimentation (GUIDEx, 2006). In 2005, Rick moved to the new Operations Support group as DSTO's coordinator of support to Defence domestic operations, which was combined with parallel involvement in supporting the Protective Security Coordination Centre (of Attorney-General's Department) in its evaluation of civilian capability through the National Security Exercise program. From mid-2007, as Head of Counter-Terrorism and Security Analysis in DSTO's new Counter-Terrorism & Security Technology Centre, Rick now leads analytical work (for DSTO and the Office of National Security of the Department of the Prime Minister & Cabinet) to inform the strategic development of science and technology for national security.

Leung Chim

Counter Terrorism and Security Technology Centre

Dr Leung H. Chim graduated with a BSc from the University of Sydney in 1989 majoring in Physics. After a brief position at the ANU he moved to the US to study theoretical physics at Rutgers University where he was awarded a PhD in 1995. His research interests were in the areas of conformal field theory and its application to statistical physics. He continued this research work in Australia from 1996 to 1999, as a Research Fellow at Melbourne University and the University of Adelaide. Since joining DSTO in September 1999, he has worked in the areas of airmobile and amphibious operations, Special Operations, and studies supporting AIR 8000, AIR 9000 and JP117. He has experience in the fields of strategic analysis, joint logistics, integrated air defence, defence experimentation and network centric warfare. Leung is currently working in the field of risk analysis for national security.

Contents

Glossary

9/11	11th September 2001 (terrorist attack)
ASD	Assistant Secretary of Defense
ATL	Acquisition, Technology and Logistics
CA	Capability Acquisition
CB	Chemical and Biological
CBDP	Chemical and Biological Defense Program
CBP	Capability Based Planning
CBRN	Chemical, Biological, Radiological and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CCMAT	Canadian Centre for Mine Action Technologies
CCS	Civil Contingencies Secretariat
CEO	Chief Executive Officer
CHNS	Committee on Homeland and National Security
CIA	Central Intelligence Agency
CIH	Central intelligence Hub
CRA	Consolidated Risk Assessment
CREATE	Center for Risk and Economic Analysis of Terrorism Events
CRTI	CBRN Research & Technology Initiative
CSA	Chief Scientific Adviser
CSAC	Chemical Security Analysis Center
CSS	Centre for Security Science
CT	Counter-Terrorism
CTSTC	Counter-Terrorism Science & Technology Centre
CTTC	Counter-Terrorism Technology Centre
CTTSO	Combating Terrorism Technical Support Office
DARPA	Defense Advanced Research Projects Agency
DDR&E	Director of Defense Research and Engineering
DoDR&E (SP)	DoD Research & Engineering Strategic Plan
DEE	Development, Engineering and Evaluation
DERA	Defence Evaluation & Research Agency
DESA	Defence Engineering & Support Agency
DHHS	Department of Health & Human Services
DHS	Department of Homeland Security
DIUS	Department of Innovation, Universities and Skills
DND	Department of National Defence (Canada)

DNDO	Domestic Nuclear Detection Office
DoD	Department of Defense
DoDHD & ASA	DoD Homeland Defense and Americas' Security Affairs
DOE	Department of Energy
DOJ	Department of Justice
DRDC	Defence Research and Development, Canada
DSAC	Defence Scientific Advisory Council
Dstl	Defence Science and Technology Laboratory
DTC	Defence Technology Centre
DTIC	Defence Technology & Innovation Centre
DTRA	Defense Threat Reduction Agency
DTS	Defence Technology Strategy (Canada)
EML	Environmental Measurements Laboratory
EOP	Executive Office of the President
ERAU	Economics & Resource Analysis Unit
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
FTE	Full-time equivalent
FY	Financial year
GDF	Guidance for the Development of the Force
GDP	Goss domestic product
GS	General Schedule
HIPS	Homeland Innovative Prototypical Solutions
HITS	High Impact Technology Solutions
HM	Her Majesty's
HOSDB	Home Office Scientific Development Branch
HS	Homeland security
HSARPA	Homeland Security Advanced Research Projects agency
HSC	Homeland Security Council
HSI	Homeland Security Institute
HSPD	Homeland Security Presidential Directives
IED	Improvised Explosive Devices
IPT	Integrated Product Teams
IRA	Irish Republican Army
JRO-CBRND	Joint Requirements Office – CBRN defense
MEAO	Middle-East area of operations

M&O	Management and Operating
MOD	Ministry of Defence
MoU	Memorandum of Understanding
NBACC	National Biodefense Analysis and Countermeasures Center
NCB	Nuclear, Chemical and Biological
NIAID	National Institute of Allergy and Infectious Diseases
NIH	National Institutes of Health
NIS	National innovation system
NORAD	North American Aerospace Defense Command
NPG	National Preparedness Guidelines
NSC	National Security Council
NSF	National Science Foundation
NSS	National Security Strategy (UK)
NSTC	National Science and Technology Council
OMB	Office of Management and Budget
ONL	Office of National Laboratories
OECD	Organization for Economic Cooperation and Development
OSCT	Office of Security & Counter-Terrorism
OSTP	Office of Science and Technology Policy
PCC	Policy Coordination Committees
PIADC	Plum Island Animal Disease Centre
PSC	Public Safety Canada
PSEPC	Public Safety Emergency Preparedness Canada
PSST	Public security science and technology
PSTP	Public Security Technology Program
QDR	Quadrennial Defense Review
R&D	Research and Development
R&E	Research & Engineering
RDA	Research, development, and acquisition
RDS	Research Development & Statistics group
RDT&E	Research, development, testing and evaluation
RTA	Research, Technology and Analysis
RTD	Research and Technology Development
S&T	Science and Technology
SARS	Severe acute respiratory syndrome
SBDA	Science-Based Departments and Agencies
SCTIP	Security & Counter-Terrorism Innovation Program

SO/LIC & IC	Special Operations and Low-Intensity Conflict and Interdependent Capabilities
SPG	Strategic Planning Guidance
SRG	Science & Research Group
TA	Technology Acceleration
TD	Technology Demonstration
TF	Trading fund
TRL	Technology readiness level
TSL	Transportation Security Laboratory
TSWG	Technical Support Working Group
TTP	Technology Transfer Program
UK	United Kingdom
UKSCTSIS	UK Security & Counter-Terrorism Science & Innovation Strategy
US	United States
USDA	U.S. Department of Agriculture
USNORTHCOM	US Northern Command
USPACOM	US Pacific Command
USSTRATCOM	US Strategic Command
WFO	Work for Others
WoG	Whole-of-Government
WMD	Weapons of Mass Destruction

1. Purpose

Most developed nations hold no higher goal than the protection of their citizens. Australia refers to this responsibility as 'national security' in keeping with the United Kingdom (UK) and others. The United States (US), however, currently draws a distinction between 'homeland security', or protecting the homeland and its people, from 'national security' which refers to (largely) foreign policy initiatives and actions that further American national interest in the global context. These are not the only distinctions between the approaches of our key allies in furthering their strategic security goals.

This paper documents the findings of a critical review of open source literature to compare US, UK and Canadian approaches to the development of national security[1] capability, the mechanisms by which science and technology (S&T) support is harnessed, and the relative roles of Defence and non-Defence S&T providers. The review was undertaken to inform the S&T Companion Review to the Defence White Paper, by contextualising Defence S&T contributions to national security goals outside strict support of Defence objectives. This document describes the (mid-2008) status of S&T input to the national security systems of the US, UK and Canada. Its purpose is to inform attempts to improve Australian arrangements, based on lessons learned overseas, and to help generate a longer-term vision for S&T support to whole-of-nation strategic challenges, such as national security.

2. Context

The scope of issues, problems or 'threats' (in a risk management sense) that need to be addressed using national security systems has evolved significantly in recent years. The events of 9/11 (September 11, 2001) focused the US (and arguably all western nations) on the threat of transnational terrorism. The US Homeland Security Strategy [1], released in 2002, framed the problem entirely in terms of terrorism. Unfortunately, there were other problems that needed to be dealt with – Hurricane Katrina was one example. In 2007 [2] the US re-worked its Homeland Security Strategy to include "*catastrophic natural disasters*" (e.g., Hurricane Katrina) and "*catastrophic accidents*" (e.g. the 2003 power blackouts in north-eastern America).

Canada released its national security policy (Securing an Open Society) in 2004 [3], and defined its scope (after its SARS[2] experiences) more broadly as "*threats that have the potential to undermine the security of the state or society…* [and] *generally require a national response…*". [3, p3] They are listed as: "*terrorism; proliferation of weapons of mass destruction*[3]*; failed and failing states;*

[1] While the term 'homeland security' will be used when referring to US approaches, the term 'national security' should be taken to mean 'security of the nation, its people and its territories'.
[2] Severe acute respiratory syndrome.
[3] WMD

foreign espionage; natural disasters; critical infrastructure vulnerability; organized crime, and pandemics." [3, pp7-8]

The UK released its national security strategy (NSS: Security in an Interdependent World) in 2008 [4]. Its introduction highlights the evolution of strategic security thinking over recent decades, and notes that the balance of power, globalisation, the complex inter-dependence of national and international infrastructures, and the capability of non-state actors to inflict harm, have all changed. The UK strategy explicitly recognises the scope and difficulties involved in managing security, and the need for a whole-of-nation response.

> "*This is the first time the Government has published a single, overarching strategy bringing together the objectives and plans of all departments, agencies and forces involved in protecting our national security... Inside government, we will develop a more integrated approach… We will build on the coalition of public, private and third sectors already involved in counter-terrorism… "*. [4, p4, p8]

The scope of security challenges identified in the UK strategy was: "*terrorism; nuclear and other weapons of mass destruction; transnational organised crime; global instability and conflict, and failed and fragile states; civil emergencies; and state-led threats*". The strategy also noted the existence of "*drivers of insecurity*", namely: "*challenges to the rules-based international system*" (e.g., the slow adaptation of the international security architecture, including the United Nations); "*climate change; competition for energy; poverty, inequality and poor governance; and global trends*" (e.g. just-in-time paradigms, internet commerce, population growth, and the strategic vulnerabilities they present); and the overall complexity and interdependence of international systems [4, chap3].

Australia's approach to its national security concerns is currently being reviewed. In July 2008, the Attorney-General, Robert McClelland, indicated that the "*concept of 'national security' has expanded…and now involves a wide range of issues – and, in turn, a wide range of agencies and activities…* [the] *Government is taking an all-hazards approach to national security*" [5, p1, p4]. More recently on the 4th December 2008, the First National Security Statement [6] was formally announced by the Government. The statement outlined a number of new priorities and initiatives that contribute to "*…an integrated approach based on a clear-sighted view of our long term national security interests."* [6, p1]

Two points can be distilled from these strategic documents. Firstly, key nations recognise the emergence of strategic challenges that threaten national integrity in ways that were previously only possible through overt war. Secondly, there is critical need to develop integrated, all-systems responses to meet these challenges.

In this context, S&T is one of a number of core national capabilities that must be harnessed effectively in order to inform and support the development and operation of national security systems. Defence S&T has grown as a distinct entity in many nations, largely since the Second World War, to service the specific needs of military clients but the distinction between military and national need, just as "*the distinction between 'domestic' and 'foreign' policy* [may now be] *unhelpful*" [4, p8]. The S&T relating to protection from chemical warfare agents, for example, has resided entirely with the defence S&T communities of western nations, but this is no longer exclusively a military need.

This document seeks to explain how the provision of S&T is being re-organised in the US, UK and Canada to meet the emerging needs of national security and, specifically, the contributions and adaptations being asked of defence S&T providers, their relationships with other S&T providers, and approaches to funding.

The various national arrangements are referenced against a common framework which is developed in Section 3. Sections 4 to 6 provide summary descriptions of the UK, Canadian and US approaches. An overview assessment of the international approaches and implications for Australia are developed in Section 7.

3. Assessment Framework

A generic template was developed to represent the core components of national security and related S&T systems, as shown below in Figure 1. It explicitly represents:

a. strategic documents (relating to national security, national S&T, and Defence S&T). These may be supplemented by documents that identify the Defence role in national security, but such documents tend to be poorly articulated;

b. key Government Departments (specifically, those departments responsible for Defence, National Security, Science and Innovation, and other government departments);

c. national capability development / management programs (specifically those for national security and national S&T);

d. S&T providers (including Defence S&T, national security S&T, industry, universities and others); and

e. end-user representatives (for example, police, customs, transport operators etc.).

The extent and quality of links between the components is the focus of the analysis reported here. Many components and their functionalities are common to the various nations; however there are differences in the way they are arranged and interact. While the differences are in part due to history and legacy, they also reflect the individual nation's approach to managing their national security problems.

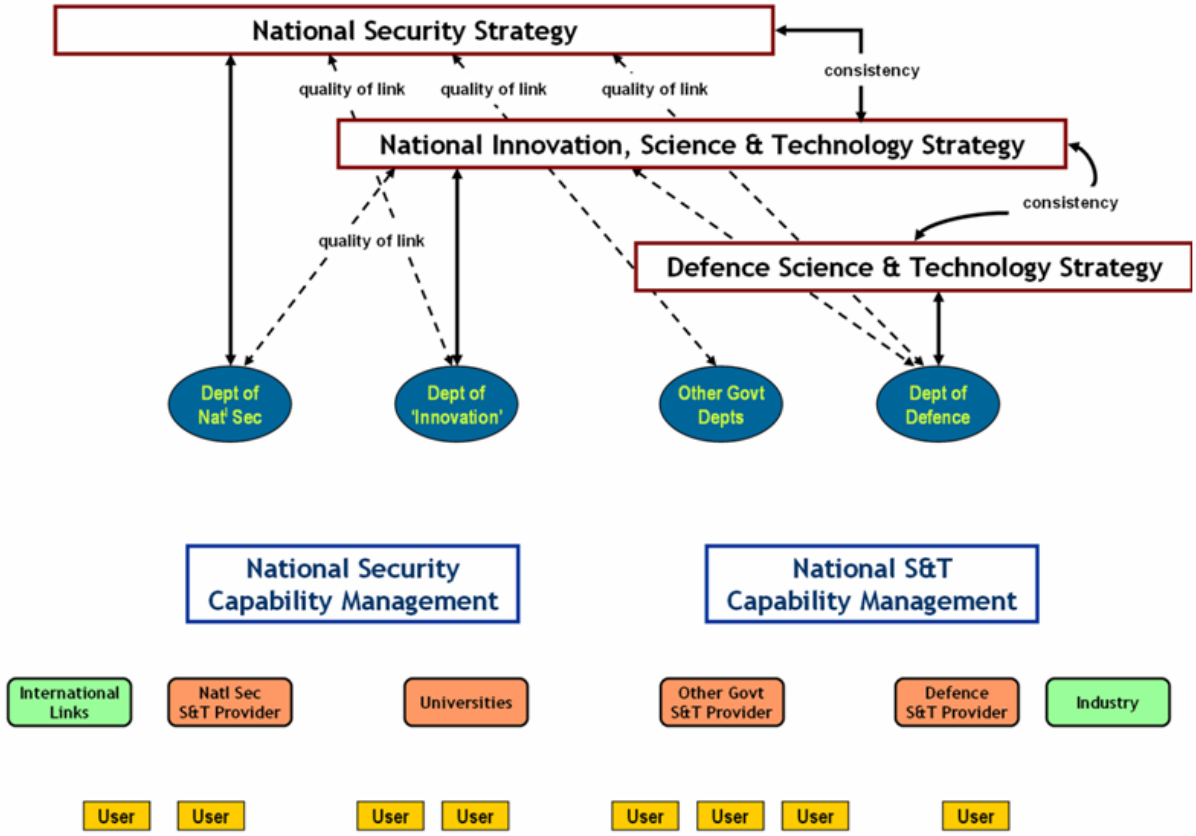

Figure 1: Generic template for S&T support for a WoG approach to national security

In assessing the various national models, common criteria were used to focus the collection and analysis of information. These relate to the manner in which each country:

a. enables and encourages the development of Defence S&T capability and capacity, for use in supporting whole-of Government (WoG) national security objectives outside Defence,

b. provides governance and oversight of Defence S&T support outside Defence,

c. manages and accesses Defence S&T in the context of contributions from all potential providers, in order to support its national security capability management program,

d. encourages and facilitates collaboration between national (Defence, other government, industry and university), and international, S&T providers, and

e. transitions innovative concepts into national capability.

The generic template and assessment criteria draw attention to the key elements of each system and how they interact with each other. They acknowledge that national arrangements are specifically tailored to the security challenges of the host nation, which naturally differ between nations. They also tend to conceal the fact that the US and the UK systems inevitably suffer from degrees of system and sub-system inconsistency, which potentially confuse the

interpretation of broad insights and their utility for Australia. For these reasons, the report provides two levels of analysis. Initially, the national models are described in broad terms followed by general conclusions that attempt to distil core insights. The Appendices that follow provide the more detailed, less interpreted and less paraphrased information on which the insights are based.

4. Summary of UK Model

Just as UK Departmental policies and strategies (e.g. [7-9]) addressing counter-terrorism were developing a degree of consistency, the NSS [4] re-defined the scope of security concerns, adding transnational crime, civil emergencies, climate change and energy security to the mix. The NSS strongly emphasised the need for cross-Departmental coordination, but organisational structures, relationships and arrangements reflect earlier concerns with terrorism and will take some time to adapt, i.e., the 'machinery' lags the rhetoric or national aspirations.

