CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES
NSSC 7 - CESN 7

A Science and Technology Strategy for Public Security

The Paradigmatic Paradox

Camille A. Boulet

INTRODUCTION

On September 11th, 2001, at approximately 08:46, American Airlines Flight 11 hit the north tower of the World Trade Center in New York City. Eighteen minutes later, United Airlines Flight 175 struck the south tower and at 09:37, American Airlines Flight 77 crashed into the Pentagon in Washington DC.[1] Fearing further attacks and uncertain as to the status of other flights, at 09:45, the United States Federal Aviation Administration closed the airspace over the United States with approximately 500 aircraft inbound from around the world. The terrorist attacks were horrifying and their devastating impact felt immediately around the world as the collapse of the World Trade Center towers was broadcast live. In this war, Al-Qaeda was the first to use "shock and awe" tactics by attacking directly the heartland of their enemy, the United States of America.

Canada was now faced with the task of diverting 270 flights with sufficient fuel to return to their origins as well as accommodating 234 flights and 33,000 passengers at Canadian airports across the country.[2] Operation Yellow Ribbon, as the Canadian operation was known, was a test of Canada's emergency response capability and clear evidence of how the impact of a catastrophic terrorist event could quickly expand beyond any nation's borders. The new global, fanatical terrorists had launched their first major attack against the United States (U.S.) on its own territory and Canada was one of the first nations to understand the immediate security implications of this new world order.

The events of September 11th, 2001 and the subsequent anthrax letter attacks launched through the U.S. postal system were watershed moments in Canadian, North American, and international security. Never before had the need to protect and even defend national security in a domestic context against the threat of terrorism been so visceral and real. Yet global extremist and fanatical religious terrorism did not have their "coming out party" in the fall of 2001, these were anticipated and visible trends in national and international security for many years.

---

[1] The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, W.W. Norton & Co., New York, NY, 2004.

[2] Transport Canada Chronology accessed at http://www.tc.gc.ca/majorissues/transportationsecurity/Chrono.htm

The August 2001 edition of *Jane's Intelligence Review*, published the month before the World Trade Center attacks, had for its cover headline **Cutting Al-Qaeda Down to Size**. [3] That edition of *Jane's* featured two articles, one examining the Al-Qaeda network[4] and the other reporting on the trial of the four Al-Qaeda terrorists convicted of the 1998 bombings of the U.S. Embassies in Nairobi and Dar es Salaam.[5] In a side bar article, tactical insights from the trial on Al-Qaeda plans included the claim that the embassy attacks "would pave the way for attacks in the USA." More chilling was the comment that the Al-Qaeda training included "the use of chemicals, poisons and toxins" for assassination and "some individuals were sent to specialist schools for training in electronics and flying aircraft." The embassy bombings in Africa and other attacks against U.S. interests in Saudi Arabia, the USS Cole attack, and even the first attempt on the World Trade Centre were all part of the same, ongoing asymmetric war waged by these "new" terrorists, fundamental religious extremists.

There were already substantial concerns about the ongoing proliferation of Weapons of Mass Destruction (WMD) prior to the anthrax letter attacks in the fall of 2001.[6] The Tokyo subway attack in March of 1995 had already shown that a dedicated group, in this case a fanatical religious cult, could develop, produce, and employ a chemical warfare agent and achieve the anticipated effects of horror, panic, and fear. The events of 2001 however were the more significant impetus that moved up the need for a national security strategy that recognized the realities of this new global security environment.

What characterizes "9/11", and other high-consequence terrorism attacks, is that they have an almost disproportionate impact across large segments of public and private activities, the rapidly expanding national consequences, and immediate international implications for security. The shock, fear, and stress caused by such events extended well beyond the

---

[3] Cover Headline, *Jane's Intelligence Review*, 13, no. 8 (August 2001).

[4] Rohan Gunaratna, "Blowback." *Jane's Intelligence Review*, 13, no. 8 (August 2001) p 42.

[5] Phil Hirschkorn, "Convictions Mark First Step in Breaking Up Al-Qaeda Network." *Jane's Intelligence Review*, 13, no. 8 (August 2001) p42.

[6] There has been considerable speculation as to whether or not these anthrax attacks were truly "terrorism" or a criminal act that resulted from other motivations. The issue is moot as the effects, and the necessary public security implications are the same regardless of the intent or identity of the perpetrators.

immediate target area and the directly affected populations in Manhattan, New York City, or event the U.S. "The most important factor driving terrorism's 'multiplier effect' is the psychological effect it has on people far removed from the incident itself. Terrorism evokes a sense of horror, indignity, and vulnerability – the last being especially powerful."[7] These events simultaneously challenged public safety, security, and emergency response authorities and responsibilities across municipal, state, or federal jurisdictions within the United States. In Canada, analogous levels of government from Transport Canada, the provinces where planes were landed, to the cities that hosted the passengers, were involved in the response. The response was inherently inter-agency requiring close coordination and cooperation for effective crisis and consequence management. These events have a high impact across multiple dimensions such as the high levels of potential casualties, the economic impact of catastrophic events, political response, environmental impacts, and the vulnerability of public confidence.

Two of the largest transformational reorganizations in government occurred in Canada and the U.S. as a direct result of the events of 2001 and new security environment that these terrorism attacks created. Canada saw the pronouncement of the so-called Public Security and Anti-terrorism (PSAT) budget which committed C$7.7 billion over five years to enhancing national security, the formation of a new department for public safety, the appointment of its first national security advisor, and the release of its first national security policy. The U.S. was to undertake one of its largest federal reorganizations in history with formation of the Department of Homeland Security. Within a continental security context, Canada and U.S. entered into a "Smart Border Accord" to ensure that significant economic imperatives and national security concerns could be addressed and managed. Prominent in these transformations has been the role of science and technology (S&T) as existing technologies were implemented to immediately improve security and as a driver for future systems.

The Paradigmatic Paradox

[7] Falkenrath p171

This paper addresses the emergence of public security as a critical mission for government and in particular the strategic role that S&T can play in addressing national, bi-national, and international priorities to combat security threats. It will outline a leadership role that defence science in Canada has played in the development of a public security S&T base to ensure a capable, timely, and meaningful response, as well as an S&T strategy, based on a common approach to assessing risk and establishing shared outcomes, to support Canada's national security capability requirements. A review of the development of national and international programs is included to document the development this new and emerging area of national and international S&T policy and collaboration.

At the centre of this paper is a "paradigmatic paradox", a paradox that arises from a public security system that is now engaged in asymmetric warfare against a new form of terrorism, an activity normally reserved for defence and military forces. The asymmetric nature of the war waged by fanatical terrorists itself defies conventional military planning processes and has already had a transformational effect on military planning, resulting in, as will described later, a paradigm shift in military threat assessment models. For the public security system involved in this war on terrorism, there are really no existing paradigms, thus best practices and experience should be recognized because they are applicable and constructive within the broader public security environment and should be embedded in the development of an effective strategy and response.

The intent of this essay is to demonstrate how a S&T strategy can contribute to public security by providing strategic direction in developing a shared approach to understanding the risk in this new security environment. By systematically assessing the risk and vulnerabilities, gaps in capabilities can be identified and research and development (R&D) programs can be targeted to provide critical solution. The S&T community, through the development of a capability based approach can assist in ensuring that Canada can best address prevention, preparedness, and response to current, anticipated, and most importantly the unanticipated security challenges. The essay will not argue that technology in itself is the only approach to ensuring public safety but that it is a key component of a long term, viable strategy.

Public security in this age of global terrorism is being driven in large measure by the vulnerability to, and consequences of, the possible use of weapons of mass destruction (WMD), chemical, biological, radiological and nuclear materials and weapons, by increasingly fanatical, extremist terrorist organizations and networks. This shift from largely state-based threats to a more undefined, amorphous, and non-quantifiable risk requires an re-evaluation of the use of threat assessment for planning and a shift towards risk assessment as the foundation for prevention, preparedness, and response. An understanding of how to assess risks, vulnerabilities, and gaps is needed to ensure that an S&T program, from conception through policy, strategy development and finally implementation, can be put in place to provide outcomes that have a measurable effect in improving security.