The Home Office has "*primary responsibility for counter-terrorism*" and is, more broadly "*responsible for keeping the UK safe from any threat to… national security*" [10]. Largely through its in-house S&T capabilities [11, 12] it runs the nation's counter-terrorism capability development program. However, this program tends to focus on tactical and operational levels, delivering technologies into the hands of police and first responders. There is no evidence, as yet, that the Home Office appreciates the need for a WoG program developing and managing national security capability and, despite growing its use of Defence S&T to address niche problems [13], there is no sign of Defence being asked to offer its expertise in capability management.

The Cabinet Office, through the Civil Contingencies Secretariat, manages the UK's Resilience program [14]. This program complements the Home Office mandate, developing the tools and information to support the management of 'emergency' risk by communities and businesses.

The UK is working to increase national investment in Research & Development (R&D) from both government and business (above other European countries, to levels equivalent to the US) believing this to be the primary determinant of both national prosperity and relative defence advantage [9, 15-20]. Its strategy with regard to positioning industry (and all potential S&T providers) as key contributors to defence and national security includes making near- and longer-term defence and security requirements and priorities publicly available [9].

Under the banner of counter-terrorism (rather than 'national security'), there is significant consistency between the high-level policies and strategies of the Home Office [12], Cabinet Office [4], Ministry of Defence (MOD) [9], and the Department of Innovation, Universities and Skills (DIUS) [21] in acknowledging the critical role of S&T, and objectives such as ensuring that the nation generates adequate numbers of graduates with required skills. There are several new initiatives, each with new money [22-24], from MOD and non-Defence

Departments (Home Office and DIUS) that acknowledge the pace of emerging strategic problems [25] and the need to stimulate innovation and facilitate rapid transitioning of concepts into capability. All seven national research councils recognise 'global threats to security' as a theme for cross-cutting research funding [21]. All Government Departments are aligned and are consistent in their approaches to innovation and exploitation.

The UK appreciates that the MOD is a critical component of the resources it needs for national security, but it is yet to articulate the role of Defence – this is the subject of an inquiry [26] initiated in April 2008 which is yet to report [27]. At a tactical/operational level, the current Defence/military role in domestic security is similar to Australia's, whereby Defence is requested to assist civilian communities or authorities when civil systems are overwhelmed, but the need for integration of core Defence capability into national systems has not been articulated. Defence S&T is explicitly recognised as a component of Defence support to security objectives and there is growing use of niche MOD S&T capability by the Home Office, in particular CBRN (Chemical, Biological, Radiological and Nuclear), explosives and counter-IED[4] capabilities, and the list is growing. Collaboration and interconnectedness between the Home Office and MOD (e.g. through MOD's Counter-Terrorism Science & Technology Centre (CTSTC) – see below) is intended to increase significantly, for example, through the growth of partnering between Defence and non-Defence S&T in sponsoring research of common value. However, there remain substantial mechanical and cultural divides between Defence (MOD) and non-Defence (Home Office and Cabinet Office), loosely characterised by the concepts of 'home' and 'away' teams. These concepts have, in the past, similarly described the roles of Defence and non-Defence S&T.[5] The NSS has articulated the need for Defence (and Defence S&T) to work much more closely with other parts of the system.

The Secretary of State for Defence is advised on Defence S&T by the Defence Scientific Advisory Council (DSAC). The Defence Technology Strategy [9] details the methodology and criteria that MOD applies to define its S&T priorities. The MOD S&T budget is managed by the Chief Scientific Adviser (CSA). Under the CSA, the Defence Technology & Innovation Centre (DTIC) has the role of taking all MOD requirements and generating a coherent S&T program [29] which it contracts out to all UK S&T providers (including MOD providers which means, primarily, the Defence Science & Technology Laboratory or Dstl). CSA manages an element called 'S&T for Counter-Terrorism & Operational Support' which 'owns' the MOD's CTSTC. The CTSTC (primarily staffed by members of Dstl on secondment) coordinates and manages all MOD counter-terrorism (CT) research activities (as a broker, rather than conducting the research in-house) but it focuses primarily on supporting offshore MOD operations and longer term CT-related issues [13]. The CTSTC has a budget of around £45m,[6] a small component of which supports Home Office objectives.

Dstl is the primary provider of S&T to the MOD [31]. Dstl was set up from the outset, in 2001 as an MOD-owned 'trading fund' (TF) [32, 33] to provide autonomy in its financial decision-making, and some ability to support internal S&T capability development. However, the reality is that all Dstl expenditure to date has required a sponsor [34], and Dstl must seek

[4] Improvised Explosive Devices.
[5] It is now apparent (December 2008) that the links between the Home Office (OSCT) and MOD/Dstl/CTSTC have been strengthened significantly [28].
[6] This was updated to £55-£60m [30].

approval from MOD on its spending intentions. There are currently no routine mechanisms to enable cross-Departmental tasking (e.g., Dstl support to Home Office sponsored research), and no means for Dstl (as the primary Defence S&T provider) to reconcile, even internally, the priorities of civilian requirements against those of MOD. It is estimated that around £30m (approximately 6%) of Dstl's annual budget goes towards meeting national security objectives (requested by the Home Office or CTSTC): this only occurs where there are no conflicts with MOD needs for Dstl's capability and capacity. Dstl has not yet spent any of its profit on unsponsored, capability development to meet its own strategic objectives; rather, it has spent much of its retained profits to date on rationalisation of its physical research sites.

As a new initiative commencing in 2008, the UK is taking its first steps into programmatic, cross-Departmental funding of (specifically) counter-terrorism capability development [35]. The Security & Counter-Terrorism Innovation Program (SCTIP, managed by the Office of Security & Counter-Terrorism (OSCT) under the Home Secretary) has ~£30m to fund project proposals that do not naturally fall within the remit of single Departments. However, the UK shows no sign of fostering the creation of cross-Departmental S&T 'communities of practice' intended to develop and share capability beyond the life of particular projects.

It will take time for the appropriate cross-agency relationships to develop and mature in the UK. Governance, funding and prioritisation mechanisms and processes are yet to be worked through. But on a positive note, at the highest level, and in the UK's newer strategic documents, there is a consistent message that these issues will be resolved.

5. Summary of Canadian Model

Canada's National Security Policy 'Securing an Open Society' was published in 2004 [3], with an update one year later [36]. It defined the scope of national security quite broadly, partly in response to its experiences with SARS, as the need to deal with "*threats that have the potential to undermine the security of the state or society*". Public Safety Canada (PSC, formerly PSEPC[7] including 'emergency preparedness' [37]) is the department responsible for Canada's national security.

Canada has since developed and published [38] many subordinate strategies, including a CBRN Strategy [39], National Strategy for Critical Infrastructure [40], and a National Crime Prevention Strategy [41]. These documents stress the importance of cross-government coordination and integration. They also define the roles and responsibilities of all agencies.

Canada's national appetite for R&D is similar to that of the UK, but the defence fraction of national R&D is substantially smaller than that of the US, UK and Australia [42-45]. Canada's per capita spend on Defence S&T appears to be little more than half that of Australia or the UK. However, Canada's strategic documentation (National Security Policy, sub-Strategies,

[7]Public Safety Emergency Preparedness Canada

Defence S&T Strategy, Industry Canada's Federal S&T Framework [46], DRDC's (Defence Research & Development, Canada) guidance etc.) requires S&T to be developed, managed, exploited and leveraged for national (as well as Departmental) objectives. Canada has adopted the consistent view that S&T is a cross-cutting enabler that should serve Canadian, rather than Departmental interests. This view allows single Department S&T providers (e.g., DRDC) to access funds from other Departments and to grow capability collaboratively and collectively, thereby partially offsetting smaller single-Department resourcing.

While barriers to effective cross-Departmental collaboration do exist [47], and are acknowledged, government is attempting to address these through changes to funding and governance arrangements. Their aim is to develop an effective matrix management system that acknowledges vertical (intra-Department) responsibilities and responsiveness while, at the same time, supporting horizontal (cross-Department) collaboration and sharing (including infrastructure and facilities). Canada has gone significantly further down this road than other Coalition countries, having identified some of the specific impediments (eg, inter-departmental settlement mechanisms), which it is attempting to address. As yet, however, visible discussion has not articulated the methods by which S&T providers might prioritise their own Department's requirements against those of others.

Canada's Defence Management Committee provides strategic oversight of Department of National Defence (DND) development, which is managed at the working level by the Defence Management Oversight Committee [44, 48]. "*The 'Assistant Deputy Minister (S&T)' exercises this functional authority, and is accountable to the Deputy Minister Defence, and the Chief of Defence Staff*" [44, page iv]. The Assistant Deputy Minister (S&T) is also, simultaneously the Chief Executive Officer (CEO) of DRDC.

DND's S&T investment is "*managed through the Defence S&T Enterprise*" [44], representing all of DND's S&T providers, users and stakeholders. "*A charter defines the Defence S&T Enterprise objectives, organizational architecture, relationships among its members and their roles, as well as its governance*" [44, p19]. The DRDC seems to be the only substantial defence-owned S&T provider within the enterprise.

Canadian science and innovation policy is framed in terms of its 'national innovation system' (NIS) [46 & 47]. The Defence S&T Enterprise, including DRDC, is a part of the NIS. The DRDC has policies for accessing external S&T, particularly industry and academia, and leveraging its investments through partnership within the NIS and internationally [48]. The philosophy of external S&T access and leveraging is a strong, consistent message of Defence, other departments and, in fact, all strategic guidance.

DRDC operates through seven research centres and its S&T Program in 2006/07 was costed at C$309m. Around 25% (~C$75m) of this total came from external (non-DND) sources [49]. Of the research centres three have direct contributions to national security, namely the Centre for Security Science (CSS) [50] representing 9% (C$28m) of the budget, the Counter-Terrorism Technology Centre at 1% (C$4m) of the budget, and the Canadian Centre for Mine Action Technologies (CCMAT) at just C$1m of the S&T program budget.

The CSS is a "*joint endeavour*" of PSC [37] and the DND (through DRDC) described under an MoU,[8] but it is "*very much a DRDC organization*" [51]. The CSS is the "*organization through which DRDC provides S&T services to Public Safety Canada*" [50] in order to address national public safety and security objectives.

The CSS has carriage of Canada's strategic public security capability development process and it has been promoting a risk-based 'Capability Based Planning' (CBP) approach to security. Two programs represent the pillars of the approach. These are the CBRN Research & Technology Initiative (CRTI, a "*centrally managed/accountable horizontal S&T program*" of ~C$35m p.a. [52]) which gained approval in 2006 for its second 5-year program [53, 54] and the Public Security Technology Program (PSTP) [55], which was initiated in 2003 although it is currently less mature than CRTI. The CRTI is largely managed by DRDC, in accordance with government mandated responsibility ("*DRDC … coordinates the Government of Canada's CBRN R&D / S&T efforts*" [39]), while the PSTP is managed by PSC.

The CRTI is seen as "*a successful horizontal initiative*" [47, p13] or a means to provide project-based funding to a broad range of S&T providers and collaborators, to meet national objectives beyond the scope of single Departments. Of 26 projects funded to Canada's 21 'Science-Based Departments and Agencies' (SBDA) in FY05-06, DRDC led six, and was a 'federal partner' in another thirteen. Under CSS arrangements, the CRTI explicitly [54] spreads its project funding across different technology readiness level (TRL) ranges: TRL three to five received 55% of all CRTI funding from 2002 to 2006, levels five to seven received 5% and levels seven to nine received 20%. There is also explicit provision for projects to progress to higher TRL funding stages in later competitive rounds of funding allocation.

The CRTI (and other horizontal programs) have, nevertheless, been criticised because their "*time limited funding … has the disadvantage in a strategic sense of being narrowly targeted with short (3-4 year) timelines which are not always compatible with the research priority being addressed. The lack of core funding means that agency scientists pursue short term … goals but this piece meal approach makes it difficult in the longer term to address strategic research priorities*" [47, p42]. Note, however, that these criticisms appeared in the government's initiative to identify and overcome such problems.

In order to facilitate effective and efficient horizontal S&T collaboration, Canada has promoted and supported the concept of 'science clusters' [56], or arrangements that promote dialogue and discussion in the federal S&T community. These are enduring communities that come together in different ways (with regard to leadership and supporting roles) to meet the needs of particular projects. Canada's CRTI program has generated five enduring clusters (chemical, biological, radiological/nuclear, forensics and explosives) involving 177 member agencies in total.

[8] Memorandum of Understanding.

6. Summary of US Model

The US makes a distinction between 'homeland security' and 'national security'. Homeland security (HS) is described [2, p1] as "*protecting and defending the Homeland*" and involves "*preventing and disrupting terrorist attacks; protecting the American people… critical infrastructure, and key resources; and responding to and recovering from incidents that do occur….*" National security [57] relates to management of issues beyond American shores: it "*seeks and supports democratic movements and institutions in every nation and culture, with the ultimate goal of ending tyranny in our world… [and] extend freedom across the globe… Championing freedom advances our interests because the survival of liberty at home increasingly depends on the success of liberty abroad…*" [57, p1]

The White House Administration's approach to homeland security is based on the principles of shared responsibility and partnership with the Congress, state, local and tribal governments, the private sector, the American people and international partners [58].

Funding of US R&D for homeland security was always large, but it grew substantially after 9/11. There currently does not appear to be a formal approach to balancing the budget allocations of federal Departments under broad programs such as homeland security; budget allocations are determined by piecewise consideration of each Department's objectives and arguments. Nevertheless, in the 2007 National Strategy for Homeland Security, a new homeland security management system was proposed as a comprehensive approach that incorporates all stakeholders [2] and sets guidance for the development of capability.

There is no US national S&T strategy: the Department of Homeland Security (DHS) and the Department of Defense (DoD) have developed their own S&T strategies and visions ([59] and [60] respectively). Formally, the DHS is responsible for leading all homeland security programs, except those related to 'homeland defense' (which are run by DoD [61]). The Under Secretary of the DHS S&T Directorate is responsible for coordinating national R&D / S&T activity for homeland security, across all relevant agencies [62]. There are many R&D providers across Government Departments and Agencies contributing to homeland security capability, but their work tends to be "*mission oriented*", serving the goals and objectives of the agency providing the funds [63]. Difficulties of coordination are further exacerbated by federal budget R&D allocations: of US$5.5bn allocated in the 2009FY federal homeland security R&D budget, the DHS receives only US$1bn (i.e., less than 20%). This compares with allocations to the Department of Health & Human Services (DHHS) of US$2.1bn, and the DoD, of US$1.5bn. There is a tangible mismatch between the formal DHS national coordination role, and the resourcing of homeland security R&D.

The Homeland Security Council (HSC) within the White House oversees all homeland security-related activities and policies among executive departments and agencies. Additional mechanisms such as the National Science and Technology Council (NSTC) and its Committee on Homeland and National Security (CHNS), and the Technical Support Working Group (TSWG), are intended to promote interagency coordination of R&D policies and plans. However, the lack of effective inter-agency coordination is acknowledged, as is the need for collaborative programs, technology leveraging and information sharing, but there are no

defined collaborative research groupings or communities that cut across Departments/agencies in homeland security. The current proposal is to use the CHNS and the Quadrennial Homeland Security Review process to facilitate coordination[9] [64, 65].

In general, DoD S&T agencies work on Defense issues and are explicitly prohibited from conducting R&D and developing capability exclusively for first responder use [66]. However the DoD does develop dual-use technologies which may be made available to other agencies through the so-called '1401 technology transfer program' (TTP) [66]. Under this program DoD can enter into a cooperative R&D agreement with DHS and other Federal agencies, State or local agencies, non-government organizations, and private sector enterprises to pursue specific projects, provided there is benefit to DoD. Similarly, the DHS in some instances can share laboratory resources with other agencies (e.g., DoD); and can conduct testing for others provided the work contributes to homeland security [62].

The DoD allocates its homeland security R&D funds (US$1.5bn in FY2009) primarily to agencies such as the Defense Threat Reduction Agency (DTRA) and the Chemical and Biological Defense Program (CBDP) [63]. Broad guidance is given by the DoD Research & Engineering (R&E) Strategic Plan [67], identifying the principles, capabilities, and technologies that should be applied in allocating DoD R&D funds (totalling US$80.7bn in FY2009). Much of the total R&D spend goes to universities (for basic research), DoD laboratories and agencies, federally funded facilities, and industry.

The US federal government recognises the importance of innovation and has implemented several policies in this regard. The Director of Innovation within the DHS S&T Directorate sponsors research to promote innovation through several programs, including Homeland Innovative Prototypical Solutions (HIPS) and High Impact Technology Solutions (HITS). The DoD's Defense Advanced Research Projects Agency (DARPA) has a unique mission to develop radical innovation for national (rather than homeland) security.

7. International Comparison

It is clear from the analysis that, particularly Canada and the UK, and from a low base, the US, are moving to increase the application and integration of niche Defence S&T capability into national S&T programs for counter-terrorism and national (or homeland) security. Defence S&T is seen increasingly as a unique, and critical component of the national response, and one that should not be quarantined for Defence needs alone.

Comparisons highlighted the following trends and insights. There is:

a. a temporal shift towards greater alignment and consistency between policies and strategies for (a) national (or homeland) security, (b) national innovation, S&T, and (c) Defence S&T,

[9] A proposal by Under Secretary DHS S&T Jay Cohen and discussed at a recent (April 2008) hearing on "The Future of Science and Technology at the Department of Homeland Security" [64].

b. a growing acknowledgement of the critical national role of niche Defence S&T capabilities,

c. greater strategic coordination of national security capability management supported by national security S&T providers, including Defence,

d. growing importance attached to overcoming departmental stovepipes, particularly the military/civilian divide,

e. growing use of programmatic (or problem-based) approaches to funding, development, management and exploitation of S&T in national security, and

f. an increasing focus on cross-Departmental collaboration, information sharing, and the promotion of enduring S&T 'communities of practice'.

To further inform this discussion it is useful to collect the information under five categories that relate to the manner in which each country:

a. enables and encourages the development of Defence S&T capability and capacity, for use in supporting WoG national security objectives outside Defence,

b. provides governance and oversight of Defence S&T support outside Defence,

c. manages and accesses Defence S&T in the context of contributions from all potential providers, in order to support its national security capability management program,

d. encourages and facilitates collaboration between national (Defence, other government, industry and university), and international, S&T providers, and

e. transitions innovative concepts into national capability.

The manner in which each country enables and encourages the development of Defence S&T capability and capacity, for use in supporting WoG national security objectives outside Defence.

a. The U.S. has not coordinated federal development of S&T capability across agencies other than via White House committees. While the DoD has allocated US$1.5bn for 'homeland defense' R&D in FY09, mostly to the DTRA and the CBDP, this is intended to meet DoD's homeland defense and civil support objectives. In general the DoD is prohibited from developing capability for first responder use, but it does intentionally develop 'dual-use' capability that may be transferred [66].

b. Formerly, the MOD accessed S&T principally from its own providers. MOD (and other Departments) is now moving towards a cross-Departmental, programmatic approach. The 2007 'UK Security & Counter-Terrorism Science & Innovation Strategy' (UKSCTSIS) [12] underpins MOD involvement in national S&T initiatives and, in 2008, the UK created a "*cross-departmental Security & Counter-Terrorism Science & Innovation Program*" [35] funded to £30m p.a., to which MOD-owned S&T is a key contributor. The Home Office has accessed Dstl's Forensic Explosives Laboratory for some years now (contributing approximately 6% of Dstl's total budget). MOD's relatively new

CTSTC is developing its partnerships with the Home Office and other Departments to address issues (e.g., counter-IED) in a nationally coherent way.

c. Canada's (2004) National Security Policy [3] talks of an "*integrated security system*", and it explicitly manages S&T at the Federal level, mandating (and creating the regulatory mechanisms to facilitate) cross-Departmental provision of S&T support. Defence is a key contributor in this process; "*the Defence S&T Enterprise plays a proactive role in contributing to the public security S&T agenda*" [68], and DRDC (Defence's primary S&T provider) both manages[10] and contributes to national security S&T provision and S&T capability development through its CSS. National arrangements allow and encourage DRDC to take a lead in areas of national security S&T where it deems it appropriate to do so.

d. **Insights.** In earlier days, the defence relationship with its science and technology capabilities was one of exclusive ownership justified by the unique and highly specialised character of defence needs. However, as the "*classical distinctions between foreign and domestic, national and international, internal and external have become blurred*" [6], the line between defence and non-defence S&T needs has also faded in common areas of concern, such as detection of improvised explosive devices, protection of aircraft from shoulder-launched missiles, and effective 'command and control' of response elements during major incidents. This is anticipated to be a continuing trend which implies that exclusive exploitation of defence S&T will become increasingly untenable.

The manner in which each country provides governance and oversight of Defence S&T support outside Defence.

a. The White House HSC coordinates homeland security-related activities and policies across executive departments and agencies, charging the DHS with responsibility to lead the civilian effort, and the DoD to direct the military effort. The CHNS, co-chaired by DoD and DHS, is charged with improving the coordination of all Federal efforts in homeland and national security R&D and *to "promote interagency policy coordination, foster collaboration, and develop Federal technology activities"* [69, p1]. The DHS Under Secretary for S&T is required to coordinate with other executive agencies to reduce R&D duplication and identify unmet needs [62].

b. The UK is moving towards greater cross-Departmental coordination and management in dealing with what it terms 'strategic challenges'. MOD's CSA administers the Defence S&T Program, and is simultaneously MOD's primary stakeholder in the 'cross-departmental Security & Counter-Terrorism Science & Innovation Program', the CTSTC's non-Defence collaborations, and Dstl's work for the Home Office. The CTSTC's relationships with non-Defence agencies are still small but growing. Although the CTSTC and Dstl acknowledge the importance of their non-Defence engagement, they are yet to develop the mechanisms to reconcile the relative priorities of Defence and non-Defence work.

[10] With PSC

c. In Canada, Defence S&T has specific national responsibility. The DRDC "*coordinates the Government's CBRN R&D/S&T efforts*" [39]. The CEO of DRDC is simultaneously the Assistant Deputy Minister (S&T) with functional authority for delivery of the Defence R&D Program, and the Chair of the Multi-Departmental Steering Committee that governs the national security CRTI Program. The CSS (>C$25m of DRDC's annual budget) manages national security development funding programs. DRDC is itself a recipient of CRTI funds which it uses to develop capability, synergistically with respect to its Defence Program. Of the 26 CRTI projects funded in FY04/05, DRDC led six and participated in another thirteen.

d. **Insights**. The need to support non-defence exploitation of defence S&T has required the creation of mechanisms to provide appropriate governance. Each nation is tackling this in a different way, but the creation of 'interface' agencies (such as the UK's CTSTC or Canada's CSS) that broker access to national S&T capabilities including those of defence, is an emerging trend. All nations acknowledge the need to improve coordination and support activity that has national benefit, but the greatest stumbling block, yet to be resolved effectively by any nation, is how to reconcile both the owner's and the nation's priorities and clarify the tasking of S&T capabilities where potential conflicts arise.

The manner in which each country manages and accesses Defence S&T in the context of contributions from all potential providers, in order to support its national security capability management program.

a. The 2007 US National Strategy for Homeland Security [2] introduced a comprehensive Homeland Security Management System that incorporates all stakeholders and is intended to guide the development of capability. At the level of the White House, the NSTC and the TSWG oversee interagency coordination of R&D policies and plans. Below this level, however, Defense / non-Defense collaboration is "*ad hoc, without comprehensive engagement and with fragmented accountability*" [70, p1]. In general DoD participates when it is beneficial to Defense, but it can enter into cooperative R&D agreements with DHS and other Federal agencies to pursue specific projects under the 1401 TTP [66].

b. The UK is moving to break the distinctions, but is still largely divided by the concepts of the 'home' (Home & Cabinet Offices) and 'away' (MOD) games. The Home Office is the primary Department responsible for national security and has formerly relied almost solely on its in-house S&T capability. Relationships with Dstl and the CTSTC are growing but are not yet large components of national security S&T provision.

c. Canada's (DRDC's) CSS has developed a national security capability management program, to which the CRTI and Public Safety Technical Program contribute. DRDC plays a central role in both managing the funding of S&T provision, and in partnering with other non-Defence agencies in providing S&T support to meet national objectives.

d. **Insights**. All relevant literature acknowledges both the pace of global change and the need to address emerging and escalating threats. In this context, the need for S&T capability development is also growing, but there is an increasing tension between

'ownership' and use. A coordinated national approach to S&T capability development under a model that identifies appropriate S&T lead agencies while at the same time supporting and encouraging broad access is clearly needed.

The manner in which each country encourages and facilitates collaboration between national (Defence, other government, industry and university), and international, S&T providers

a. The U.S. DoD is currently developing its longer term S&T priorities and goals in concert with other departments [71]. There are also signs that the US sees value in improving cross-Departmental coordination of research. A recent Defence Science Board task force recommended "*that coordination and integration between the* [DoD and DHS] *departments be institutionalised through a formal Memorandum of Understanding (MOU) with a scope that includes planning, research and development, acquisition, operations, and training"* [70, p2].

b. The UK Defence Technology Strategy expresses MOD's intentions to access and support all potential providers of S&T. Since 2001, MOD has shifted from a model in which almost all S&T was provided in-house, to one in which 60% of S&T funds are competitively allocated. The CTSTC similarly acts a broker for R&D, working with the Home Office to access support on problems of common interest. There is significant convergence in the strategies and approaches of the MOD, the Home and Cabinet Offices, and the DIUS, in creating a fertile S&T environment to serve national needs. National Research Councils have recently initiated a 3-year, £113m funding program called 'Global Threats to Security' which strongly aligns with MOD's 2006 Defence S&T Strategy.

c. Canada's 'Framework for Federal Science & Technology' [46] "*sets out the Government of Canada's continuing commitment to effectively conduct and manage science and technology (S&T) in support of action on issues of concern to Canadians…* [It] *applies to* <u>*all*</u> *federal departments and agencies…* [and aims] *to bring an integrated government-wide approach to S&T*". The DND S&T Strategy is entirely consistent with the Federal Framework. Canada groups Government S&T providers with industry, academic and community providers under its NIS. The extent to which its policies have generated collaboration is demonstrated in the large number and mix of partnerships in CRTI-funded national security projects. Canada has also moved to identify and resolve structural impediments to inter-Departmental work and transfer of funds.

d. **Insights**. In line with the increasing interaction between S&T providers, there is a commensurate need for new mechanisms to support and enhance collaboration. This is partially achieved through a combination of government (and relevant Departmental) policy, and funding initiatives that promote inter-agency development, but must be supplemented by programs that weaken stovepipes and related cultures.

The manner in which each country transitions innovative concepts into national capability

a. Since 2007 the US DHS S&T Directorate has established new mechanisms specifically to improve this process. DHS uses the concept of Integrated Product Teams (IPT) to identify requirements and its Director of Product Transitions is required to deliver low risk projects within three years [59]. DoD has partnered DHS in the development and transition of specific technologies under the 1401 TTP [66].

b. While there is strategic alignment across all UK Departments on the need for, and mechanisms to, stimulate innovation, the MOD and Home Office largely manage the development of capability independently for Defence and national security purposes, respectively. As discussed above, there is collaboration on issues such as counter-IED, but the Home Office has traditionally managed, through in-house S&T, the provision of equipment etc. into the first responder community. There has been comment (e.g. [72]) on the lack of coordinated, strategic management of the UK national security 'architecture', and the recent (2008) UK NSS addresses this point, but current systems and methods do not yet reflect aspirations.

c. Canada's CSS leverages DRDC knowledge and experience of Defence capability development, in its management and development of national security capability. Funding of R&D under CSS programs is purposefully balanced across the spectrum (1-9) of the TRLs, and individual projects may receive funding in successive years but are expected to progress in TRL. The balance of funding under the first 5 years of the CRTI Program was 68% to TRLs 3-5, 6% to TRLs 5-7, and 25% to TRLs 7-9.

d. Insights. This is another area in which there is acknowledged need for improvement but no clear mechanisms to achieve desired results. A national model for the development of capability (and S&T capability) is envisaged but this is yet to take form in any of the nations studied.

Appendices A, B and C provide the detailed information relating to each country's approach to national security S&T funding and prioritisation, upon which these summaries were based.

8. Acknowledgements

We wish to thank our colleagues Mr Neil Bryans, Dr John Percival and Dr Jolanta Ciuk for their support, useful discussions and comments on the work. We would also like to acknowledge feedback from Dr Lynn Booth and other members of the Defence White Paper S&T Companion Review team.

9. References

1. Office of Homeland Security. *National Strategy for Homeland Security*. July, 2002 [cited 2008; Available from: http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf]
2. Homeland Security Council. *National Strategy for Homeland Security*. October, 2007 [cited 2008; Available from: http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf]
3. Canada Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. April, 2004 [cited 2008; Available from: http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat_e.pdf]
4. UK Cabinet Office. *The National Security Strategy of the United Kingdom: Security in an Interdependent World*. March, 2008 [cited 2008; Available from: http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf]
5. McClelland, R. *Address to the Safeguarding Australia Conference*. 23 July, 2008 [cited 2008; Available from: http://www.safeguardingaustraliasummit.org.au/2008/files/SA08_Attorney_Generals_Speech_Opening.pdf]
6. Rudd, K. *The First National Security Statement to the Parliament: Address by the Prime Minister of Australia*. December, 2008 [cited 2008; Available from: http://www.pm.gov.au/media/Speech/2008/speech_0659.cfm]
7. CONTEST. *Countering International Terrorism: The United Kingdom's Strategy*. July, 2006 [cited 2008; Available from: http://www.fco.gov.uk/resources/en/pdf/contest-report]
8. HM Government. *Confident Communities in a Secure Britain - the Home Office Strategic Plan 2004-2008*. July, 2004 [cited 2008; Available from: http://www.crimereduction.homeoffice.gov.uk/publications10.htm]
9. MOD. *Defence Technology Strategy for the demands of the 21st Century*. 2006 [cited 2008; Available from: http://www.ndi.org.uk/NDILtd/Library0.nsf/ab283684d03f231d80256b520047d321/FDEABDFF5C3EE683802572190038D5F9/$file/Defence%20Technology%20Strategy.pdf]
10. UK Home Office website. [cited 2008; Available from: http://www.homeoffice.gov.uk/security/]
11. UK Home Office. *UK Home Office Science & Innovation Strategy (2005-2008)*. 2005 [cited 2008; Available from: http://www.homeoffice.gov.uk/documents/science-strategy.pdf/]
12. UK CT Unit. *The United Kingdom Security & Counter-Terrorism Science & Innovation Strategy*. 2007 [cited 2008; Available from: http://security.homeoffice.gov.uk/news-publications/publication-search/general/science-innovation-strategy1?view=Binary]

13. Thompson, P., *Personal communication, UK MOD Counter-Terrorism Science & Technology Centre*. February, 2008.

14. The UK Government. *UK Resilience website*. [cited 2008; Available from: http://www.ukresilience.gov.uk/]

15. HM Treasury. *Science & Innovation Investment Framework 2004-2014*. 2004 [cited 2008; Available from: http://news.bbc.co.uk/nol/shared/bsp/hi/pdfs/science_innovation_120704.pdf]

16. HM Treasury. *Budget 2008*. 2008 [cited 2008; Available from: http://www.hm-treasury.gov.uk/bud_bud08_index.htm]

17. MOD. *Maximising Benefit from Defence Research*. October, 2006 [cited 2008; Available from: http://www.science.mod.uk/Strategy/documents/max_benefit_DefResearch_UNC.pdf]

18. MOD. *Maximising Defence Capability Through R&D*. October, 2007 [cited 2008; Available from: http://www.science.mod.uk/Strategy/documents/max_def_cap_thru_randd.pdf]

19. MOD. *Science, Innovation, Technology Research Program, 2007/08*. 2007 [cited 2008; Available from: http://www.science.mod.uk/Strategy/strategy.aspx]

20. Council for Science & Technology. *Strategic Decision Making for Technology Policy*. 2007 [cited 2008; Available from: http://www2.cst.gov.uk/cst/reports/files/strategic-decision-making.pdf]

21. DIUS. *The Allocations of the Science Budget*. 2007 [cited 2008; Available from: http://www.dius.gov.uk/publications/sciencebudget.html]

22. MOD. *Grand Challenge science and technology competition*. [cited 2008; Available from: http://www.science.mod.uk/Engagement/Grand_Challenge/grand_challenge.aspx]

23. MOD. *Defence Research Suppliers Information Portal*. [cited 2008; Available from: http://www.ideas.mod.uk/]

24. MOD. *Grand Challenge announcement*. July, 2007 [cited 2008; Available from: http://www.mod.uk/DefenceInternet/DefenceNews/EquipmentAndLogistics/ChallengeIsOnToFindBritainsBestTechnologyInnovatorsvideo.htm]

25. Strategy Unit Cabinet Office. *Realising Britain's Potential: Future Strategic Challenges for Britain*. 2008 [cited 2008; Available from: http://www.cabinetoffice.gov.uk/strategy/work_areas/strategic_challenges0208.aspx]

26. UK Parliament. *Defence Committee inquiry into UK national security and resilience*. April, 2008 [cited 2008; Available from: http://www.parliament.uk/parliamentary_committees/defence_committee/def080402___no__37.cfm]

27. Committee, D. *Defence Committee inquiry into UK national security and resilience*. April, 2008 [cited 2008; Available from: http://www.parliament.uk/parliamentary_committees/defence_committee/def080402___no__37.cfm]

28. Neill, M., *Personal communication*. December, 2008.

29. House of Commons. *The work of the Defence Science & Technology Laboratory, and the funding of defence research*. February, 2007 [cited 2008; Available from: http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmdfence/512/512.pdf]

30. Thompson, P., *Personal communication*. December, 2008.

31. House of Commons. *Defence - Written Evidence*. 2007 [cited 2008; Available from: http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmdfence/84/84we01.htm]

32. Newbery, D., L. Bently, and R. Pollock. *Models of Public Sector Information Provision via Trading Funds*. February, 2008 [cited 2008; Available from: www.opsi.gov.uk/advice/poi/models-psi-via-trading-funds.pdf]

33. HM Treasury. *Guide to the Establishment and Operation of Trading Funds*. 2006 [cited 2008; Available from: www.hm-treasury.gov.uk/d/Guide_to_the_Establishment_and_Operation_of_Trading_Funds.pdf]