The impetus for this paper arises from the leadership and innovative position Defence R&D Canada (DRDC) has assumed with respect to developing an S&T strategy to support public security. Its 2003-2004 Annual Report is entitled *Protecting Our World in Uncertain Times*, reflecting the increased importance of national defence and public security and the role that defence science can play in supporting Canadian national security and security partners.[8] Science in support of security is a broader mission that recognizes the traditional target of defence and military affairs but broadens the horizons for research and development to include the public requirements for security. Defence R&D Canada has led the federal innovation system in developing the first "horizontal" S&T initiative, a program involving multiple departments and agencies with a common requirement in public policy, to address chemical, biological radiological or nuclear terrorism with the CBRN[9] Research and Technology Initiative (CRTI) and the implementation of the Canada – U.S. Public Security Technical Program (PSTP).

[8] Canada. Defence R&D Canada, *Annual Report 2003-2004: Protecting Our World in Uncertain Times*, (Ottawa: Defence R&D Canada, 2004).

[9] CBRN: Chemical, Biological, Radiological/Nuclear

The terms "superterrorism"[10] and "catastrophic terrorism"[11] have been coined to describe a new form of terrorism where there would effectively be a quantum leap in the terror potential should a chemical, biological, radiological, nuclear, or explosive (CBRNE)[12] material be employed.[13] The associated security concern has been the proliferation of CBRNE materials, technologies, and the necessary knowledge needed for their effective employment by terrorists with potentially catastrophic effects. Inherent in the use of these terms is a terrorist mindset that would want to employ these materials specifically to produce casualties on a scale never seen before with more "conventional" terrorist attacks such as small scale bombings, hijackings, or armed attacks. This "new" terrorism is at the core of the national and international security concerns articulated in Canadian, U.S. and European security policies and strategies. Fanatical religious terrorism is an increasingly significant and distinct form of terrorism and the examination of this emerging form of terrorism forms a body of considerable literature and scholarship that is extensively examined elsewhere. As religious extremism and the proliferation of weapons of mass destruction are at the core of the national security policy an appreciation of how these shift strategic planning from a threat-based system, where preparedness is based on specific information on intent, to a risk-based system that examines probabilities, is integral to the discussion.

[10] Yonah Alexander, "Superterrorism: A Global Threat," *World & I* 86, no.3 (June 1993): 86-92.

[11] Ashton Carter, John Deutch, and Philip Zelikow, "Catastrophic Terrorsim: Tackling the New Danger," Foreign Affairs 77, No.6 (November/December 1998): 80-94.

[12] Within this essay the term "CBRNE" will be used instead of Weapons of Mass Destruction (WMD except where it part of the original material or concepts being cited from other works. While convenient as a form of shorthand and frequently used in the literature, in the context of this essay that is advocating a more rigorous risk analysis and the systematic development of cross cutting prevention, preparedness, and response capabilities, WMD implies effects and consequences at only one end of their spectrum of employment. Traditionally, WMD has only included chemical, biological, or radiological nuclear materials however here explosive are included in recognition of the destructive power that explosive, incendiary devices had on September 11, 2001 and an emerging hazard posed by novel explosives such as thermobaric bombs (David Hambling, Preparing for the Worst*," NewScientist*, 20 March 2004, 8-9.

[13] It is beyond the scope of this essay to provide a complete review the technical nature of the, their physical, chemical or toxicological properties, their production methods, or weaponization technologies. Similarly the increasing concerns over the proliferation of these hazards is examined in an extensive and ever growing literature on chemical and biological terrorism for which leading references have been provided in the bibliography.

It is the confluence of the new fanatical, extremist terrorism and the interests in CBRNE weapons by terrorists that is of significant concern.[14] Terrorist studies specialists such as Walter Laqueur believe that the use of weapons of mass destruction by the contemporary, fanatical terrorist is inevitable.[15] As Laqueur states "It is only question of time until radiological, chemical, or biological weapons will be used more or less systematically by terrorists; the first steps in this direction have been made" and that restraints, if there were any self-imposed by terrorist are "weaker or no longer existent". He concludes now that "if the nineteenth-century terrorism was the era of 'propaganda by deed', the twenty-first century could be the age of catastrophic terrorism."[16]

Under the *Criminal Code of Canada*, "terrorism" is "an act or omission, in or outside Canada, that is committed in whole or in part for a political, religious or ideological purpose, objective, or cause and in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security."[17] Terrorism thus by definition is designed to attack and defeat personal, societal, economic, and even governmental systems therefore one should not *a priori* assume that any existing system is invulnerable to a terrorist attack. It is also neither practical nor prudent to allow the "negative stakeholders", the terrorists in society identify any vulnerability in existing systems through their actions or attacks. The challenge is for the "positive stakeholders", such as national governments and international security organizations, to examine the system, its vulnerabilities, and develop a comprehensive strategy to ensure that public security is achieved. Particularly important will be the need for sound strategic and operational level decision making and in the context of this essay, the role that strategic S&T planning can

[14] The assessment that there is a growing threat from this new terrorism and the use of CBRNE weapons is not universally accepted. Richard Falkenrath, writing in the Spring 2001 *International Security* issue characterized two schools of opposing thought: the first essentially believes that terrorism in itself is not a sufficient threat to U.S. national security while the second school believes that terrorism is a threat but that it is mostly conventional in nature. "Problems of Preparedness," *International Security* 25, no. 4 (Spring 2001):147-186.

[15] Walter Laqueur, *No End to War: terrorism in the twenty-first century* (New York: Continuum, 2003), 226, 227, 231.

[16] Walter Laqueur's opinion has changed dramatically as a result of the new terrorism. His assessment in 1977, referring to CB weapons, was that "it can be taken for granted that most terrorist groups existing at present will not use this option, either as a matter of political principles or because it would defeat their purpose." Walter Laqueur, A History of Terrorism (New Brunswick, N.J.: Transaction, 2002): p231.

[17] Canada. Department of Justice. Criminal Code Part II.1 Terrorism; http://laws.justice.gc.ca/C-46/41918.html; Internet; accessed 2 April 2005.

play in assisting other national security partners in transforming to respond to the national security environment is considered.

PUBLIC SECURITY AND PUBLIC SECURITY SCIENCE &TECHNOLOGY

"In the war against terrorism, America's vast science and technology base provides us with a key advantage."

President George W. Bush, June 2, 2002[18]

"*The United States has a critical need for cutting-edge technology that can quickly and effectively detect, analyze, facilitate interdiction of, defend against, defeat, and mitigate the consequences of WMD*."

National Strategy to Combat Weapons of Mass Destruction, December 2002[19]

Public Security in Canada and the United States

In Canada, the federal response to the terrorist attacks of 9/11 was captured in the "Public Security and Anti-Terrorism" (PSAT) budget of December 2001.[20] This budget outlined C$7.7 billion of measures over 5 years intended to address immediate requirements for national security and "enhance personal and economic security by keeping Canadians safe, keeping terrorists out of Canada and keeping Canada's borders secure, open and efficient." $6.5 billion of investments were directed towards improvement of air security, intelligence and policing, and border security enhancements. $1.6 billion was allocated to emergency

[18] United States. The White House. *The Department of Homeland Security*. Washington, D.C.; June 2002; available from http://whitehouse.gov/homeland/book/nat_strat_hls.pdf; Internet; accessed 2 April 2005.

[19] United States. The White House. *National Strategy to Combat Weapons of Mass Destruction*. Washington, D.C.: July 2002; available from http://www.whitehouse.gov/news/releases/2002/12/WMDStrategy.pdf; Internet; accessed 2 April 2005.