34. Dstl, *personal communication*. 2008.

35. Szabo, A., *CONDS London personal communication*. 2007.

36. Canada Privy Council Office. *Securing an Open Society - One Year Later - Progress Report on the Implementation of Canada's National Security Policy*. May, 2005 [cited 2008; Available from: http://www.pco-bcp.gc.ca/docs/information/Publications/secure/secure_e.pdf]

37. Public Safety Canada. *PSC website*. [cited 2008; Available from: http://www.publicsafety.gc.ca/index-en.asp]

38. PSC. *PSC policies and legislation*. [cited 2008; Available from: http://www.publicsafety.gc.ca/pol/index-eng.aspx]

39. PSC. *The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada*. 2005 [cited 2008; Available from: http://www.publicsafety.gc.ca/pol/em/fl/strat_e.pdf]

40. PSC. *National Strategy for Critical Infrastructure*. 2005 [cited 2008; Available from: http://www.publicsafety.gc.ca/prg/em/cip-eng.aspx]

41. PSC. *National Crime Prevention Strategy*. [cited 2008; Available from: http://www.publicsafety.gc.ca/prg/cp/ncps-eng.aspx]

42. Acharya, L. *Research & Development in Canada: Federal Expenditures and Policies.* December, 2002 [cited 2008; Available from: http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/PRB-e/PRB0247-e.pdf]

43. Statistics Canada. *Federal scientific activities 2002-2003*. May, 2003 [cited 2008; Available from: http://www.statcan.gc.ca/pub/88-204-x/88-204-x2003000-eng.pdf]

44. Canadian Defence. *Defence S&T Strategy: Science and Technology for a Secure Canada*. December, 2006 [cited 2008; Available from: http://www.drdc-rddc.gc.ca/ststrategy/ststrategy_e.pdf]

45. Government of Canada. *Mobilizing Science & Technology to Canada's Advantage*. 2007 [cited 2008; Available from: http://www.ic.gc.ca/epic/site/ic1.nsf/en/h_00856e.html]

46. Government of Canada. *Canada's Innovation Strategy*. February, 2002 [cited 2008; Available from: http://www.collectionscanada.gc.ca/webarchives/20071115003345/ http://www.innovation.gc.ca/gol/innovation/site.nsf/en/in04113.html]

47. Government of Canada. *Overcoming Barriers to S&T Collaboration: Steps Towards Greater Integration.* March, 2006 [cited 2008; Available from: http://www.brp-gde.ca/en/submissionGet.cfm?submission_id=43]

48. Defence Research and Development Canada. *New Challenges, New Opportunities: DRDC Annual Report.* March, 2007 [cited 2008; Available from: http://www.drdc-rddc.gc.ca/publications/annual/annualreport_e.asp]

49. Canada News Centre. *Government of Canada Invests Over $30 Million for Science and Technology Projects to Enhance Canada's Security and Safety*. February, 2008 [cited 2008; Available from: http://news.gc.ca/web/view/en/index.jsp?articleid=381279]

50. DRDC. *Centre for Security Science*. [cited 2008; Available from: http://www.css.drdc-rddc.gc.ca/index-eng.asp]

51. Williams, M., *Direct communication with Deputy Director General, DRDC CSS*. 2008.

52. DRDC. *CRTI website*. [cited 2008; Available from: http://www.css.drdc-rddc.gc.ca/crti/index-eng.asp]

53. DRDC. *CRTI Annual Report Part 1: Delivering Capabilities*. 2005 [cited 2008; Available from: http://www.css.drdc-rddc.gc.ca/crti/publications/reports-rapports/ar04_05_pt1-eng.pdf]

54. DRDC. *Evaluating Results: CRTI Annual Report 2005-2006*. 2006 [cited 2008; Available from: http://www.css.drdc-rddc.gc.ca/crti/publications/reports-rapports/ar05_06_pt1-eng.pdf]

55. DRDC. *Public Security Technical Program website*. [cited 2008; Available from: http://www.css.drdc-rddc.gc.ca/pstp/index-eng.asp]

56. DRDC. *Science Clusters website*. [cited 2008; Available from: http://www.css.drdc-rddc.gc.ca/crti/clusters-grappes/index-eng.asp]

57. Department of Defense, *The National Security Strategy of the United States of America.* March 2006.

58. The White House, *Homeland Security Presidential Directive-1* 2001.

59. DHS S&T Directorate. *Science and Technology for a Safer Nation ….* March, 2008 [cited 2008; Available from: http://www.dhs.gov/xlibrary/assets/st_safer_nation.pdf]

60. Director of Defense Research and Engineering Department of Defense *Department of Defense Research and Engineering Strategic Plan*. 2007 [cited; Available from: http://www.dod.mil/ddre/doc/Strategic_Plan_Final.pdf]

61. Department of Defense. *Strategy for Homeland Defense and Civil Support*. June, 2005 [cited; Available from: http://www.defenselink.mil/news/Jun2005/d20050630homeland.pdf]

62. Shea, D. and D. Morgan. *The DHS Directorate of Science and Technology: Key Issues for Congress*. CRS Report for Congress. February, 2008 [cited 2008; Available from: http://www.fas.org/sgp/crs/homesec/RL34356.pdf]

63. American Association for the Advancement of Science. *Research and Development FY 2009, AAAS Report XXXIII*. 2008 [cited; Available from: http://www.aaas.org/spp/rd/rd09main.htm]

64. Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. Hearing on *the Future of Science and Technology at the Department of Homeland Security*. April, 2008 [cited 2008; Available from: http://homeland.house.gov/Hearings/index.asp?ID=123]

65. Shea, D.A., J.D. Moteff, and D. Morgan. *Comments on Coordination of Homeland Security Science and Technology*. CRS memorandum to House Committee on Homeland Security. March, 2008 [cited 2008; Available from: http://homeland.house.gov/SiteDocuments/20080401143529-46747.pdf]

66. OASD for Homeland Defense and America's Security Affairs. *1401 Technology Transfer Program FAQ*. Office of the Under Secretary of Defence for Policy website [cited 2008; Available from: http://www.defenselink.mil/policy/sections/policy_offices/hd/faqs/techTransfer/index.html]

67. The DoD DDR&E. *Department of Defense Research and Engineering Strategic Plan*. 2007 [cited 2008; Available from: http://www.dod.mil/ddre/doc/Strategic_Plan_Final.pdf]

68. Department of National Defence. *Defence S&T Strategy: Science and Technology for a Secure Canada*. December, 2006 [cited 2008; Available from: http://www.drdc-rddc.gc.ca/ststrategy/ststrategy_e.pdf]

69. National Science and Technology Council. *Charter of the Committee on Homeland and National Security*. May, 2006 [cited 2008; Available from: http://www.ostp.gov/galleries/NSTC/CHNS%20Charter%20signed%205-30-06.pdf]

70. Office of the Under Secretary of Defense for Acquisition, T., and Logistics,. *Report of the Defense Science Board Task Force on Critical Homeland Infrastructure Protection*. January, 2007 [cited 2008; Available from: http://www.acq.osd.mil/dsb/reports/2007-01-Critical_Homeland_Infrastructure_Protection.pdf]

71. DHS S&T Directorate. *Coordination of Homeland Security Science and Technology*. December, 2007 (revised January 2008) [cited 2008; Available from: http://homeland.house.gov/SiteDocuments/20080401143438-63338.pdf]

72. Edwards, C. *National Security for the Twenty-first Century*. December, 2007 [cited 2008; Available from: http://www.demos.co.uk/files/National%20Security%20web.pdf]

73. UK National Audit Office. *MOD: The Management of Defence Research & Technology: HC 360 Session 2003-2004*. March, 2004 [cited 2008; Available from: http://www.nao.org.uk/publications/nao_reports/03-04/0304360.pdf]

74. Neill, M., *MOD personal communication*. 2007.

75. MOD. *DTC website*. [cited 2008; Available from: http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/ScienceandTechnology/DTC/]

76. House of Commons. *The work of the Defence Science and Technology Laboratory and the funding of defence research: Government Response to the Committee's Eighth Report of Session 2006–07*. May, 2007 [cited 2008; Available from: http://www.publications.parliament.uk/pa/cm200607/cmselect/cmdfence/512/512.pdf]

77. Ministry of Defence. *Memorandum from the Ministry of Defence: The Defence Science and Technology Laboratory*. September, 2006 [cited 2008; Available from: http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmdfence/84/84we02.htm]

78. Ministry of Defence. *Second memorandum from the Ministry of Defence: Counter Terrorism*. September, 2006 [cited 2008; Available from: http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmdfence/84/84we03.htm]

79. Ministry of Defence. *Supplementary memorandum from the Ministry of Defence*. January, 2007 [cited 2008; Available from: http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmdfence/84/84we04.htm]

80. Sharp, L., *Dstl Chief of Division personal communication*. 2008.

81. MOD. *The Defence Support Group Trading Fund Order 2008*. April, 2008 [cited 2008; Available from: http://www.opsi.gov.uk/si/si2008/uksi_20080563_en_1]

82. Ploughshare Innovations. *Ploughshare Innovations website*. [cited 2008; Available from: http://www.ploughshareinnovations.com/]

83. MOD. *The MOD Counter Terrorism Science & Technology Centre website*. [cited 2008; Available from: http://www.ctcentre.mod.uk/index.php]

84. Cabinet Office. *Civil Contingencies Secretariat website*. [cited 2008; Available from: http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx]

85. UK Home Office. *Office for Security and Counter Terrorism website*. [cited 2008; Available from: http://security.homeoffice.gov.uk/]

86. Szabo, A., *CONDS London personal communication*. 2008.

87. HM Treasury. *Sainsbury Review of Science and Innovation* October, 2007 [cited 2008; Available from: http://www.hm-treasury.gov.uk/sainsbury_review_index.htm]

88. DRDC. *Technology Acquisition Projects: Strengthening Operational Capacity 2002-2005*. 2005 [cited 2008; Available from: http://www.css.drdc-rddc.gc.ca/crti/invest/acquisition/tech_acquisitions02_05-eng.pdf]

89. Chief Review Services. *CRTI Formative Evaluation*. August, 2006 [cited 2008; Available from: http://www.forces.gc.ca/crs/pdfs/crti_eval_e.pdf]

90. Chouinard, P., *CSS personal communication*. 2008.

91. DRDC. *Risk Portfolio website*. [cited 2008; Available from: http://www.css.drdc-rddc.gc.ca/pstp/priorities-priorites/risk-risques-eng.asp]

92. Chouinard, P. *Capability Based Planning within Canadian Public Security*.

93. Department of Defense. *The National Defense Strategy of the United States of America*. March, 2005 [cited 2008; Available from: http://www.defenselink.mil/news/Apr2005/d20050408strategy.pdf]

94. Joint Chiefs of Staff Washington DC. *The National Military Strategy of the United States of America*. 2004 [cited 2008; Available from: http://www.defenselink.mil/news/Mar2005/d20050318nms.pdf]

95. Staff, C.o.t.J.C.o. *National Military Strategic Plan for the War on Terrorism*. February, 2006 [cited 2008; Available from: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA443609&Location=U2&doc=GetTRDoc.pdf]

96. Strategy Division US Northern Command. *Department of Defense Homeland Security Joint Operating Concept*. February, 2004 [cited 2008; Available from: http://www.dtic.mil/jointvision/hls_joc_v1.doc]

97. Office of Force Transformation Office of the Secretary of Defense Washington DC. *Military Transformation a Strategic Approach*. 2003 [cited 2008; Available from: http://www.oft.osd.mil/library/library_files/document_297_MT_StrategyDoc1.pdf]

98. Office of the Secretary of Defence Washington DC. *Defense Science and Technology Strategy 2000*. May, 2000 [cited 2008; Available from: http://handle.dtic.mil/100.2/ADA379104]

99. Office of the Under Secretary of Defense for Policy Department of Defense. *Quadrennial Defense Review Report*. February, 2006 [cited 2008; Available from: http://www.defenselink.mil/qdr/report/Report20060203.pdf]

100. Department of Defense. *Joint Service Chemical and Biological Defense Program FY 08-09 Overview*. [cited 2008; Available from: http://www.acq.osd.mil/cp/cbdreports/cbd0vw08.pdf]

101. Wikipedia site entry on *Homeland security*. [cited 2008; Available from: http://en.wikipedia.org/wiki/Homeland_security]

102. The US Government. *National Strategy for Combating Terrorism*. September, 2006 [cited 2008; Available from: http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf]

103. Carafano, J.J. *Homeland Security in the Next Administration*. Heritage Lectures. May, 2008 [cited 2008; Available from: http://www.heritage.org/Research/HomelandDefense/hl1085.cfm]

104. Grimmett, R.F. *9/11 Commission Recommendations: Implementation Status*. CRS Report for Congress RL33742. December, 2006 [cited 2008; Available from: http://www.fas.org/sgp/crs/homesec/RL33742.pdf]

105. Koizumi, K. *Science, Technology, and the Federal Budget*. June, 2008 [cited 2008; Available from: http://www.aaas.org/spp/rd/propm608.pdf]

106. OSTP. *Science and Technology: A Foundation for Homeland Security*. April, 2005 [cited 2008; Available from: http://www.ostp.gov/galleries/Issues/ST%20A%20foundation%20for%20HNS.pdf]

107. Marburger, J. Memorandum for the Heads of Executive Departments and Agencies [cited 2008; Available from: http://ostp.gov/galleries/Budget09/FY2009FINALOMB-OSTPRDPriorityMemo.pdf]

108. Cohen, J.M., *Statement for the Record Jay M. Cohen Under Secretary, Science and Technology Directorate Before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Emergency Preparedness, Science, and Technology.* September, 2006. [cited 2009; Available from http://www.dhs.gov/xnews/testimony/testimony_1158337375757.shtm]

109. Carafano, J.J. *Rethinking Research, Development, and Acquisition for Homeland Security*. Heritage Foundation Backgrounder report. January, 2007 [cited 2008; Available from: http://www.heritage.org/Research/HomelandSecurity/upload/bg_2000.pdf]

110. Knezo, G.J. *Homeland Security Research and Development Funding, Organization, and Oversight*. CRS Report for Congress. August, 2006 [cited 2008; Available from: http://www.fas.org/sgp/crs/homesec/RS21270.pdf]

111. Cohen, J.M. *DHS Science & Technology: Enabling Technology to Better Secure the Nation*. Address to the AAAS Forum on Science & Technology Policy. May, 2007 [cited 2008; Available from: http://www.aaas.org/spp/rd/forumcohen.pdf]

112. DHS S&T Directorate. *Science & Technology Strategy to make the Nation safer….* June, 2007 [cited 2008; previously available from http://www.dhs.gov/xabout/strategicplan]

113. Marcella, G. *National Security and the Interagency Process*. U.S. Army War College Guide to National Security Issues Volume II: National Security Policy and Strategy, 3rd edition. June, 2008 [cited 2008; Available from: http://www.strategicstudiesinstitute.army.mil/]

114. The US Government. *TSWG website*. [cited 2008; Available from: http://www.tswg.gov/about.html]

115. The US Government. *CTTSO website*. [cited 2008; Available from: http://www.cttso.gov/about.html]

116. The US Government. *Work for Others program website and FAQ*. [cited; Available from: http://www.ornl.gov/adm/wfo/exthome.htm]

117. The US Government. *Homeland Security Technology Advancement Act*. [cited 2009; Available from: http://www.opencongress.org/bill/110-h4290/show]

Appendix A: The UK Model: in Detail

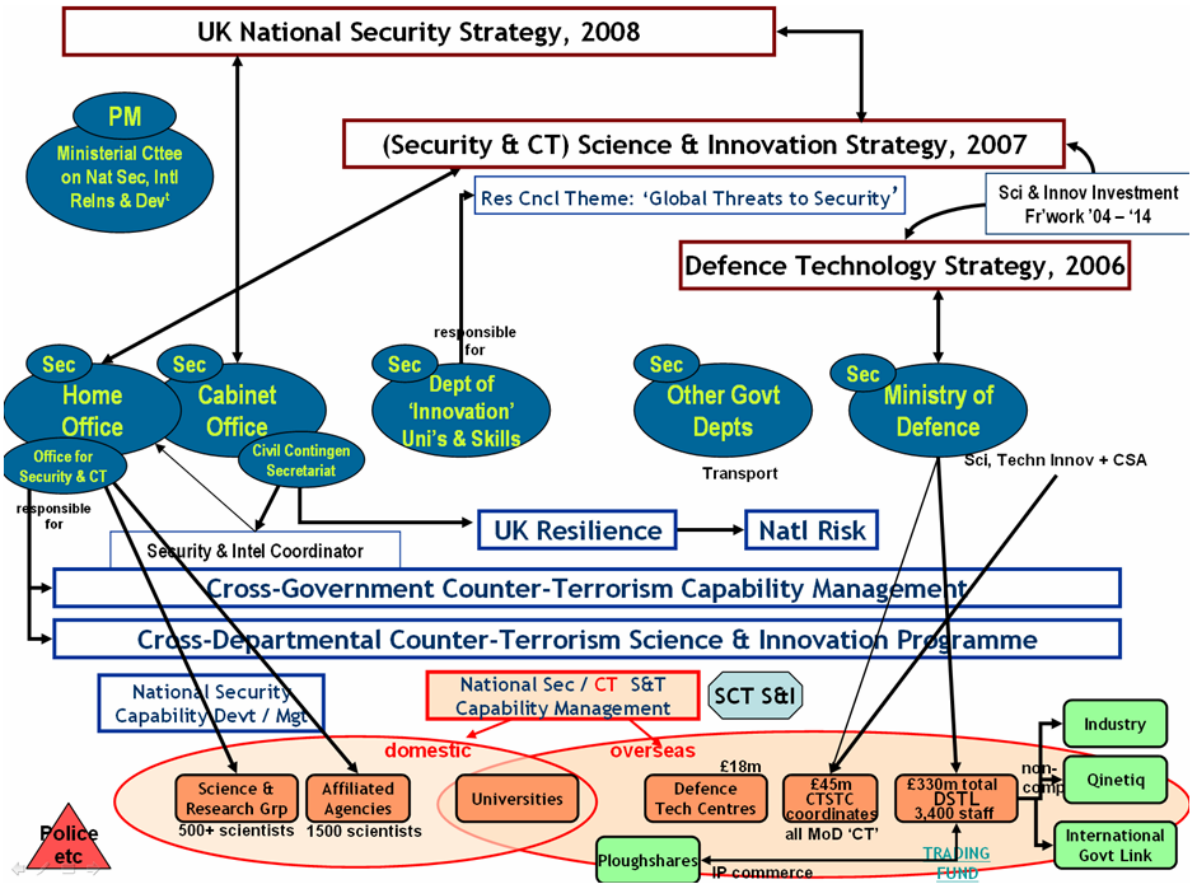

Figure 2: A template for the UK national security S&T support model

Figure 2 provides a rough roadmap of the key players and components of the UK national security and counter-terrorism arrangements. Strategic documents are shown at upper-right, in relation to their Government Department owners. The Home and Cabinet Offices share primary responsibility for domestic security and community resilience development. The Ministry of Defence is taking more of a domestic role, particularly in supporting science and technology for counter-terrorism. The Department of Innovation, Universities and Skills is the primary player in developing the required national skill base and science and technology capabilities. Beneath the Departments, Figure 2 shows the primary organising initiatives and programs under which security and counter-terrorism relationships are developed. The lower part of the figure shows the primary groups and players that own and develop national security science and technology.