[20] Canada. Department of Finance. "Budget 2001: Securing Progress in an Uncertain World," http://www.fin.gc.ca/toce/2001/budlist01_e.htm; Internet; accessed 1 April 2005.

preparedness, improvements to the protection of Canadian infrastructure, and to "support Canadian military participation in the international war on terrorism." This budget also allocated $170 million to "improve laboratories and purchase specialized equipment to strengthen Canada's ability to respond to chemical, biological and nuclear threats." The specific enhancements and comprehensive strategy to improve Canada's response to CBRN threats includes international collaboration, particularly amongst G8 nations on proliferation control measures, improvements to domestic security and intelligence, disease surveillance, and health security measures such as National Emergency Stockpile System.[21]

In June of 2002, U.S. President George Bush proposed the creation of the Department of Homeland Security.[22] The requirement for the new department was based on the recognition that the "responsibilities for homeland security are dispersed among more than 100 different government organizations" and that this "confusing patchwork of government activities" needed to be focused into a single department. This new department would have four divisions: Border and Transportation Security; Emergency Preparedness and Response; Chemical, Biological, Radiological and Nuclear Countermeasures; and Information Analysis and Infrastructure Protection. Integral to this department was the recognition of the role that S&T could have in supporting the mission preventing attacks, reducing vulnerability, and minimizing consequences should an attack occur.

The U.S. Department of Homeland Security was itself established in March of 2003. It brought together a number of federal agencies and departments organized into functional areas. Border and Transportation Security incorporated the Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement. Emergency Preparedness and Response built on the Federal Emergency Management Organization, and the U.S. Citizenship and Immigration Services, the U.S. Coast Guard and the U.S. Secret Services also comprise significant DHS Agencies. Among the subcomponents was the visible inclusion of the Directorate of Science and Technology to

[21] Public Security and Emergency Preparedness Canada, "Responding to CBRN Threats: A Federal Perspective, February 2003," http://psepc-sppcc.gc.ca/publications/nationa_security/pdf/CBRN_Backgrounder_e.pdf; Internet; accessed 1 April 2005.

[22] United States. The White House. The Department of Homeland Security, Washington: Government of the United States of America, June 2002; http://www.dhs.gov/dhspublic/theme_home1.jsp; Internet; accessed 18 March 2005.

serve as the "primary research and development arm" to " provide federal, state, and local officials with the technology and capabilities to protect the homeland".[23]

In Canada, the creation of the Public Safety and Emergency Preparedness portfolio, the strengthening of the profile of security within government and cabinet by putting responsibility for security in the hands of the Deputy Prime Minister, and the naming of a National Security Advisor were immediate, visible, and significant responses to the 2001 terrorism.[24] Consolidating the former Department of the Solicitor General, the Office of Critical Infrastructure and Emergency Preparedness, and the National Crime Prevention Centre created the Department of Public Safety and Emergency Preparedness Canada (PSEPC).

> "*The most fundamental role of Government is the protection of its citizens. When the Prime Minister created the Department on December 12, 2003, the Government of Canada took a critical step towards strengthening the safety and security of Canadians, their communities and our country*."[25]
>
> Honourable Anne McLellan
> Deputy Prime Minister and
> Minister of Public Safety and Emergency Preparedness Canada.

The Minister is also responsible for a broader security portfolio that includes the Royal Canadian Mounted Police and the Canadian Security Intelligence Service, the Canada Firearms Centre, and the Canadian Border Services Agency and for establishing the strategic priorities for and coordination of the portfolio agencies.[26]

---

[23] United States. Department of Homeland Security, Washington: Department of Homeland Security: Department Subcomponents and Agencies. http://www.dhs.gov/dhspublic/; accessed 18 March 2005.

[24] Canada. Public Safety and Emergency Preparedness Canada. News: Legislation to Establish Department of Public Safety and Emergency Preparedness Introduced. http://www.psepc.gc.ca/publications/news/20041008-2_e.asp; Internet; accessed 9 February 2005.

[25] Canada. Public Safety and Emergency Preparedness Canada.

[26] The PSEP portfolio also includes the National Parole Board. Among the other "progressive" measures to improve public safety, security and emergency preparedness, beyond the establishment of PSEPC and the publication of a National Security Strategy, the Government identifies such "hallmark" approaches creating a National Security Advisor to the Prime Minister, a Cabinet Committee on Security, Public Health and Emergencies, a National Security Committee of Parliamentarians, and Advisory Council on National Security, a

In April 2004, the Government of Canada issued *Securing an Open Society: Canada's National Security Policy*, the "first-ever policy of its kind in Canada."[27] The policy focused on three key objectives:

1. *Protecting Canada and Canadians at home and abroad;*
2. *Ensuring Canada is not a base for threats to our allies; and*
3. *Contributing to international security.*

The National Security Policy (NSP) outlines an integrated approach to protect Canadian sovereignty against the new challenges of global terrorism but also other threats to the security of Canadians from rapidly spread, global pandemics such as Sudden Acute Respiratory Syndrome (SARS). The NSP identifies eight current threats to safety of Canadians and Canadian Society. These threats are terrorism, the proliferation of weapons of mass destruction, failed and failing states, foreign espionage, natural disasters, critical infrastructure vulnerability, organized crime, and pandemics, Terrorism is given particular attention and religious extremism, violent secessionist movements, state-sponsored terrorism, and domestic extremism are examples of motivation for terrorism acts. This point is emphasized in the NSP by the attacks in Madrid, Bali, and 9/11. The proliferation of weapons of mass destruction is particularly singled out, as "the impact on our security could be immense. The physical effects of such attacks would not respect borders and would have a significant impact on the global economy." The catastrophic potential for mass casualties is implicit to these attacks.

The approach is to build an integrated security system, able to respond to the current security environment but to also be sufficiently flexible to accommodate both intentional terrorism events and unintentional pandemic outbreaks as well as adapt through continuous learning and improvement. The NSP broadly outlines four capability targets: threat assessment, protection and prevention, consequence management, and evaluation and oversight. Key measures include the appointment of a National Security Advisor, enhancing Canada's

---

Cross Cultural Roundtable on National Security and a Federal-Provincial-Territorial Forum on Emergency Preparedness. http://www.psepc.gc.ca/publications/news/20041008-2_e.asp#PSEPC

[27] Canada. Privy Council Office, Securing an Open Society: Canada's National Security Policy (Ottawa: 2004)

intelligence collections capacity, and the establishment of a Government Operations Centre to co-ordinate emergency planning and management. Public health security is given greater visibility through the creation of the Public Health Agency and a Chief Public Health Officer for Canada. Transport security, cargo, aviation and marine security in particular are strengthened thorough certain specific measures.

The NSP also identifies the first areas of S&T investment to counter the security threats. Table 1 provides a summary analysis of NSP stated goals or objectives and the technologies required to achieve that goal. In some instances, there is an explicit statement of the technologies targeted for investment (e.g. CBRN response equipment, high frequency surface radar, or biometric systems) while in other instances such as all source threat information integration or the development of an integrated national support system, the S&T contributions are more implicit requiring the involvement of the science community to identify requirements and develop standards.

Table 1: Selected examples of S&T contributions or foundations to NSP Priorities

NSP Priority	Requirement	Technology
Threat Assessment and Intelligence	All source threat information integration	Real time data fusion and Integration
	Threat Information Sharing	Robust secure communication networks
	Threat Assessment Center	Co-operative decision making and support tools
Emergency Planning and Management	Modern integrated national support system	Interoperability standards for training, response, communications and equipment
	Critical Infrastructure Protection	Interdependency Modeling
		Improved materials
	Cyber security	Secure Network architectures
Public Health Emergencies	Enhanced Laboratory Capacity	Rapid diagnostics
	Disease Surveillance	Global Public Health Intelligence Network
		Canadian Public Health Intelligence Network
Transportation Security	Threat Detection	Advanced explosive detectors
	Marine Security & Surveillance	High-Frequency Surface Wave Radar
	Cargo tracking and inspection	Transponders, radiological screening systems
Border Security	Terrorist interdiction	Biometrics/facial recognition systems
	Document Integrity	Secure document systems and information sharing

	Integrated Border Enforcement teams	Secure communications, integrated and common operating picture

Science and Technology Response and Public Security: National, Bi-National International Security Research and Collaboration

CBRN Research and Technology Initiative (CRTI)

Within Canada, strategic science policy leadership over the last decade has changed how the federal S&T community responds to a national priority and represents a significant shift in roles for federal S&T from one of supporting the development of government policy to a more active role of leading the nation's innovation system to address a national priority. Underpinning this policy is a strong, community building approach to ensure the broadest possible response to the public security and safety S&T objective.[28] In *Towards a Shared Vision for Federal S&T*, based on goals established at the 2002 Federal Science and Technology Forum, several principles were established as part of the overall vision.[29] The outcomes of implementing this vision are expected to "contribute consistently to the development of better policies and delivery of superior services throughout the Government of Canada."