The Secretary of State for Defence is advised on Defence S&T by the Defence Scientific Advisory Council (DSAC), a non-Departmental Public Body that sits "*at arm's length*" from ministers. DSAC primarily advises on the content and management of MOD's research programs, and the use of its resources. The Defence Technology Strategy [9] details the

methodology and criteria that MOD applies to define its S&T priorities. The Strategy also details those priorities publicly, in order to inform and position its potential S&T providers.

Prior to 2001 most MOD S&T was provided by the Defence Evaluation & Research Agency (DERA). On 1 July 2001, DERA was split into an MOD-owned Trading Fund (TF) called the Dstl [29, p3] and a private company Qinetiq (which was floated on the London Stock Exchange in February 2006).

The MOD has an annual R&D budget[11] of ~£3bn [9], which represents ~9% of the total Defence budget (~£33bn) which, in turn, is roughly 2.5% of GDP[12] (~£1,300bn) [73].

MOD specifically identifies ~£0.5bn as the 'research' (or S&T) component, termed the 'Science, Innovation & Technology Top-Level Budget' [74]. This budget is managed by the MOD's Chief Scientific Adviser (CSA). The CSA has a staff of approximately 120 in Whitehall and a further 120 in the Defence Technology & Innovation Centre (DTIC) Shrivenham (formerly the Research & Acquisitions Organisation, formed in 2003). DTIC's role is to take all MOD requirements and generate a coherent S&T program which it contracts out to all S&T providers (including MOD providers). CSA staff in Whitehall include an element called 'S&T for Counter-Terrorism & Operational Support' which owns the MOD's Counter-Terrorism Science & Technology Centre (CTSTC) at Porton Down. MOD partially funds (~£20m total) four Defence Technology Centres (DTCs) [75], or consortia of industry, academia and Defence (usually Dstl), designed to fast track promising emerging technologies into service. MOD also runs a number of initiatives in addition to the Top-Level Budget, such as 'The Grand Challenge' [22, 24], 'Competition of Ideas' [23] and 'Research Concept Demonstrators' [24] (each of ~£10m) to stimulate and exploit innovation.

Since the DERA split in 2001, MOD has consistently increased the proportion of research funds that it allocates competitively [29]. Approximately 37% of its budget is stable, reserved funding for Dstl, and is intended to remain so. Qinetiq's assured funding has been progressively reduced from ~60% (i.e., the remainder) in 2001, and will reach zero in 2009/10 [73, p21]. Qinetiq, alongside industry, academia and other providers, will then compete for MOD funds [73].

Dstl [76-79] is the primary provider of S&T to the MOD. It employs ~3,500 staff, currently across 15 sites (soon to be rationalised to 3 sites). Dstl does those things that are "*best done in government*" [29, p7], that is, where the work is of a sensitive nature, or represents sovereign knowledge that MOD identifies as a core requirement. The MOD also notes that the effectiveness of its international S&T relationships relies on Dstl's status as a non-commercial organisation [76, p3]. Dstl lists [29] its work (in order of decreasing funds) as: equipment capability; acquisition; other government departments; commercial; operations; intelligence; and policy. It does not explicitly list 'national security' as a defined role.

Dstl receives approximately half of its total (~£400m) budget from assured funding under the CSA's Top-Level Budget. This funding is assigned to elements of Dstl's program by agreement with the CSA; projects that fail to gain assured funds must (theoretically) compete

[11] 2006 figures
[12] Goss domestic product.

with other providers (but in reality there are few alternative providers for the work requested). Determining which programs are funded has, in the past, relied more on timing than advance planning[13]. An additional, equivalent fraction of Dstl's budget also originates from MOD, but comes via DTIC and the Defence Engineering & Support Agency (DESA) and is allocated for support mainly to MOD's equipment capability and acquisition processes. The remaining funds come (mostly) from non-Defence Departments, primarily the Home Office. A criticism of Dstl's funding model has been that all funding allocations were relatively short-term. Dstl is currently addressing this issue and intends to identify (four) core themes or objectives that will define areas in which it will adopt longer-term, strategic approaches to S&T capability needs [80].

Dstl was set up, from its birth, as a TF [33]. The UK currently has more than 20 Government Departments or Executive Agencies set up (with permission of HM Treasury) as TFs. An early example was the Royal Mint (1975). Defence Support Group was established as a TF on 1st April 2008 [81]. "*Trading funds are a means of financing the revenue-generating operations of a government department...* [they engender] *a more commercial and business-like approach to managing … activities…* [C]*ompared with being financed from Supply, it offers more flexibility... Trading funds retain their trading income which is used to meet expenditure… They are not separate legal entities and remain part of a department* [in Dstl's case, MOD] *(or are departments in their own right)…"* [32] "*Trading Funds are required by statute to recover principally their costs (i.e. to recover a majority of their costs) through income derived from operations within the trading fund…*" [33]. In 2005/06 Dstl's profit was £21.8m from which it paid a £3m 'dividend' to MOD. Dstl is currently rationalising its sites, at a cost of £92m, which it will fund from retained profits.

Dstl's status as a TF should, theoretically, give it some autonomy in defining its program, and some ability to support 'sustainment' or internal capability development. In practice, all Dstl expenditure has, in the past, required a sponsor and Dstl must seek approval from MOD on its spending intentions. To date, Dstl has not spent on unsponsored development [80].

Most of the work requested by other government departments has originated from the Home Office, and was undertaken by the Forensic Explosives Laboratory at Fort Halstead. There is no specific mechanism that defines or supports this relationship and tasking by non-MOD agencies is only supported where it leverages existing (MOD-derived) capability, and where Dstl assesses it has the capacity to do so [80]. Dstl has not developed mechanisms to enable it to prioritise this work in the context of MOD requests but "*sometimes priorities are quite clear*" [80] such as support to high profile issues like the London bombings and other major terrorism incidents.

In 2005, Dstl formed (and retains management of) a technology transfer company, Ploughshare Innovations [82] to commercialise Dstl intellectual property. Ploughshare has created several 'spin-out companies' and 'strategic joint ventures'.

The CTSTC [83], also known as 'The MOD CT Centre' is funded under the CSA's Top-Level Budget and acts as "*the hub for UK MOD counter-terrorism S&T*". It has a staff of 21[14], 18 of whom came from Dstl (the remainder from commercial companies) and an annual budget of

[13] Personal communication with a Dstl Chief indicated it is closer to 'first-in-best-dressed' [80].
[14] Increased to 25 on latest (December 2008) information [30]

~£40m[15] mainly used to contract R&D [74]. It also administers a ~£5m fund which it uses to stimulate and exploit innovation (see the MOD Grand Challenge [22]).

The CTSTC was set up to carry out MOD and other government CT work, exploiting MOD's strengths in translating technologies into end-use capabilities. The vast majority of the CTSTC's work is for MOD and is focused on quick reaction operations-support for UK troops deployed in the Middle East Area of Operations (MEAO) and other high risk areas, as well as longer term CT-related research, again, for the MOD. The CTSTC is conducting some R&D for other Departments (mainly the Home Office), this is below target levels and the CTSTC has introduced management changes to enhance the non-MOD component. While the Home Office tasks the CTSTC (and places staff within the CTSTC on secondment) there is currently no reciprocal arrangement whereby the Home Office is tasked to support MOD interests. While the rhetoric (on public domain websites) would suggest otherwise, there is a notional divide between the 'home' and 'away' games, such that the Home Office addresses domestic CT, while the CTSTC looks after offshore concerns. Cross-fertilisation is most evident in areas of counter-IED research.[16]

MOD, Dstl and the CTSTC are increasingly seen as key assets in the Government's evolving plans to address security and counter-terrorism, under the UK's NSS. The Home Office has "*primary responsibility for counter-terrorism*" and is, more broadly "*responsible for keeping the UK safe from any threat to… national security*" [10]. In these roles, it works very closely with the Cabinet Office, whose Civil Contingencies Secretariat (CCS) [84] manages the 'UK Resilience' [14] program. While Defence has formally contributed to strategic policy (e.g., the 'UK Security & Counter-Terrorism Science & Innovation Strategy' (UKSCTSIS), 2007, which was an initiative of the Office of Security & Counter-Terrorism or OSCT [85]) MOD involvement has been limited to the CTSTC and Dstl roles described above.

The OSCT, which reports directly to the Home Secretary and the Minister, is housed in the Home Office and has about 300 staff. It is strongly focused on CT rather than broader national security objectives and would not consider the security implications of climate change, for example, which would instead, fall within the remit of its parent, and the Cabinet Office. The OSCT is currently building on the UKSCTSIS, developing a capability framework and identifying capability gaps and priorities via scenario-driven, cross-departmental working groups [86]. The OSCT identifies research that meets its CT objectives that is carried out within particular Departments (e.g., Home Office, MOD etc.) but it also sponsors research (with a budget of ~£30m in 2008/09) under the new cross-departmental 'Security & Counter-Terrorism Innovation Program' (SCTIP). Like the Canadian CRTI (see below), the SCTIP is expected to operate by calling for proposals and conducting analysis to identify projects that are likely to deliver capability. MOD, in particular Dstl (for CBRN and explosives research) and the CTSTC (for broad CT) are expected to become key contributors to this initiative. Where a conflict of resources occurs within MOD, for example, key staff are required for both MOD and OSCT projects, it is expected that the CTSTC will coordinate as far as possible, but ultimate arbitration will reside with the Defence R&D Board which is chaired by the MOD CSA.

---

[15] Increased to £55-£60m on recent information (December 2008) [30].

[16] This situation appears to be changing quite significantly and there is a growing interaction between Home Office and CTSTC [30].

As the Home Office's roles and responsibilities with respect to CT have evolved from the days of IRA[17] terror, the Home Office has largely developed or acquired its own, in-house S&T capabilities rather than accessing these from other Departments [11]. Its collective S&T capability is called the 'Science & Research Group' (SRG) and numbers several hundreds of scientists if the boundary is drawn strictly around the Home Office, or some thousands if affiliated agencies such as the Forensic Science Service are also included. The Home Office annual S&T budget is ~£70m which includes a ~£14m component for "cross-Whitehall CBRN" (involving MOD). The primary Home Office S&T capabilities reside in the: Home Office Scientific Development Branch (HOSDB, formerly the Police Scientific Development Branch) which provides 'physical and technical' support; the Research Development & Statistics group (RDS) which works primarily in 'social sciences' related to crime reduction; the Economics & Resource Analysis Unit (ERAU) which conducts economic modelling; and the Central intelligence Hub (CIH), which works to the Home Office CSA and provides, amongst other things, security risk advice.

Home Office S&T capabilities have grown primarily to address crime fighting including trans-national crime, and their focus has been largely on tactical/operational 'kit' to be placed in the hands of the police. The OSCT is an attempt to raise the perspective, which has necessarily generated appreciation of the need to cross Departments which, in turn, has led to cross-Departmental initiatives such as the SCTIP.

The Department of Innovation, Universities and Skills (DIUS) is responsible for the UK's national science and innovation program. The UK recognises the importance of R&D (Sainsbury Review [87]) as a primary driver of national growth, and its long-term objective is to raise national R&D to 2.5% of GDP by 2014[18].This can be compared (in 2004 figures) with 2.7% GDP in the US, 2.2% in France and 2.5% in Germany. DIUS' budget will correspondingly rise from ~£3.3bn now, to ~£4bn by 2010/11. The (7) national research councils have recently agreed on four themes for cross-program funding, one of which is 'Global Threats to Security', allocated $113m (or 9% of the cross-Program pool) [21].

There is a significant degree of alignment and consistency between the objectives and methods of MOD [9, 19] and DIUS [15] in stimulating and exploiting innovation. In addition to a number of new initiatives (e.g., Grand Challenge) MOD [9] relies substantially on Dstl to develop "*close and effective relationships with the universities*" [9, p9] in support of its aim to create a "*DARPA-like effect*" [9, p9], that is rapid transitioning of concepts into end-user capability. MOD also aims to expand its S&T provider base into industry through strategic documents that provide clear guidance on Defence R&D priorities.

The recently released UK National Security Strategy (or NSS, 2008) 'Security in an Interdependent World' [4] defines the scope of its national security concerns more broadly than counter-terrorism and trans-national crime. It explicitly includes, for example, civil emergencies, climate change and energy security. The rhetoric of the Strategy is relatively new. It reveals an emerging appreciation of the fundamental need for cross-Departmental approaches to dealing with strategic challenges like national security. While it understands

[17] Irish Republican Army
[18] From about 2.0% in 2008

that the MOD is a critical element of the resources it needs, the UK is yet to articulate the role of Defence – this is the subject of an inquiry [26] initiated in April 2008, considering:

a. *"what contribution the MoD makes to national security and resilience, and what resources are committed to delivering it;*

b. *what specific capabilities maritime, land and air forces provide for national security and resilience;*

c. *what the MoD understands to be the nature and scale of the threat to national security, and how it gathers information;*

d. *how the changing security agenda has affected Defence Planning Assumptions;*

e. *how the MoD cooperates with other Government departments and agencies both to determine and, when necessary, to deliver the military component of national security, and how that dialogue is organised."*

While the UK has been thinking and developing structures to deal with counter-terrorism, it must now re-think [72] methods to address the scope of its national security objectives. The 'machinery' of government appears to lag significantly behind the goals of its new thinking.