These principles include:

> *The Canadian federal Public Service will enhance its research, development, and science services in order to secure Canada's place as a world leader in innovation, opportunity and quality of life.*
>
> *The Government of Canada's S&T efforts will identify emerging issues that matter to Canadians and refocus, in response to changing needs in areas such as health and safety, public security, natural resources and the environment, and the growth of the knowledge economy*.

The CRTI was funded in the PSAT budget to address the S&T requirements of national security related to CBRN preparedness. It is a joint, interdepartmental initiative between 15

---

[28] Camille A. Boulet. *Development of an S&T Response for CBRN Terrorism: The Canadian CBRN Research and Technology Initiative*, Science and Technology Policies for the Anti-Terrorism Era, Proceedings of the NATO Advanced Research Workshop, Manchester, UK, 2004 (in press).

[29]Canada. Industry Canada. *Science and Technology Advice: A Framework to Build On. A Report on Federal Science and Technology 2002.* (Ottawa: Industry Canada Communications and Marketing Branch) 2002. available at www.innovation.gc.ca/s-tinfo.

science-based departments and agencies, security based departments, and central agencies to strengthen Canada's preparedness for, prevention of, and response to a CBRN attack by fostering new investments in research and technology.[30] Initially funded with a five year, C$170 million budget, it specifically targets CBRN terrorism by addressing capacity, knowledge, science, and technology gaps.[31]

Smart Border Accord

Internationally there is increasing and significant attention being placed on the role of S&T can play with respect to enhancing public security. The U.S. *National Strategy for Homeland Security* [32] describes the four foundations that support the national security requirements; law, S&T, information sharing and systems, and international cooperation. By integrating and consolidating federally funded security research, engaging the innovation system and the private sector, the research and development program would invest in and develop "revolutionary capabilities." The U.S. Strategy also recognises that the increased global and trans-national nature of terrorism requiring international cooperation to improve domestic security overall. Among the nine major initiatives are the creation of "smart borders" and the amplification of "international cooperation on homeland security science and technology."

On December 12, 2001, Canada and the U.S issued their "*Smart Border Declaration: Building a Smart Border for the 21st Century on the Foundation of a North American Zone of Confidence.*"[33] This declaration, and its initial 30-point Action Plan, had four major pillars:

---

[30] At its inception, the CRTI program was limited to CBRN hazards. It was considered at the time that other security and S&T programs were adequate to deal with explosive hazards but subsequent risk analysis studies utilizing the risk assessment methodology described later in this essay have shown that there are considerable vulnerabilities and capability gaps. Explosives will be included in future programs and possibly within the CRTI renewal request to the Treasury Board of Canada.

[31] For more information and project details see www.crti.drdc-rddc.gc.ca

[32] United States. Office of Homeland Security. National Strategy for Homeland Security, Washington: Government of the United States of America, July 2002; available from http://www.dhs.gov/dhspublic/theme_home1.jsp; Internet; accessed 18 March 2005.

[33] Canada. Department of Foreign Affairs and International Trade. http://www.dfait-maeci.gc.ca/can-am/; Internet; accessed 24 March 2005.

1. *The Secure Flow of People*
2. *The Secure Flow of Goods*
3. *Secure Infrastructure*
4. *Coordination and Information Sharing in the Enforcement of the Objectives*.

Two additional points, Biosecurity and Science and Technology Cooperation would be added later. In Point 31, *Biosecurity*, a bi-national working group was established to develop an action plan that would address "shared risks to the food supply, to human, plant and animal health, and to the environment on which these depend." Point 32, *Science and Technology*, acknowledged that an agreement in principle had been reached to "enable any Canadian federal government agency to engage in co-operative research and development with any U.S. federal agency in the area of critical infrastructure protection and border security." This later point recognized that to date collaborative agreements had been largely structured on national defence imperatives between respective defence departments and the expansion of the collaboration to all security partners and sectors was needed.

The Canada-U.S. Public Security Technical Program

In December 2002, U.S. Governor Ridge and Canadian Minister Manley agreed to expand the Canada-U.S. Smart Border Accord to include an element to address S&T as it contributes to the nations' mutual border security. Consistent with the scope of the Accord itself, a broad and holistic view of border security and its S&T dimensions has been taken, one that is not uniquely focused on the security of a physical perimeter. The effort to establish the program was led by the U.S. Department of Homeland Security's Science and Technology Directorate and DRDC. In June 2004, U.S. Under Secretary of State for Global Affairs Paula Dobriansky and Canadian Ambassador to the U.S. Michael F. Kergin signed the "*Agreement for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security*". To enable the collaboration under this agreement, the Public Security Technical Program (PSTP) has been established "*to enhance our mutual capabilities in public security*

by collaboratively delivering S&T solutions". The CA U.S. Bi-national PSTP[34] will have four strategic outcomes:

- S&T Support & Advice: provide timely and relevant S&T support and advice to public security policy, operations and readiness;
- R&D and Technology Demonstration: close knowledge gaps, enable interoperability and reduce risk in the acquisition of new and improved national capabilities;
- S&T Foresight: Anticipate emerging and future public security threats and develop appropriate mitigation strategies and countermeasures; and
- Outreach: Engage the national innovation systems in identifying and providing leading-edge S&T solutions.

The PSTP will initially be comprised of four "Mission Areas"*;* CBRNE, Disruption and Interdiction, Critical Infrastructure Protection, and Systems Integration, Standards, and Analysis. The PSTP in itself represents a significant stage in the development of a comprehensive strategic plan to address public security S&T as it is possibly the first international collaboration agreement to address public security[35] as a whole and thus establishes a model for other international programs. Clearly both the Canadian and U.S. governments recognized that there was an immediate need for increased international coordination and cooperation between key security portfolios and that S&T will be central to this effort.

European Security Research

The European Union has also identified the significant security advantages of engaging their S&T community. In *Research for a Secure Europe*, the "Group of Personalities" noted that to

[34] Canada. CA US Public Security Technical Program. *Public Security Technical Program: Introduction and History*. http://pstp.drdc-rddc.gc.ca/introhistory_e.asp#5; Internet; accessed 3 April 2005.

[35] The UK and the U.S. signed, on 8 December 2004, a Memorandum of Agreement for: *Co-operation in Science and Technology for Critical Infrastructure Protection and Other Homeland/Civil Security Matters*. The Memorandum will "allow the UK and the US to work together on counter-terrorism research, and to seek the best expertise available to carry out a joint science and technology programme." United Kingdom. Home Office. http://homeoffice.gov.uk/terrorism/govprotect/cbrn/usuk.html; Internet; accessed 3 April 2005.

achieve its security objectives of protecting its citizens at home and to contribute to international security by cooperating with its international partners and alliances, "…Europe must take advantage of its technological strength. Technology itself cannot guarantee security, but security without the support of technology is impossible."[36] Of significance is that this report in itself establishes the field of "Security Research" where in its title it characterizes the expert panel as a "Group of Personalities in the Field of Security Research." While certain deficiencies are noted that impede the full exploitation of its scientific, technological, and industrial strengths, the European report identifies key measures to ensure that technology can be the true "force enabler": effective coordination of research activities, systematic analysis of security-related research, and fully exploiting the synergies between defence, security, and civil research.[37] In 2004 when implementing its Preparatory Action the field of security research, the European Commission noted, "Europe must invest in a 'security culture' that harnesses the combined and relatively untapped strengths of the 'security' industry and the research community in order to effectively and innovatively address existing and future security challenges."[38]

RISK ASSESSMENT AS A FOUDATION FOR S&T STRATEGY

"An ancient cliché holds that strategy is an art, not a science. Specifically, strategy is the linking of the ends and means – a "game plan" that tells how finite resources will be

[36] European Commission, Research for a Secure Europe – Report of the Group of Personalities in the Field of Security Research (Luxembourg: Office for Official Publications of the European Communities, 2003), 6.