Appendix B: The Canadian Model: in Detail

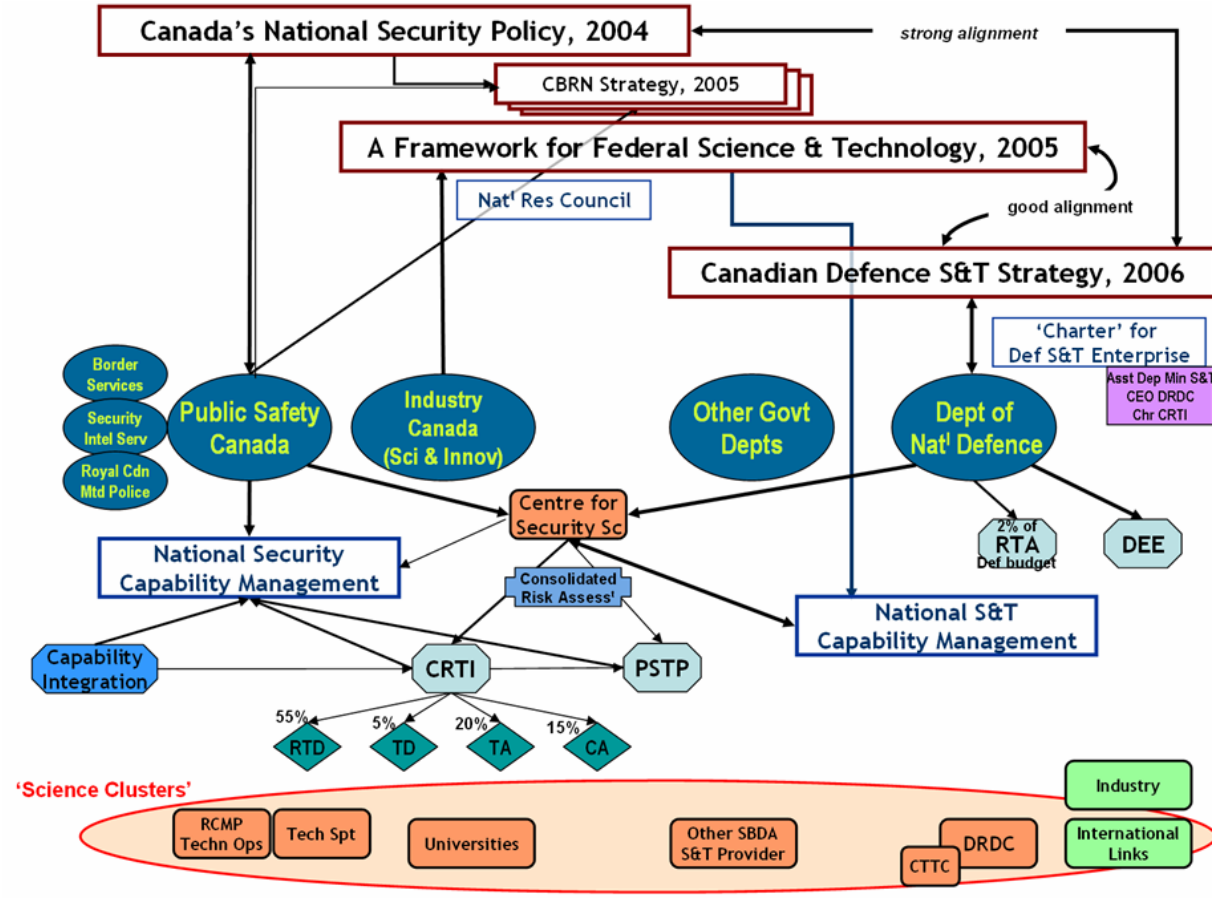

Figure 3: A template for the Canadian national security S&T support model

Figure 3 provides a rough roadmap of the key players and components of the Canadian national security and counter-terrorism arrangements. Strategic documents are shown in the upper part of the figure, in relation to their Government Department owners. Public Safety Canada (PSC) has primary responsibility for domestic security issues. The Department of National Defence which owns Defence Research & Development, Canada (DRDC) partners PSC in managing and developing the Centre for Security Science, which is a key driver of national security science and technology. The Department of Industry Canada is the primary player in developing the required national skill base and science and technology capability. Beneath the Departments, Figure 2 shows the primary organising initiatives and programs under which security and counter-terrorism relationships are developed. These include the CBRN Research & Technology Initiative (CRTI) which has been the largest organising framework and funder of security science and technology. The lower part of the figure shows the primary groups and players that own and develop national security science and technology.

Canada's DND budget, in 2008, was C$18.2bn (or ~1.4% of GDP compared with 2.5% for the UK). Canada has committed to raising the Defence budget by 2% every year until 2031, at which time it should reach C$31bn (although this represents a reducing fraction of GDP, which is itself growing at 2.7% pa).

Figures for Defence spending on R&D and S&T are difficult to find. In 2000, Canada's total spend (from all Departments) on R&D was 1.8% of GDP (the same as the UK). Of that total, Defence R&D accounted for only 5.6%, compared with the OECD average of 30.3%[19]. Similarly, spending from all government departments explicitly identified as S&T totalled C$7.7bn in 2002/03 [43] – DND was ranked 12th relative to other government departments, at C$330m (4% of national S&T spend, compared with the US where defence accounts for more than 50% of S&T spend). Current documents indicate that DND spends a long-term average of 2% of its budget on S&T (representing ~C$360m in today's figures).

Canada's Defence Management Committee provides strategic oversight of DND development, which is managed at the working level by the Defence Management Oversight Committee. "*The 'Assistant Deputy Minister (S&T)' exercises this functional authority, and is accountable to the Deputy Minister Defence, and the Chief of Defence Staff*" [44, page iv]. The Assistant Deputy Minister (S&T) is also the CEO of DRDC.

Canada's first 'Defence Technology Strategy' (DTS) [68], an initiative led by DRDC, was released in 2006. The Strategy promotes "*effective direction, delivery and exploitation of the departmental investment in S&T… and establishes the conditions to maximize … impact … by ensuring that* [S&T investment] *is aligned with priorities… harnessed to be a force multiplier and is … supportive … of defence … and its core business processes.*"

DND's S&T investment is "*managed through the Defence S&T Enterprise*", [68, page iv] representing all of DND's S&T providers, users and stakeholders. "*A charter defines the Defence S&T Enterprise objectives, organizational architecture, relationships among its members and their roles, as well as its governance*" [68, p11]. The DTS explicitly names the Royal Military College as an S&T provider within the Enterprise, but DRDC seems to be the only substantial defence-owned S&T provider.

"*For reasons of interoperability, economy of scale and affordability, Canada emphasizes non-developmental procurement. Through the provision of smart buyer and smart user advice, S&T can directly support this approach.*" [68, p9]. The DTS defines two "*complementary programs of work for managing the departmental S&T investment*": the Research, Technology and Analysis (RTA) program; and the Development, Engineering and Evaluation (DEE) program. This appears to be a distinction that DND makes between 'S&T' funds (~C$360m for the RTA program) and broader 'R&D' funds (~C$1bn[20] for DEE).

Under the RTA program, the DTS indicates that "*approximately 50% of … funds support in-house delivery of S&T, with the other 50% used to engage external S&T performers*" [68, p20]. This appears consistent with scarce information about staff numbers in DRDC, suggesting a relatively light organisation of less than 2,000 (< 1,000 'scientific and professional') employees [43]. DRDC

[19] 1998 figures
[20] This figure is inferred from other scant data.

also sets targets for both national and international leveraging. "*The huge investments outside the department in industry and academia, domestically and internationally, produce vast amounts of knowledge that can be accessed and applied to departmental and Canadian Forces needs*" [68, p6]. In 2006/07 it achieved C$63m of leveraged value[21] [48] from national partners, and C$95m of value from international partners.

The total value of DRDC's S&T Program in 2006/07 was C$309m [48]. Of this total, 45% (~C$140m) was funded internally, 30% (~C$94m) came from R&D contracts, and 25% (~C$75m) came from external (non-DND) sources. Approximately 35% (C$109m) of the 2006/07 budget paid DRDC salaries, 28% funded contracts, and 21% went to capital works and maintenance. Of DRDC's seven research centres, the Centre for Security Sciences (CSS) accounted for 9% (C$28m) of DRDC's budget and the Counter-Terrorism Technology Centre (CTTC) represented 1% (C$4m). While the CSS administers national funding programs of substantial value (CRTI ~C$35m / year) the running costs of the CSS are monies that DRDC brings to the venture.

The philosophy of external S&T access and leveraging is a strong, consistent message of Defence, other departments and, in fact, all strategic guidance [46]. "*The Defence S&T Enterprise only has the capacity, even with partners, to generate but a fraction of the scientific and technological knowledge that is needed by the department and the Canadian Forces. Therefore…* [the Enterprise] *depends upon access to the international S&T base and to S&T providers outside of the department…".* [68]

Industry forms a key component of the Canadian innovation system. The Defence S&T Enterprise seeks to develop strategic relationships with domestic and multi-national industry, and granting "*councils including consideration of shared investments in critical S&T infrastructure*" [68]. "*The Defence S&T Enterprise plays a proactive role in contributing to the public security S&T agenda, just as the Canadian Forces contribute to the public security agenda*" [68, p16].

All of this is consistent with Industry Canada's (the government department responsible for science and innovation) 'Framework for Federal Science & Technology' (2005) [46]. The Framework "*applies to all federal departments and agencies and their employees*" and "*sets out the Government of Canada's continuing commitment to effectively conduct and manage science and technology (S&T) in support of action on issues of concern to Canadians*". The Framework: articulates "*the role of federal S&T*"; guides "*the conduct and management of federal S&T*", and "*identifies the features of an environment that promotes and supports federal S&T*".

The Framework, and Departmental strategies make frequent reference to 'Science-Based Departments and Agencies' or SBDAs, as those areas of government that contribute to, or rely on S&T. Canada recognises 21 SBDAs of which DND is one. Under three 'core principles' the Framework states [46] that:

> *"… the complexity of … areas such as … security… demands a collaborative, horizontal approach to S&T across departments… No single department can successfully address such challenges in isolation… partnerships, collaboration and integration expand the value and*

[21] "*We estimate the value of our collaborations based on the likely cost of acquiring similar value through research contracts.*" [48, p42].

> *reach of federal S&T….* [enable] *more efficient and innovative use … and facilitate quick mobilization in response to emerging issues…*
>
> *SBDAs are … develop*[ing] *mechanisms to encourage interdepartmental S&T integration, including ways to collectively set and fund priority areas, … sharing of physical infrastructure for S&T, and … development of multi-party R&D network clusters around critical public policy and scientific issues…* [to enhance] *efficiency and effectiveness through asset sharing, co-location and facilities integration".*

Under the Framework's philosophy, the Government has since taken steps to identify and address the many 'barriers' to effective S&T collaboration across government [47].

> *"… the federal science and technology (S&T) community has recognized the growing need to work collaboratively on cross-cutting S&T issues… Reconciling vertical accountability at the departmental level with the collective, horizontal responsibility of a linked S&T system is one of the biggest obstacles… Centrally managed/accountable horizontal programs such as the Public Security Science and Technology Program (PSTP) and CRTI*[22] *have identified that there are gaps in the mechanisms to transfer funds and the timeliness of transfer between federal institutions…"* [47, p12].
>
> "[In the CRTI]*… a lead department is selected to oversee research on a particular priority on behalf of the other departments, and money is provided to it through an interdepartmental settlement. Funding is provided to universities by contract…"* [47, p13]

Canada recognises that effective collaborative arrangements do not develop naturally:

> *"A significant gap is that there is still no broad cultural basis for horizontal collaboration. The continuing experience in CRTI is that project teams do not develop because they inherently value the interdepartmental approach or may recognize the value of collaboration, but because they are obligated to by mandatory criteria that force collaboration…"* [47, p24]

Canada's National Security Policy 'Securing an Open Society' was published in 2004 [3], with an update one year later [36]. It defined the scope of national security quite widely when compared with the views of partner nations at the time. This was prompted by its experiences with SARS; a member of a class of "*threats that have the potential to undermine the security of the state or society*" [3, p3]. The Policy outlined the integrated security system that was in conception, and created a new Department 'Public Safety and Emergency Preparedness Canada' which became (in 2007) 'Public Safety Canada', the department responsible for Canada's national security. The Policy also adjusted governance, creating a new 'National Security Committee of Parliamentarians', noting that: "*The Government is committed to providing the leadership, resources and structures necessary to build a fully integrated and effective security system*".

Following release of the Policy, PSC has since developed and published many subordinate strategies, including a CBRN Strategy [39], a National Strategy for Critical Infrastructure [40], a National Crime Prevention Strategy [41], and others [38]. The Strategies are consistent with

[22] Described below.

one another, and with other strategic documents [47 and 68]. They stress the importance of cross-government coordination and integration. They also define the roles and responsibilities of all agencies; for example, the CBRN Strategy states that "*DRDC … coordinates the Government of Canada's CBRN R&D / S&T efforts*".

In 2002, the 5-year, C$170m CRTI [52, 54, 55, 88 & 89] was established as one of the first federal S&T programs attempting to link many SBDAs under common S&T objectives. It was set up to address and inform federal stakeholders on CBRN risks and vulnerabilities, federal CBRN preparedness, and the status of federal S&T / industry alignment and its links to end user needs. Its primary aim was to "*mobilize Canada's innovation system*" through six key activities, namely "*creating laboratory clusters, building S&T capability, accelerating technology to first responders, funding national S&T capacity, building horizontal capability, and building CBRN expertise and knowledge*" [54, pp1-2]. DRDC was the key architect of, and a contributor to, the CRTI. Its success led, in 2005, to creation of the CSS [50].

The CSS is a "*joint endeavour*" of PSC[23] and the DND (through DRDC) described under a Memorandum of Understanding, but it is "*very much a DRDC organization*" [51]. It provides S&T to address national public safety and security objectives. It is part of the Government's approach to public security science and technology (PSST). The CSS is the "*organization through which DRDC provides S&T services to Public Safety Canada*" [50]. The CSS "*functions within the 'Framework for Federal S&T', and the Federal S&T Enterprise Framework…*". It "*coordinates an S&T development program*" with 19 other SBDAs [47].

The CSS has carriage of Canada's strategic public security capability development process. DRDC has been instrumental in applying its expertise to promote a CBP approach to security [90], recognising the analytical overheads involved, the need to prioritise and balance input costs against output values, the need to balance operational priorities against future capability and capacity needs, and the organisational complexities of managing across a multi-departmental, multi-stakeholder environment [51]. Two programs represent the pillars of the approach. These are the CRTI which gained approval in 2006 for its second 5-year, C$175m (phase 2) program, and the PSTP, which was initiated in 2003, but is much less mature than CRTI[24] (it is due to call for 'studies' in September 2008). The CRTI is largely managed by DRDC (through the CSS), while the PSTP is managed by PSC.

In accordance with the Federal Framework for S&T (which it preceded by several years), CRTI has generated, as core elements of its cross-Departmental model, five enduring 'laboratory clusters' (sometimes called 'science clusters' [56]). These are "*arrangements for dialogue and discussion in the federal science and technology (S&T) community. They focus on the joint needs of scientific labs and the operational community… share their ideas, knowledge, experience, and resources, and discuss challenges and solutions*" [56]. The CRTI's five clusters are: 'chemical', 'biological', 'rad/nuclear', 'forensics', and (since 2006) 'explosives'. Each cluster "*will maintain and grow leading-edge scientific capabilities both to support its response roles and responsibilities and to enhance the nation's preparedness*". Cluster members are agencies (for example, DRDC, the Royal

[23] Agencies of PSC include the Canadian Security Intelligence Service, Canada Border Services, Correctional Service Canada, and the Royal Canadian Mounted Police.
[24] There appears to be a 3rd program recently added to the CSS website's Programs: Canadian Police Research Centre

Canadian Mounted Police) or SBDAs. The clusters "*are managed and guided by non DRDC science champions but include DRDC scientists*" which has been "*important in maintaining the system credibility and avoiding conflict of interest… The model has matured greatly and conflict issues or claims/perceptions very rarely arise if at all*" [51].

An early component of the CRTI's work driven by DRDC involved developing a strategic risk view – the Consolidated Risk Assessment (CRA) [91] - to inform priorities and funding allocation decisions. The CRA is a scenario-driven "*systematic approach to risk and gap analysis… integrated with longer reaching foresight methodologies*" [90], and is now a centrepiece in the CRTI's CBP 'Investment Model'. This model enables the CSS to identify 'mission critical strategic outcomes' (five years out), intermediate (3-5 years) and immediate (1-3 year) required outcomes.

Phase 2 of CRTI (2006-2011) aims to shift the emphasis towards transitioning and exploiting earlier S&T investments, and demonstrating value and impact associated with enhanced operational capabilities. The CSS sees itself as the "*conduit for government to capitalize on prior S&T investments*" [92].

The CRTI funds research under four categories. Research and Technology Development (RTD) projects are of 3-5 years' duration, $1m to $4m total, and generate outputs at the low to middle part of the technology readiness spectrum. RTD projects account for 55% of CRTI funds expended to date.

Technology Demonstration (TD) projects are of 2-3 years' duration, funded to $1m-$3m total, and generate products in the mid-to-higher end of TRLs. TD projects account for 5% of CRTI funds spent to date.

Technology Acceleration (TA) projects are of 0.5 to 2 years' duration, $1m to $4m total and focus on the high end of technology readiness. These projects account for 20% of CRTI funds to date.

The fourth category was termed Technology Acquisition, but more recently changed to Capability Acquisition (CA). It is intended to enhance the equipment or infrastructure of the 'laboratory clusters' and build national S&T capability and capacity. It has expended ~15% of CRTI funds to date (primarily in phase 1).

For funding under the RTD, TD and TA project categories, "*a Proposal Selection Committee, composed of experts in the fields of CBRN S&T, public security, and counterterrorism, evaluates the project proposals*". For funding under the CA category, "*the laboratory clusters identify requirements through consensus and make submissions to a Project Review Committee, chaired by the Director of CRTI and made up of the laboratory cluster leaders, before going to the Steering Committee for funding approval*" [54 Annex C].

Each funded proposal under CRTI (or PSTP) has a lead agency, and a defined set of collaborators. Of the 26 projects funded in the 2005/06 round of CRTI proposals, six were led by DRDC, and DRDC was a member in fifteen others. CRTI projects have involved: 23 federal government departments, 57 industries, 21 provincial agencies, 21 universities, 6 foreign universities, 32 foreign agencies and 17 other agencies.

Continuing and future work under the CRTI is aimed at improving understanding of the less well known components of the CRTI Investment Model (e.g., 'Full Spectrum Threat Scenarios', 'Capability Audit' etc.), and dealing with acknowledged continuing structural challenges, ie, fragmented stakeholder communities, limited analytical resources and the conceptual difficulties of a CBP approach [54].

Over the last seven years of CRTI, it has adjusted a number of balances, namely, (a) from earlier generation of cluster S&T capability/capacity towards production of operational capability for end users, (b) from a focus on the 'consequence' end of the CBRN spectrum, towards the 'prevention' end, and (c) from exclusive funding of 'low risk' R&D towards acknowledging the need for some 'high risk, paradigm shifting' R&D. Note also, that while the CRTI operates under a 'call for proposals' model guided by CBP priorities and objectives, it is now supplementing this process through focused investment in areas that were relatively unsubscribed, through 'specified capability' and 'specified exploitation' projects [51, 90].

Appendix C: The US Model in Detail

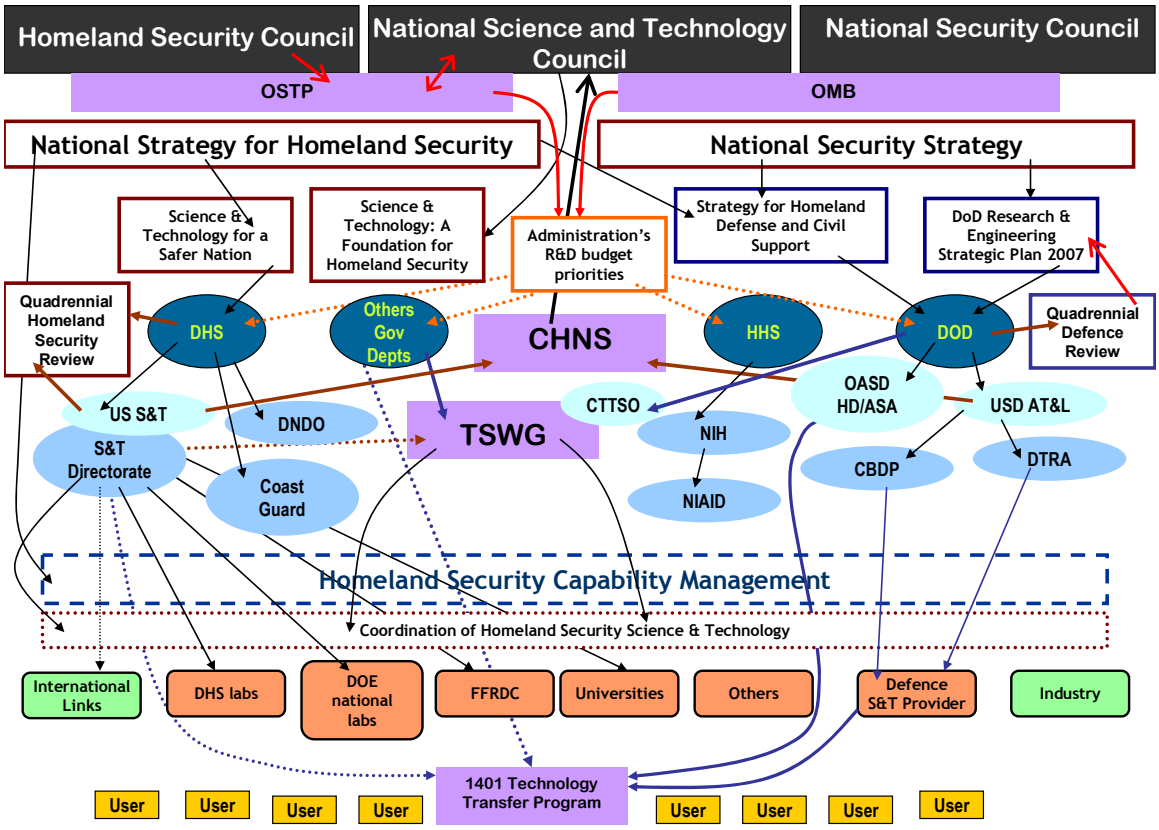

Figure 4: A template for the US homeland security S&T support model

Homeland security is officially defined by the 2007 U.S. National Strategy for Homeland Security [2, p3] as "*a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur*".

The DoD contribution to homeland security (referred to as homeland defense and civil support [61]) is led chiefly by the US Northern Command headquartered (USNORTHCOM) in Colorado Springs, Colorado, in collaboration with US Pacific Command (USPACOM), North American Aerospace Defense Command (NORAD), US Strategic Command (USSTRATCOM) and other DoD combatant commands and agencies. The Assistant Secretary of Defense, for Homeland Defense and Americas' Security Affairs provides overall supervision of DoD's homeland security activities and policy guidance.

The Strategy for Homeland Defense and Civil Support [61] articulates the DoD's role and responsibilities for defending against and responding to attacks on the homeland. It carefully

distinguishes the DoD's roles from those of DHS and the Attorney General in dealing with terrorist threats.

"The DoD is responsible for … the protection of US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President" [61, p5]. The DoD also provides "*Defense support of civil authorities… including Federal military forces, the Department's career civilian and contractor, and DoD agency and component assets, for domestic emergencies and for designated law enforcement and other activities... Defense support of civil authorities* [is provided] *when directed to do so by the President or Secretary of Defense."* [61, pp5-6]

The Strategy draws directly from the National Security Strategy [57], the National Strategy for Homeland Security [1] and the National Defense Strategy (2005)[25] [93]. In addition it complements other high level documents including standing National Security and Homeland Security Presidential Directives [58], the National Military Strategy [94], the National Military Strategic Plan for the War on Terrorism[26] [95], the DoD Homeland Security Joint Operating Concept [96], and Military Transformation: a Strategic Approach [97].

The Strategy focuses on the DoD's goal of securing the US from direct attack through an active, layered defense, which "*… is global, seamlessly integrating US capabilities in the forward regions of the world, the global commons of space and cyberspace, in the geographic approaches to US territory, and within the US. It is a defense in depth."* [61, pp1-2]. In this way, the DoD marries its domestic responsibilities with its off-shore roles in a unified fashion: *"The Department can no longer think in terms of the "home" game and the "away" game. There is only one game."* [61, p40].

The Office of the Director of Defense Research and Engineering (DDR&E) published its Defense Science and Technology Strategy in 2000 [98]; a more updated Strategic Plan (DoDR&E (SP)) was completed in 2007 [60]. The Research and Engineering (R&E) strategic plan identifies the principles, capabilities, and technologies that are used to guide the investment and management of the DoD R&E program. It provides guidance for all Services, agencies, and other DoD Components. While it does not explicitly address Homeland Defense and Civil Support, its guidance was derived from related higher level guidance: The National Security Strategy [57], National Defense Strategy [93], National Military Strategy [94], the Strategic Planning Guidance (SPG)[27] and the Quadrennial Defense Review (QDR) [99]. Strategic required outcomes are articulated as "*Defeat terrorist networks; Defend the homeland in-depth; Shape the choices of countries at strategic crossroads; and Prevent the use of* [Weapons of Mass Destruction] *WMD*" [99].

In addition "*the QDR establishes a strategy whereby the Department is prepared to accept some risk in countering traditional challenges, while enhancing capabilities to combat irregular, catastrophic, and disruptive threats*" [60, p15].

The DoD expenditure represents more than half of the total US Federal R&D budget. The total DoD discretionary budget for 2009 is US$515.4bn. Much of the Defense spend is on

[25] The US National Defense Strategy was recently updated in June 2008
[26] Updated in 2006
[27] The SPG was replaced in 2008 by the new Guidance for the Development of the Force (GDF)

development of equipment and weapon systems (US$69bn). DoD S&T spending, which includes basic and applied research, medical research, and technology development, totals US$11.7bn [63]. Some additional Defense-related R&D comes from the Department of Energy (DOE), which is responsible for maintaining the US nuclear weapons stockpile.

R&D in the DoD is largely the responsibility of the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (ATL). A number of offices and agencies are relevant to homeland security R&D. These are briefly described below. Generally DoD S&T comes under the Director, Defense Research & Engineering (DDR&E). However the Assistant to the Secretary of Defense, Nuclear & Chemical & Biological Defense Programs manages all CBRNE[28] R&D policies, plans and activities, including those of the DTRA.

The DDR&E is responsible for research and engineering (R&E) programs relating to DoD budget items 6.1 (basic research), 6.2 (applied research), 6.3 (advanced technology development) and 6.4 (Advanced Component Development and Prototypes programs). The items 6.1, 6.2 and 6.3 are considered by DoD as S&T activities. The DDR&E is the principal staff advisor for research and engineering matters, and serves as the Chief Technology Officer for the DoD.

The DoD R&D Budget fund (US$11.7bn) is spent predominately by universities (on basic research), DoD Services and labs, and industries (mainly for development) [63]. While there are more than 100 DoD R&D facilitates and laboratories, the following three programs and agencies are most relevant to homeland defense and civil support.

Defense Threat Reduction Agency (DTRA) is "*charged with the mission to safeguard the US and its allies from WMDs by providing capabilities to reduce, eliminate, and counter the threat and mitigate its effects*" [60, p12]. It invests in technology, as well as leveraging other Federal and industry R&D where appropriate, to develop enabling technologies to address the WMD threat. DTRA's Research and Development Enterprise conducts S&T research within four directorates: Chemical Biological Technologies (CB), Nuclear Technologies, Counter WMD Technologies, and Basic and Applied Sciences.

DARPA is the central R&D organisation for the DoD. It manages and directs selected basic and applied R&D projects for DoD, and pursues research and technology where risk and payoff are both very high. It is DoD's only research agency not tied to a specific operational mission. It conducts research that bridges the gap between fundamental discoveries and their military use, ideally leading to transformational capabilities for all DoD mission areas.

CBDP is a DoD program to provide chemical and biological defense capabilities in support of the National Military Strategies. Its research, development, and acquisition (RDA) programs aim to support US forces "*with the best equipment to ensure their survivability and mission accomplishment on any future battlefield where chemical or biological agents may be employed*" [100, p3]. The program utilises the Services laboratory (such as the Army's Edgewood Chemical Biological Center) and test facilities, with Army as the executive agent. The USD ATL provides oversight via the Assistant to the Secretary of Defense, NCB (Nuclear, Chemical and Biological). A Joint Requirements Office (JRO-CBRND) is responsible for the planning,

[28] Chemical, Biological, Radiological, Nuclear and Explosive

coordination, oversight of Joint CBRN defense operational requirements, and development of overarching operational concepts, joint doctrine and plans [100].

As a result of the Homeland Security Act of 2002, a new cabinet-level department called Homeland Security (DHS) was formed to consolidate the many activities and responsibilities of much of the executive branch of the US government, including the US National Guard, the Federal Emergency Management Agency (FEMA), the US Coast Guard, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, US Citizenship and Immigration Services, the US Secret Service, the Transportation Security Administration and Civil Air Patrol [101]. In addition to counter-terrorism, inclusion of FEMA added the responsibility for preparedness, response, and recovery to natural disasters and accidents.[29]

While DHS's primary mission is to prevent terrorist attacks within the US, much of the nation's homeland security capability and activity lies outside of DHS; for example, the FBI (Federal Bureau of Investigation) and CIA (Central Intelligence Agency) are not part of the Department, and other agencies such as the DoD and Department of Health and Human Services (DHHS) play significant roles in homeland security [101].

The 2007 National Strategy for Homeland Security [2] provides a common framework to focus the nation's efforts on achieving four goals:

a. "*Prevent and disrupt terrorist attacks,*

b. *Protect the American people, our critical infrastructure, and key resources,*

c. *Respond to and recover from incidents that do occur, and*

d. *Continue to strengthen the foundation to ensure our long-term success*."

While the first three goals help to organise the US national efforts, the last goal entails creating and transforming its homeland security principles, systems, structures, and institutions. The strategy builds the case that this would require [2]:

a. "*a comprehensive approach to risk management,*

b. *building a culture of preparedness,*

c. *developing a comprehensive Homeland Security Management System,*

d. *Improving incident management,*

e. *better utilizing S&T, and*

f. *leveraging all instruments of national power and influence*"

[29] There are continuing calls to move FEMA out of the department amid criticisms that FEMA's emergency response capability has eroded while DHS focuses on counter-terrorism. This was evident during the Hurricane Katrina disaster.

The Strategy builds upon the 2002 National Strategy for Homeland Security [1] and incorporates lessons learnt from exercises and real-world catastrophes such as Hurricane Katrina. The Strategy complements both the National Security Strategy [57] and the National Strategy for Combating Terrorism [102].

The White House Administration's approach to homeland security is based on the principles of shared responsibility and partnership with the Congress; state, local and tribal governments; the private sector; the American people; and international partners [58]. Homeland security is coordinated at the White House by the HSC,[30] chaired by the President and led by the Assistant to the President for Homeland Security and Counterterrorism. Together with the National Security Council (NSC)[31] it provides inter-agency coordination of all homeland security-related activities among executive departments and agencies, and promotes the effective development and implementation of all homeland security policies.[32] The Secretaries of Defense and Homeland Security are members of the HSC.

While the DHS was established to oversee the development of US's homeland security capability, the Congress has failed, so far, to pass a homeland security authorization bill [103]. This has hampered DHS's ability to create a multi-Departmental cooperative response network and a homeland security enterprise [103]. The Congress has also yet to authorise an Undersecretary for Policy and Planning within DHS and an associated secretariat to oversee the Department's activities and plans [103]. A review [103] has found that the department needs a high-level office, with appropriate authority: to develop policies that bind the more than 22 federal entities consolidated within the Department; to coordinate with other federal agencies; and to manage international affairs for the Department. Of particular concern is the need to complete a comprehensive strategy for planning and preparing for large-scale national disasters. Shortfalls in this area are attributed to ineffective interagency processes between federal, state and local government and the private sector. "*Accomplishing these tasks requires a DHS leader with suitable rank and scope of responsibility*" [103, p3].

The 9/11 Commission Report recommended the formation of a principal panel in each Chamber of Government (Congress & Senate) responsible for oversight and review of DHS [104]. However these recommendations have not been fully implemented by Congress, and DHS officials have to report to a plethora of committees that offer conflicting and competing guidance. This has resulted in numerous operational mandates imposed on the department, and micro-management of its structure by various congressional committees [103].

As there is no Department of S&T and no central budget for R&D, the task of coordinating policies across agencies is daunting [105]. The Office of Science and Technology Policy (OSTP) in the Executive Office of the President (EOP) was established statutorily in 1976 to provide the President with advice on S&T issues. OSTP leads interagency efforts to develop and

[30] Website http://www.whitehouse.gov/hsc/
[31] Website http://www.whitehouse.gov/nsc/
[32] The HSC does this through its Policy Coordination Committees (HSC/PCCs) that are the main day-to-day fora for interagency coordination. HSC/PCCs are established for eleven functional areas, each chaired by the designated Senior Director from HSC. If the PCC is unable to reach consensus or a more formal imprimatur is needed they will bring the policy proposal to the HSC Principles or Deputies Committee. Other tools include having the President promulgate Executive Orders, memoranda, of Homeland Security Presidential Directives (HSPD) [8].

implement sound S&T policies and budgets. The OSTP endeavours to achieve this through the management of the President's NSTC activities in conjunction with federal agency staff. The NSTC, a Cabinet-level council, is the principal means for the President to coordinate S&T policies across the Federal Government. It establishes national goals for federal S&T investments and prepares coordinated R&D strategies. For example, it issued in 2005 a guideline for S&T for homeland security [106]. The CHNS, established by the NSTC as part of its internal deliberative process, provides advice, guidance and direction on S&T related to homeland and national security [69]. Whilst the OSTP has the lead role, it is regarded as a "*…small office with no budget power.*" [105, p28]

Each year, Departments and agencies determine their budgets separately and submit their proposals to be collated into the President's budget, which is submitted for Congressional approval. The OSTP and OMB (Office of Management and Budget) issue guidelines for budget preparation that include Presidential priorities for national and homeland security R&D [107]. While some of the R&D priorities are cross-agency, most of the approved R&D is mission-oriented; that is, it serves the goals and objectives of the agency that provides the funds [63].[33] The federal government divides the budget into 20 "*functional*" groupings (such as 'defense', 'transportation', 'justice' etc.) to represent these national missions. Although there is much talk of homeland security becoming a major new federal mission, in the 2009 budget the associated spending remains a category that cuts across spending on traditional government missions. R&D in the DHS, for example, serves the three missions of administration of justice, general science, and transportation [63].

Proposed 2009 budget funding of homeland security R&D within the various agencies shows a continuing arrangement whereby the majority of the multi-agency portfolio (roughly 80%) remains outside of DHS, with the largest part in NIH (National Institutes of Health)[34] for its biodefense research portfolio. DoD's homeland security related R&D ($1.5 billion) goes almost exclusively to Defense agencies such as the CBDP and the DTRA. Note that homeland security R&D funding is dominated by the CBRN sub-component of the threat space.

The Homeland Security Act of 2002, which established the DHS, created within DHS a Directorate of Science and Technology, headed by an Under Secretary of Science and Technology. Most (DHS) homeland security R&D is carried out within this Directorate and the Domestic Nuclear Detection Office (DNDO). The directorate was not given a concise statutory mission. Instead, the Homeland Security Act gave the Under Secretary wide-ranging lists of responsibilities and authorities. The current Under Secretary, Admiral Jay Cohen, has summarised his interpretation of the S&T Directorate's multifaceted mission as follows: "*The S&T Directorate's mission is to protect the homeland by providing Federal, State, local and Tribal officials with state-of-the-art technology and resources.*" [108, para6].