[37] The Commission of European Communities will undertake the main recommendations of the Group of Personalities report including the establishment of a European Security Research Advisory Board (Autumn 2004 and a European Security Research Programme to commence in 2007. Commission of the European Communities: Security Research: The Next Steps, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions COM(2004) 590 final (Brussels, 7.9.2004).

[38] Commission of the European Communities: On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of security research, Towards a programme to advance European security through Research and Technology, COM(2004) 72 final (Brussels, 3.2.2004).

employed to accomplish declared objectives. Coherent strategy is the key to institutional success; it is as important for business and universities as it is for countries." [39]

While Canada has articulated a NSP, no coherent strategy to provide a basis for a comprehensive planning environment necessitated by the Policy has been put forward by PSEPC. To successfully implement the NSP and to ensure it meets the stated objectives of securing Canadians now and into the future, a strategy is clearly required. In "*The Art of Strategy and Force Planning*", the authors offer a simple model for planners and decision makers that focuses on key variables that are constantly reviewed and re-assessed. Two of Bartlett's key variables, "risk" and "goals" are examined in this essay as the elements of the "paradigmatic paradox" that arises from adapting military concepts, knowledge, and experience to the emerging civilian "public security" environment. These elements are risk assessment and the development of common capabilities.

Threat and Risk

Threat assessment, which is very much at the centre of military planning, attempts to understand the strategy, doctrine and motives of a known adversary. "The threat approach involves identifying potential opponents and assessing their capabilities. The constant monitoring of the military arsenal of North Korea illustrates the nature of this approach."[40] This has led to what Richard Betts described as "conceptual inertia" where "the Cold War accustomed strategists to worrying about an enemy with thousands of WMD, rather than foes with a handful."[41]

There are two "limiting" examples of the failure of the threat assessment paradigm, regrettably both are dramatic and tragic. The first example demonstrates the inability of existing intelligence systems to assess threat at the non-state actor level, the level of terrorist organization, while the second is an example at level of a state actor. The first example is

[39] Henry C. Bartlett, G. Paul Holman, Jr., and Timothy E. Somes, "The Art of Strategy and Force Planning." in *Strategy and Force Planning* (Newport, RI: Naval War College, 2004), 17-33.

[40] *Ibid.,* 26

[41] Richard K. Betts, "The New Threat of Mass Destruction," *Foreign Affairs (*Jan/Feb 1998): 26.

found in the analysis of the factors and intelligence indicators leading up to the September 11, 2001 attacks. In their chapter "The System was Blinking Red", the 9/11 Commission examined the threat reports and indicators that led the then CIA Director John Tenet to believe that "the system was blinking red." Yet despite the indicators of a "high probability of near-term 'spectacular' events", there was no specific response from domestic intelligence agencies because they "did not know what to do" and consequentially there was a response void where no prevention measures were taken.[42] In physical science terms, this failure could be considered a "false negative", the "system" did not respond to a threat even though one was present.

The second limiting example is a dramatic "false positive", an artefact created by a system that was acted upon even though there was no real event. The recent Robb Commission report examined in considerable detail the threat assessment failure upon which the U.S. government based its decision to launch a pre-emptive war against the Iraqi threat of Weapons of Mass Destruction:[43]

> *On the brink of war, and in front of the whole world, the United States government asserted that Saddam Hussein had reconstituted his nuclear weapons program, had biological weapons and mobile biological weapon production facilities, and had stockpiled and was producing chemical weapons. All of this was based on assessments of the U.S. Intelligence Community. And not one bit of it could be confirmed when the war was over.*

Their conclusion, offered in the letter to the President of the United States, is direct and unambiguous: "We conclude that the Intelligence Community was dead wrong in almost all of its pre-war judgements about Iraq's weapons of mass destruction." If the intelligence system can fail at its most "classical" level of analysis, that of state-based threats, then what validity will intelligence have to assess threats at micro levels of individual terrorism cells or even individual terrorists? In both instances a risk was present and preparedness measures

[42] United States. The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, W.W. Norton & Co., New York, NY, 2004; pp 254-277.

[43] United States. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Report to the President of the United States, March 31, 2005; Internet http://www.wmd.gov/, accessed March 31, 2005.

could have been taken such as enhancing security at airports against trained terrorist pilots or further diplomatic measures against a state actor.

The new "cadence" of terrorism further reinforces the need for a paradigmatic shift from threat to risk based-planning.[44] "Now a system designed for comparatively slow state-based threats has to cope with much more rapid non-state-based threats."[45] "Non-state groups can move, act and adapt more quickly than Western national security capability can respond."[46] These non-state groups activities are buried "in the noise" of daily activity in Western society and traditional indicators of activity used to identify threats of state actors are not sufficiently sensitive. This argument with respect to the faster cadence of non-state actors is compelling if there was evidence that national security systems had coped even with the slow cadence of terrorism, an example being the interval between the first World Trade Centre bombings, where in 1993 terrorists first attempted to collapse the buildings and 2001 when they were tragically successful.

Traditional counter-terrorism preparedness emphasized the use of an intelligence model that was to provide a forecast of future events based on prior information, analytical models, and threat assessment. "On an operational level, governments have traditionally dealt with terrorism . . . . as essentially a tactical rather than a strategic problem."[47] The anthrax letter attacks in particular negate this tactical intelligence model. There were no known public indicators that such an attack was imminent as they were below the visibility of national and domestic intelligence systems and perhaps even below the visibility level of local police forces.

[44] Lesley Seebeck, "Cadence, War and Security", *Australian Journal of International Affairs* 58, Issue 4 (December 2004): 494-510.

[45] *Ibid*., 501.

[46] *Ibid*., 502.

[47] Kevin O'Brien and Joseph Nusbaum. Intelligence gathering on asymmetric threats, Part 2, *Jane's Intelligence Review*, November 2000: pp 50-55.

Terrorism is asymmetric warfare against civilian targets thus the challenges to intelligence systems that asymmetric warfare already poses are only further complicated.[48] "These threats do not present the danger of a major conventional war to developed countries but do present equal (sometimes greater) dangers to the populations and governments of these states." In examining the threat from an asymmetric actor's point of view, the methods and means available to the actor include weapons of mass destruction, cyber or cyber-based warfare and non-conventional operations and the realisation that "the most devastating asymmetric attacks on civilians in North America, Europe, and Japan to date have not relied on military platforms of delivery."

Previously, military paradigms utilized to assess the threat from CBRN warfare were also examined and in particular the need to "shake", abandon, certain paradigms to better understand the new nature of CBRN terrorism which targets unprotected civilian populations, is not limited doctrinally to known "weapon systems" and are employed by adversaries who are not deterred by a strong defence.[49] As Anthony Cordesman states "Far too often the United States attempts to address the evolving threat and consequences of each type of CBRN attack by using dated research and modeling that has been designed for the needs of the Cold War, or that has been developed to deal with selected generic threats."[50]

This stasis in thinking or lack of imagination was particularly exemplified in the often-limited lists of chemical hazards. When the intent is to cause harm or death, the list need not be limited to classical chemical warfare agents on the Schedules of the Chemical Weapons Convention. For example, to resolve the Chechnyan hostage taking at the Moscow Dom Kultura theatre in October 2002, Russian Special Forces used a "knock-out gas" to subdue the terrorists. While both terrorists and hostages were "incapacitated", the narrow therapeutic index of the potent analgesic utilized resulted in the death of one hundred and nineteen

[48] Kevin A. O'Brien and Joseph Nusbaum. Intelligence gathering on asymmetric threats, Part 1, *Jane's Intelligence Review* October 2000: pp50-55.

[49] Camille A. Boulet and Shaye K. Friesen, *CBRN Terrorism: Shaking Military Paradigms - A Risk-Assessment Based Approach to S&T Investments for Chemical and Biological Defence*, RTO Lecture Series 239 Pre-Prints, AC/323(SAS-046)TP/45, October 2003.

[50] Anthony H. Cordesman, *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland* (Westport, CT: Praeger Publishers, 2002). p26.

hostages and 35 rebels. This is not to suggest that the actions of the Russian forces was terrorism, it just serves to illustrate clearly the vulnerability of unprotected civilians and the great range of chemical agents available to terrorists. Relative to the Tokyo subway attack using Sarin[51], where 12 people died, the use of an unconventional fentanyl analgesic produced an order of magnitude more fatalities. Importantly, the event opened up new avenues of knowledge and information to potential terrorist groups. The magnitude of a chemical incident is currently established by the 1984 tragedy of Bhopal, India where a leak of methyl isocyanate from a Union Carbide plant killed approximately 3,800 persons and left thousands more disabled.[52] The potential for catastrophic events arising from toxic industrial or hazardous materials must be considered in the terrorism risk analysis spectrum, particularly where environmental damage could be extensive. [53]

Traditional deterrence will not stop a disgruntled group without any identifiable address from striking out. "The main problem of deterrence, however, is that it still relies on the corpus of theory that undergirded Cold War policy, dominated by reliance on the threat of second-strike retaliation. But retaliation requires knowledge of who has launched an attack and the address at which they reside. These requirements are not a problem when the threat comes from a government, but they are if the enemy is anonymous."[54] In summary, the threat assessment paradigm, particularly for terrorism prevention and preparedness, is now limited if not completely invalid.

Montgomery Meigs introduces another subtlety to the asymmetric warfare model to describe current terrorism, one where "idiosyncrasy" characterises the nature of these events. The

[51] World Health Organization. Public Health Response To Biological And Chemical Weapons: WHO Guidance – 2nd. Ed (Geneva: World Health Organization) 2004.

[52] Bhopal Incident Review, http://www.bhopal.com/review.htm; Internet; accessed 2 April 2005.

[53] In 1999, the U.S. General Accounting Office report limited its assessment largely to classic chemical warfare agents such as choking, nerve, blood, and blister agents. It did identify some toxic industrial chemicals such as chlorine, phosgene, and hydrogen cyanide (United States General Accounting Office. *Combating Terrorism. Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Agents* (GAO/NSIAD-99-163) September 1999. Recently the U.S. Centers for Disease Control and Prevention have taken a much more comprehensive approach to hazardous chemicals. Their list includes methyl isocyanate (added March 17, 2005) and the fentanyl opiods (added March 11). United States. CDC Emergency Preparedness and Response. Chemical Categories. http://www.bt.cdc.gov/agentlistchem-category.asp; Internet; accessed 5 April 2005.

[54] Betts, p 34.

overall asymmetric strategy of the terrorism has been relatively constant; it is essentially the definition of the strategy employed by a less capable adversary whether it is terrorism, insurgency, or guerrilla warfare. "The combination of asymmetry and the terrorist's ability continually to devise idiosyncratic approaches presents our real challenge." In Meigs' definition, "idiosyncrasy connotes an unorthodox approach or means of applying a capability, one that does not follow the rules and is peculiar in a sinister sense." "Terrorists will adapt lawful capabilities from the public domain, or purloin them from secure areas, and combine them in ways that are unprecedented and destructive. How do we anticipate their ability to innovate?"[55] This observation is reinforced by Seebeck's assessment of the March 11, 2004 Madrid bombings of commuter trains and stations that resulted in 191 killed. The materials required to conduct the attack, explosives, cellular phones, and SIM cards were all locally procured or available. The careful planning of these attacks was conducted by local nodes of the terrorist network.[56]

If the threat assessment model is no longer valid, then the essence of the problem is how to characterize the risk, and from there derive plans and priorities. Paul Slovic has characterized this form of terrorism as a "new species of trouble" that "strains the capacity of quantitative risk analysis." He states, "Our models of the hazard-generating process, terrorists' minds, are too crude to permit precise predictions of where, when, and how the next attacks might unfold."[57] This characteristic has led some to consider the current security environment as fostering the "politics of fear" but as Anthony Giddens argues "scaring people – getting them to see that the risk is real – may be the very condition of minimising or avoiding danger."[58] It is not sufficient to argue that because further attacks have not occurred or that the technical difficulties of a catastrophic CBRN attack as reasons to completely discount any investment in preparedness.

---

[55] Montgomery C. Meigs, "Unorthodox Thoughts about Asymmetric Warfare," *Parameters*, (Summer 2003): 4-18.

[56] Lesley Seebeck, "Cadence, war and security", *Australian Journal of International Affairs* 58, Issue 4 (December 2004): 494-510.

[57] Paul Slovic, "Terrorism as Hazard: A New Species of Trouble," *Risk Analysis* 22, no. 3 (2002): 425.

[58] Anthony Giddens, "Scaring people may be the only way to avoid the risks of new-style terrorism", *New Statesman*, January 10, 2005, 29-31.

The differentiation between risk and threat in the public security preparedness context is particularly important as the challenges posed by these fanatical terrorists cannot be mitigated if one waits to have sufficient indicators of the intent, the "threat", to develop counter-terrorism approaches. As Woo points out, "The task of quantifying terrorism risk should not be confused with predicting the next attack."[59] "Thus", as Falkenrath puts it, "all threats are risks, but not all risks are threats."[60] This distinction between *risk* assessment and *threat* assessment is not simply semantic, it is vitally important to public security because on one hand adequate preparedness and response measure must be developed and where possible, any imminent threat immediately disrupted. The risk assessment model is crucial for establishing investment and program priorities, recognising that while substantial investments are being made to address national security requirements, a shotgun, wholesale spending across all dimensions is not in itself a risk management approach.[61]

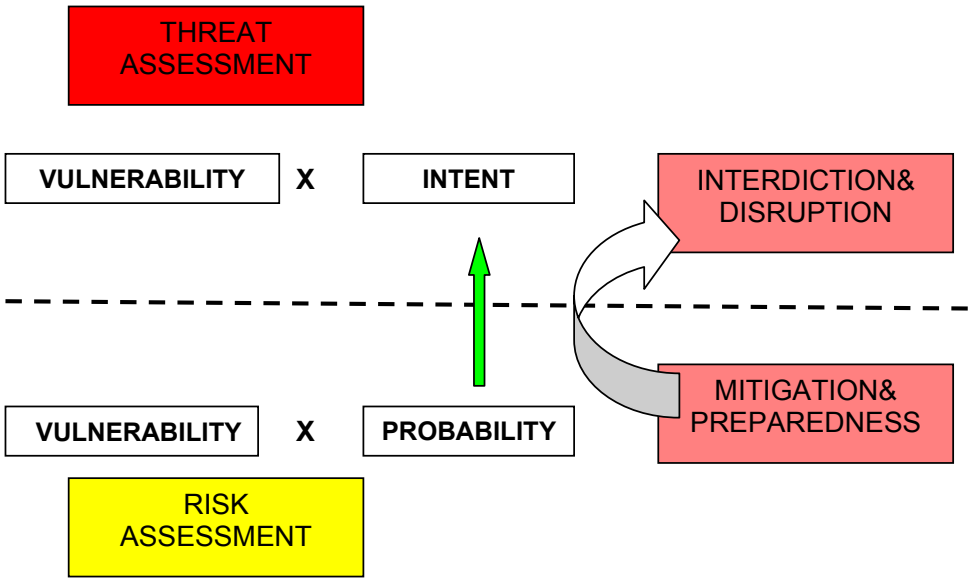
Figure 1 shows conceptually the difference between threat and risk assessment. In both cases, the assessment is based on factoring the vulnerability and the probability of an attack. What differentiates the two is that in the case of "threat", probability is now measured as intent, the indications of deliberate planning action or activities by a person, group, or state. Where there is a probability of an event, any response measures are part of planning, preparedness and mitigation. Once intent is known, there is a need for active intervention to disrupt or interdict the persons and the threat.