The DHS began life with only a few R&D laboratories and programs that it inherited from USDA (US Department of Agriculture), DOE, and DOD, together with a transfer of less than $300 million of programs in 2002. From its foundation in FY 2003 DHS grew rapidly to become the seventh-largest R&D funding agency. Congress has been critical of the S&T

[33] One exception is the National Science Foundation (NSF) that has a broad mission to support basic and applied research, research facilities and education across science and engineering disciplines.
[34] NIH is a part of the Department of Health and Human Services (DHHS).

Directorate's' R&D spending and of its management and performance [62, 109, 110]. Despite changes and cuts, the S&T directorate still had nearly $300 million in unspent funds to carry over to FY 2008. Cohen proposed an extensive restructuring of the DHS R&D portfolio in the 2008 budget request, consolidating many program lines and reshuffling others to create new program portfolios. The FY 2009 budget ($1.033bn in total R&D fund for whole DHS) requests would continue this new structure and would boost funding after two years of retrenchment [63]. The S&T Directorate has a 2009 budget of US$869m, of which US$737m is allocated for R&D.

Consistent with the Homeland Security Act of 2002, the S&T Directorate goals [111] are to:

a. "*accelerate delivery of enhanced technological capabilities to meet requirements and fill capability gaps to support DHS Agencies in accomplishing their mission,*

b. *establish a lean and agile GS-manned,*[35] *world-class S&T management team to deliver the technological advantage necessary to ensure DHS Agency mission success and prevent technology surprise, and*

c. *provide leadership, research and educational opportunities and resources to develop the necessary intellectual basis to enable a national S&T workforce to secure the homeland.*"

DHS is required to coordinate the federal government's civilian efforts in homeland security. In reality, however, this has proven to be a difficult task [62] and the Under Secretary of DHS' S&T Directorate aims to use the CHNS, as well as the Quadrennial Homeland Security Review, to achieve better coordination [64, 65]. The S&T Directorate is to promote R&D and to test and evaluate technologies related to homeland security in cooperation with private companies, academic institutions, and other government agencies. These new capabilities should be made available to operational end users in the DHS and the rest of the federal government and to other public and private actors, including state and local emergency responders.

In the last two years, Under Secretary Cohen has narrowed the Directorate's focus and introduced major restructuring of its R&D management. The Directorate now consists of six technical divisions[36] that are the main performers and funders of R&D. Cross-cutting coordination of the Divisions' activities are provided by three Offices, namely Research, Innovation/Homeland Security Advanced Research Projects agency (HSARPA), and Transition. Other Directorate functions are performed by the Office of Test and Evaluation and Standards; Special Programs; and Agency and International Liaison. The Directorate has 257 full-time equivalent (FTE) management and administration positions of which only 124

[35] GS refers to General Schedule, a name used to describe a pay scale utilized by the majority of white collar personnel in the civil service of the U.S. federal government. The GS includes most professional, technical, administrative, and clerical positions in the federal civil service; and is a way to keep federal salaries equitable among various occupations.

[36] These are the Chemical and Biological; Explosive; Command, Control, and Interoperability; Borders and Maritime Security; Infrastructure and Geophysical; and Human Factors Divisions.

are allocated to research, development, acquisition, and operations. Much of the Directorate's business involves brokering of research[37] on behalf of clients.[38]

To address the congressional criticisms [65], the Directorate has issued its first strategic plan, a five-year R&D plan [112]. The plans introduced the concepts of IPT to better identify the requirements of their clients within DHS. The Directorate has recently updated its S&T strategy [59] with an S&T Strategic framework that explicitly relates the Directorates' goals and objectives to the strategic goals of the DHS.

The S&T Directorate can access a variety of R&D assets to support its research, development, testing and evaluation (RDT&E) activities. These include

a. four DHS-S&T laboratories,[39]

b. eleven DOE national laboratories (e.g. Los Alamos National Laboratory),[40]

c. other government sites (e.g. the Chemical Security Analysis Center (CSAC) at U.S. Army's Edgewood Chemical and Biological Center),

d. FFRDC (Federally Funded Research and Development Centers) such as the Homeland Security Institute (HSI), and

e. seven university centres of excellence (e.g. the Center for Risk and Economic Analysis of Terrorism Events (CREATE), led by the University of Southern California).

DHS has a special statutory relationship with DOE under the Homeland Security Act of 2002. The S&T Directorate can use this authority to engage the DOE national laboratories to perform research for DHS as if they were being tasked by DOE. This authority reduces costs for DHS and gives its tasks equal priority with DOE tasks. Furthermore DOE and DHS have entered created a memorandum of agreement regarding the use of DOE assets by DHS, within which the S&T Directorate has established strategic alignment of lab capabilities to its Divisions' research interests. DHS utilisation of DOE laboratories amounted to 5% of total funding in FY2006, half of which was for the S&T Directorate.

DHS, through its Office of National Laboratories (ONL), is currently developing new laboratory facility infrastructure, and supporting construction elsewhere with DOE and DoD.

The S&T Directorate also conducts some non-R&D activities. Of particular interest is the awarding of scholarships and fellowships as a means to build capacity for future R&D in homeland security [62], although these are being re-aligned with the Universities Centre of Excellence approach.

---

[37] In a January 2007 interview with Innovation Magazine the Under Secretary Cohen states that "*we don't do S&T, we resource and we manage S&T.*"

[38] Under Jay Cohen the cliental has been down-scoped to the operating components of DHS.

[39] These are the Environmental Measurements Laboratory (EML), the National Biodefense Analysis and Countermeasures Center (NBACC), the Transportation Security Laboratory (TSL) and the Plum Island Animal Disease Center (PIADC).

[40] The DOE national laboratories, while government-owned, are managed and operated by contractors.

The DNDO was carved out of the S&T Directorate in 2006 and is now a stand-alone entity within DHS devoted to radiological and nuclear countermeasures.[41] Although much of DNDO's activity is operational, it also funds a substantial amount of R&D, and conducts testing and evaluation. Its basic and applied research portfolio in FY2009 will be US$279m, within a total budget of US$564m.[42]

The Department of Health and Human Services (DHHS) R&D budget for FY2009 is US$30bn, of which US$2.1bn is allocated for homeland security related R&D. The largest component is in the NIH for their biodefense research portfolio. NIH's portfolio, mostly in the National Institute of Allergy and Infectious Diseases (NIAID), totals US$1.86bn in FY2009 [63].

While US federal departments and agencies are mission-oriented, and those involved with national and homeland security are well resourced, there is wide-spread recognition that interagency cooperation is important to achieving national objectives. This is evidenced by references to interagency cooperation within the various strategic documents and plans, as well as Presidential priorities. However achieving greater interagency cooperation and coordination is challenging for the large US federal system [103, 109, and 113]. Nevertheless various programs and initiatives have been introduced to better enable interagency cooperation with varying degree of success. In general this cooperation tries to

a. "*improve the sharing of information,*

b. *identify gaps and reduce redundancies,*

c. *leverage results, outcomes and technologies across agencies, and*

d. *where appropriate share resources to save on costs and improve overall efficiency.*"

The CHNS is co-chaired by the DHS Under Secretary for S&T and the DoD USD ATL. The Charter for the CHNS [69] lists its functions as

a. "*Facilitate planning, coordination, and communication among Federal departments and agencies involved in homeland or national security R&D,*

b. *Help identify, define, and advise the NSTC on Federal priorities and plans for homeland or national security R&D, and recommend options for Federal priorities,*

c. *Review and advise on Federal policy and programs that affect international efforts related to homeland or national security R&D,*

d. *Address, as deemed necessary, technical programmatic and operational issues that affect two or more Federal agencies,*

[41] One apparent motivation for this was Congress's displeasure with the management of the S&T Directorate prior to Cohen's appointment, as discussed above. It also appears to reflect an increase in the priority DHS places on countering radiological and nuclear threats [13].

[42] The difference between the two totals is due to procurement of nuclear detection devices for U.S. ports of entry, management costs, and operations support costs.

e. *Identify and recommend Federal priorities in national security R&D, intelligence R&D, and homeland security R&D and develop options for Federal R&D budget crosscuts, and*

f. *Coordinate with other NSTC committees and facilitate NSTC clearance of documents generated by interagency groups that are established under its aegis.*"

OSTP and OMB annual budget guidelines and presidential priorities [107] explicitly identify R&D areas that require interagency coordination, and urge agencies to "*maximize planning and coordination through participation in applicable interagency coordination groups, especially the NSTC*" [107, p3].

At the working level, there are examples of collaboration across agencies. A recent Defense Science Board task force [70, p1] found cooperative relationships between DHS and DoD to be "*ad hoc, without comprehensive engagement and with fragmented accountability*." The task force found that this resulted in "*gaps, overlaps, and poor integration*" [70, p1]. Moreover the task force recommended that: "*The Deputy Secretaries of DoD and DHS direct that coordination and integration between the two departments be institutionalised through a formal Memorandum of Understanding (MOU) with a scope that includes planning, research and development, acquisition, operations, and training.*" [70, p2]

The previous paragraphs describe the general nature of interagency processes between DHS and other federal departments. The following details some of the specifics, focusing on those that facilitate cross-agency tasking and sharing of resources.

TSWG is an "*interagency research and development program for combating terrorism requirements at home and abroad*" [114]. Organizationally TSWG "*operates as a program element under the Combating Terrorism Technical Support Office (CTTSO)*" [114, para1]. The program office CTTSO works closely with numerous agencies, organizations and first responders to "*field rapid combating terrorism solutions to meet continually evolving requirements defined by end users*" [115, para1]. The CTTSO operates under the Assistant Secretary of Defense (ASD) for Special Operations and Low-Intensity Conflict and Interdependent Capabilities (SO/LIC & IC).

The TSWG comprises of a number of subgroups that "*addresses a technical specialty to meet requirements across the four pillars of combating terrorism: antiterrorism, counterterrorism, intelligence support, and consequence management. External Federal agencies*[43] *appoint senior technical experts to participate as chair persons for the subgroup.*" [114, para2] While the primary focus of the TSWG is rapid prototyping, the overall aim is to transition products to end users. "*Each subgroup maintains an extensive online repository of products, technologies, and publications that are available to Federal, State, and local government agencies and the first responder community.*" End users and agencies participates in the subgroups to "*…work together to generate requirements, fund projects, and lend technical expertise to monitor program development.*" [114, p1]

The core funding of TSWG is provided predominantly by the DoD, with additional funding supplied by the Department of State. Other government departments and agencies "*share the costs of selected projects. Core funding is apportioned across subgroups to provide the resources necessary to fund projects that satisfy combating terrorism requirements.*" [114, para4]

[43] Agencies other than DoD

1401 TTP. In general the DoD is prohibited from developing capabilities exclusively for first responder use [66]. However the DoD does develop technologies that may be of use to first responders, and in fact does purposely develop dual-use technologies. These technologies could be made available to other agencies through the 1401 TTP. [66] states that Section 1401 of the Bob Stump National Defense Authorization Act for FY 2003 required the Secretary of Defense to designate a DoD senior official to coordinate DoD effort to identify, evaluate, deploy, and transfer DoD technologies and equipment to Federal, State, and local responders technology, items, and equipment in support of homeland security. This program is run by a team comprising DoDHD & ASA (DoD Homeland Defense and Americas' Security Affairs), the DHS S&T Directorate and the DOJ's (Department of Justice) National Institute of Justice Science and Technology. [66] defines 'Technology transfer' is the intentional provision of knowledge, expertise, facilities and equipment and other resources for application to military and non-military systems. Under this program DoD can enter into a cooperative R&D agreement with DHS, DOJ, other Federal agencies, State or local agencies, non-government organizations, and private sector enterprises to purse specific projects. The program does not provide funds to purchase technology or equipment for first responders.

The DOE laboratories and technology centres operate under a special arrangement known as a Management and Operating (M&O) Contract. Through this arrangement the government contracts for the operations, maintenance, or support of a government-owned-or-controlled research, development, special production, or testing establishment. The DOE laboratories and technology centers are available to conduct work for other federal agencies on a full cost-recovery basis through a program known as Work for Others (WFO) [116]. Such projects must support the missions of DOE and the laboratory or technology centre and may not compete directly with capabilities that are available in the US domestic private sector. The program operates with the following objectives [116]:

a. "*accomplish research or technology goals that may otherwise be unattainable, and avoid unnecessary duplication of effort,*

b. *access highly specialized or unique facilities, services, or technical expertise,*

c. *transfer technologies from DOE laboratories and technology centres to the marketplace for further development or commercialisation, and*

d. *maintain core competencies and enhance the S&T base at DOE facilities.*"

The program serves as a bridge connecting all of the country's research communities, universities, industries, and federal, state, and local governmental agencies [116]. While the program realizes cost savings by using existing technologies and facilities, reciprocal benefits to DOE include enhanced skills, expertise, and application of the technological advances to ongoing and future DOE programs. One should note that the program does not take precedence over DOE's objectives and priorities. Note that DHS's relationship with DOE laboratories is different to WFO and DHS is able to task DOE resources directly with the same authority and priority as DOE [62].

The H.R. 4290 Homeland Security Technology Advancement Act directs the Under Secretary for S&T Directorate to: "*make available to any person or entity, for an appropriate fee, the services of*

any DHS owned and operated center or other facility for the testing of materials, equipment, models, computer software, and other items designed to advance the homeland security mission…" provided this does not interfere with government use [117].

Introduction of the Homeland Security Management System builds upon the current focus on doctrine and planning through the National Preparedness Guidelines (NPG). National efforts are aligned under this approach by using national planning scenarios and the associated capabilities that must be developed or maintained by various level of government. "*In this manner, the NPG constitutes a capabilities-based preparedness process for making informed decisions about managing homeland security risk and prioritizing homeland security investments across disciplines, jurisdictions, regions, and levels of government, helping us to answer how prepared we are, how prepared we need to be, and how we prioritize efforts to close the gap.*" [2, p43]

The Strategy explicitly acknowledges S&T as "*an essential and enduring enabler*" [2, p49], but it does not articulate how S&T might be used to support the Homeland Security Management System.

Many US documents on homeland and national security advocate the use of risk to inform planning and decision making. The national strategy [2] states that "*the assessment and management of risk underlies the full spectrum of our homeland security activities, including decisions about when, where, and how to invest in resources that eliminate, control, or mitigate risks …We must apply a risk-based framework across all homeland security efforts in order to identify and assess potential hazards (including their downstream effects), determine what levels of relative risk are acceptable, and prioritize and allocate resources among all homeland security partners, both public and private, to prevent, protect against, and respond to and recover from all manner of incidents*." [2, p41]

The DHS S&T Directorate have already taken steps to adopt a risk-based approach. These steps include its support of a FFRDC known as the HSI. The HSI assists the directorate in addressing homeland security issues that require scientific, technical, and analytical expertise. The HSI is to provide effective and independent analysis of DHS programs by applying systems analysis and evaluation; and to support decisions and guide investment using a risk-based approach. Yet despite exposure to these sources of risk expertise, a recent review found that the DHS's risk-based approach lacks consistent application of tools and methodologies [70]. The same review [70, p3] also found that the DoD is "*far from practicing a risk-based approach*."

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Defence Science and Technology Support for National Security: An International Review

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Rick Nunes-Vaz and Leung Chim

5. CORPORATE AUTHOR

Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TN-0888	AR-014-513	Technical Note	May 2009

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2008/1144627/1	07/239	DSTO	52	117

13. URL on the World Wide Web

http://www.dsto.defence.gov.au/corporate/reports/DSTO-TN-0888.pdf

14. RELEASE AUTHORITY

Research Leader
Counter Terrorism and Security Technology Centre, DSTO, Edinburgh

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DEFTEST DESCRIPTORS

Literature surveys, Science and technology management, Defence policy, Science policy, Defence White Paper 2009

19. ABSTRACT

A critical review of open source literature enables comparison of the US, UK and Canadian approaches to the development, coordination and harnessing of science and technology for national security capability, the mechanisms by which science and technology (S&T) support is harnessed, and the relative roles of Defence and non-Defence S&T providers. The review was undertaken to inform the S&T Companion Review to the Defence White Paper, by contextualising Defence S&T contributions to national security goals outside strict support of Defence objectives. This document describes the (mid-2008) status of S&T input to the national security systems of the US, UK and Canada. Its purpose is to inform attempts to improve Australian arrangements, based on lessons learned overseas, and to help generate a longer-term vision for S&T support to whole-of-nation strategic challenges, such as national security.

The analysis shows that Canada and the UK and, from a low base, the US, are all moving to increase the application and integration of niche Defence S&T capability into national S&T programs for counter-terrorism and national (or homeland) security. Defence S&T is seen increasingly as a unique, and critical component of the national response, and one that should not be quarantined for Defence needs alone. Primary insights indicate that there is: increasing effort to improve the alignment and consistency of policies and strategies for (a) national (or homeland) security, (b) national innovation, S&T, and (c) Defence S&T; growing acknowledgement of the critical national role of niche Defence S&T capabilities; greater strategic coordination of national security capability management supported by national security S&T providers, including Defence; growing recognition of the need to overcome departmental stovepipes, particularly the military/civilian divide; growing use of programmatic (or problem-based) approaches to funding, development, management and exploitation of S&T in national security; and an increasing focus on cross-Departmental collaboration, information sharing, and the promotion of enduring S&T "communities of practice".