[59] Gordon Woo, "Quantitative Terrorism Risk Assessment," *The Journal of Risk Finance* (Fall 2002):7.

[60] Falkenrath, p 178 footnote 13.

[61] OAG reports and federal policy requiring a sound risk assessment methodology to prioritise investments in a resource constrained environment.

Figure 1: Conceptualizing Threat and Risk Assessment



Threat and risk assessment are not exclusionary but in fact have a symbiotic relationship. Where risk assessment is proposed as the basis for mitigation and preparedness, the assessed risk can assist security and intelligence agencies in better identifying or understanding threats. Reciprocally, information may come from threat assessments that necessitate a broader assessment of risk in other scenarios or contexts.

High consequence, low probability events such as catastrophic bioterrorism provide a particular challenge to quantitative risk assessment and risk management approaches. "Catastrophic bioterrorism" is exemplified in Richard Danzig's planning scenarios, or "cases" to develop a common vernacular to enable effective planning, preparation, and response. For example, his Case 1, the large-scale aerosol release of anthrax, could result in primary effects 40 miles downwind and the immediate infection of 200,00 people; lesser but still significant infections could occur up to 120 miles downwind.[62] These consequences exceed even the definition of "macroterrorsim" put forward by Woo - "a spectacular act of

[62] Richard Danzig, *Catastrophic Bioterrorism – What Is To Be Done?,* (Washington, D.C.: Center for Technology and National Security Policy, National Defence University.

terrorism (which may be a multiple strike at several locations) which causes more than $ 1 billion of loss, or 500 deaths."[63] Thus, where risk is probability multiplied by consequences, catastrophic bioterrorism could result in an extremely high number of casualties but the probability of this event occurring may be immeasurably small.

It may not be possible to ever arrive at an entirely rigorous system for assessing terrorism risk relative to all other risks or threats facing a society. However, for any government, where a variety of risks must be balanced, it cannot concentrate solely on the extremely low probability but must also consider the very high consequences events. "National security policy analysis is and will remain a highly subjective affair, one in which judgement and the careful weighing of qualitative considerations matter as much as or more than quantitative indices."[64]

Capability Planning

> The second paradigm of the "paradigmatic paradox" derives from the logical consequences of considering terrorism a form of asymmetric warfare and the implications that a risk assessment approach has had in recent military transformation. This shift away from threat-based planning resulted in a capability-based model that is now one of the central tenets of the 2001 U.S. Department of Defense Quadrennial Review[65] and the transformation agenda for the U.S. Army. This model concentrates on analyzing the risks, "how the adversary might fight" rather than specific threats or "specifically whom the adversary might be or where the war might occur."[66] In developing an S&T

[63] Woo, p 10

[64] Falkenrath, p176.

[65] Donald H. Rumsfeld, Quadrennial Defense Review Report, Department of Defence, September 30, 2001.

[66] United States. Department of Defense. Quadrennial Defense Review Report. Washington: Government of the United States of America, September 30, 2001; available from http://www.defenselink.mil/pubs/qdr2001.pdf ; Internet; accessed 14 March 2005.

strategy to enable an effective and resilient response to terrorism, this distinction is critical.

"Capabilities-based planning (CPB) is planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances while working within an economic framework that necessitates choice."[67] It has become integral to long-term force structure planning within The Technical Cooperation Program (TTCP) Nations (Australia, Canada, New Zealand, United Kingdom, and United States) and "represents an attempt to break down traditional stovepipes and provide for transparency and cohesion."[68]

While not an entirely satisfactory simile, the new security partners formally incorporated into the new Public Safety and Emergency Portfolio, and the security partners that contribute directly to national security (DND, Health Canada, Public Health Agency of Canada, Canadian Food Inspection Agency, Transport Canada, Environment Canada, etc.) are analogous to the service stovepipes of the U.S. and Canadian militaries. To meet current and future security challenges, there has been a need to move towards increased integration, interoperability, and the horizontal nature of the response to national security requires a new strategic approach to capability development.

> *The Government of Canada agrees that the key to providing greater security for Canadians and to getting the most out of our security expenditures is to co-ordinate and better integrate our efforts. The Government is committed to providing the leadership, resources and structures necessary to build a fully integrated and effective security system.*[69]

Given the stated objectives of the NSP to build an integrated security system, a rigorous planning approach to developing the protection, prevention, and consequence management capabilities identified are clearly required. As the *TTCP Guide to Capability Planning* notes, "When CBP is properly implemented one of the key benefits lies in its ability to help take the

---

[67] Paul K. Davis, "Analytical Architecture For Capabilities-Based Planning, Mission System Analysis, And Transformation,: RAND MR-1513-OSD, 2002.

[68] TTCP Technical Report, "Guide to Capability Based Planning," TTCP Technical Report TR-JSA-TP3-2-2004 (1 Oct 2004).

[69] NSP, 9.

focus away from single service stovepipes. This accrues from the need to usually use systems and concepts from multiple services to achieve each capability in the capability partition space."[70]

> CPB is very much interconnected with the concepts of scenario–based planning.[71] At the core is the use of a robust set of scenarios that can run from specific to general and serve to examine risk, vulnerabilities, and capability requirements.
>
> *The system begins with a comprehensive threat assessment. It provides both the tactical and strategic information about risks to Canada. This threat information is used to structure and trigger proportionate, integrated capabilities to prevent or mitigate the effects of the threat. When an event occurs, an integrated system for managing its consequences is triggered. In order to ensure the continuous improvement of the system, effective evaluation and review* [sic] *are conducted*."[72]

Here the use of the term "threat" is consistent with the threat and risk model as it serves to direct the capabilities needed for prevention and mitigation in advance and consequence management when an event occurs. Missing is the step between mitigation and consequence management, a key element addressed by the Disruption and Interdiction mission area construct developed for the PSTP.

A PUBLIC SECURITY S&T STRATEGIC MODEL

The challenge for developing a comprehensive S&T strategy is to model key elements of a security process that links hazards and targets and identifies key processes to enable prevention, preparedness, and response. The Public Safety and Emergency Preparedness Framework cycle (Figure 2) shows the cyclical nature of any emergency whether it derives from an accident, a natural disaster or from an act of terrorism.[73]

---

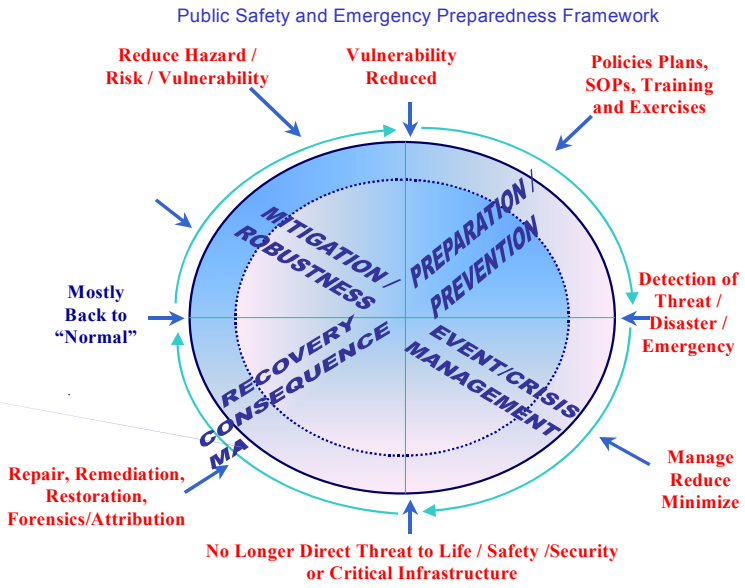
[70] TTCP Technical Report, "Guide to Capability Based Planning," TTCP Technical Report TR-JSA-TP3-2-2004 (1 Oct 2004): p3.

[71] Paul J.H. Schoemaker, "Scenario Planning: A Tool for Strategic Thinking," *Sloan Management Review* 36, no. 2 (Winter 1995): 5-39.

[72] NSP,10.

[73] This model has been used within PSTP and CRTI working groups and originates from materials prepared by PSEPC participants. An original source could not be located.

Figure 2: A Public Safety and Emergency Framework[81]



Adopting this model is significant as it allows for a more holistic and system of system based approach where many elements of emergency management can be identified and applied for dual purposes. Assuming the starting point is in "Mitigation and Response", one can assign response requirements, indicated by arrows, to each phase of the response cycle.

The need to assess and reduce vulnerabilities and develop policies, procedures, standards and training for responders is part of readiness measures. As the cycle moves from readiness to response, there is increasing emphasis on event detection, characterization, and consequence management. Where these events are deliberate in nature or originate from a terrorist act, forensics and criminal investigation requirements increase. The cyclical process is key to developing a learning approach where lessons learned are incorporated into future planning, mitigation actions, and response procedures. While S&T itself contributes to each of these elements, an "R&D program" would formally constitute part of the Mitigation quadrant of

the Public Security Framework cycle as a proactive activity or program designed to reduce vulnerability and enable response throughout the cycle.

The Canadian Consolidated Risk Assessment Model

At the centre of terrorist risk assessment is the recognition that a terrorist attack is not an accident, it is an intentional and deliberate act. "However, unlike natural disasters, it features human intelligence, and unlike industrial disasters, it features human intent."[74] This changes the analytical framework where the initial departure point is not to ask, "What can go wrong?" but rather "How can I make something go wrong?"[75] Central to the Canadian Consolidated Risk Assessment (CRA) model has been the use of a Delphi-like process[76] to engage, through a broad consultation, the S&T, operational and law enforcement, and intelligence communities to ask them "what can go wrong". "Characteristic Scenarios", Annex 1, are used to briefly describe the nature of individual events that would require prevention, preparedness, or responses are evaluated for the vulnerability they pose to public safety. In the Canadian context, Vulnerability is a factor of both Feasibility, which considers technical factors of ease of materials availability, production, planning, and attack and the Impact where the consequences to people, social systems, critical infrastructure an the economy are factored. This Vulnerability is considered the "consequences" of the terrorist act described in the scenario. As noted previously quantifying the extremely low probability of any such terrorist attack is difficult however, probability here is based on an intelligence judgement that examines key indicators for risk rather for a threat assessment. The CRA model (Figure 2) was first developed for CBRNE hazards but is sufficiently robust to assess terrorism risk in the Disruption and Interdiction and Critical Infrastructure. The elements of the CRA model that have been used in the establishment of investment priorities,

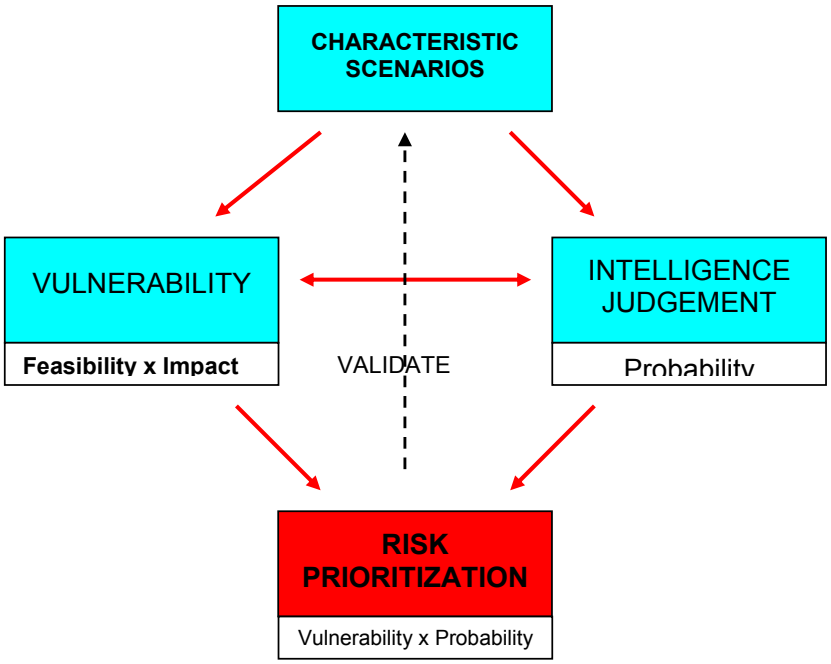
[74] John A. Major, "Advanced techniques for Modeling Terrorism Risk," *The Journal of Risk Analysis* (Fall 2002): 15-24.

[75] B. John Garrick, "Perspectives on the Use of Risk Assessment to Address Terrorism," *Risk Analysis* 22, No. 3 (2002): 421.

[76] The Delphi method was developed by the Rand Corporation and is a process for technology forecasting that examines issues where there is a lack of quantitative data for analysis of complex problems. It is a dynamic group process that uses the knowledge and experience of a group of experts from a diverse background to build consensus on a particular issue. For a more complete description of the Delphi process http://www.fs.fed.us/servicefirst/sustained/minerals/gen-delpdes.rtf; Internet; accessed 26 May 2005.

identification of capability gaps and the selection of S&T project within CRTI. [77] (Annex 2). The CRA model presented is to allow for the use of a parallel process to examine the risk of all mission areas, not just CBRNE scenarios and has been adapted for the Disruption and Interdiction and the Critical Infrastructure missions within the CA- U.S. PSTP.

Figure 2: The Canadian Consolidated Risk Assessment Model



[77] An outline of the CRA methodology is provided in Annex 2. The CRA is updated annually and the intelligence, counter-terrorism communities, and science-based departments and agencies use the results.

Strategic Capability Model

The final element of the S&T strategy is to formulate and adopt a Strategic Capability Plan, and associated processes, that will ensure outcomes that support the NSP. A national public safety and security business model, that has as an outcome the development and management of national capabilities, can be informed and enabled by S&T. While Canada has very much pioneered the use of Risk Assessment in for example the CRTI and the CA U.S. Binational PSTP program formulations, the United Kingdom, through its Civil Contingencies Secretariat has articulated the first strategy model to employ capability based planning in public security context. *The Resilience Capability Framework*[78] contains significant elements that correlate closely with the military capability-based planning already in place within the UK MOD:

> *Capability targets will be clearly defined in terms of the desired effects of the required capability as opposed to the characteristics of the capability itself. For example, they will refer to the speed with which an area should be decontaminated rather than the numbers of mobile decontamination units required to make this possible. In general terms, the targets should convey the required geographical coverage, speed of implementation or recovery and the necessary sustainability. Underpinning each target will be an assessment of the capability components required to satisfy this target. These capability components include:*
>
> ***Doctrine*** *– guidelines which set out best practice for responders (i.e. UK guidance on the decontamination of people);*
>
> ***Plans*** *– setting out response arrangements for an incident (i.e. local operational plans);*
>
> ***Legislation*** *– enabling responders to carry out their duties within the confines of the law;*
>
> ***Equipment*** *– the type and quantity of equipment necessary to enable responders to carry out their duties safely and effectively;*
>
> ***Personnel*** *– the number of people required to achieve the desired effect;*

[78] United Kingdom. Civil Contingencies Secretariat. The Resilience Capability Framework:. Overview and Approach.. (UK Restricted). 2 May 04.

Training *– for personnel in the use of equipment and for their understanding of plans; and*

Supplies *– the services and stock required to enable an effective response (i.e. prophylactics) should be clearly defined in terms of the desired effects of the required capability, as opposed to the characteristics of the solution to be implemented.*

The capability components in the UK model are analogous to the PRICIE[79] model that is used in the CF capability-planning framework. This model as shown is adapted to Canadian requirements to serve as a sound basis for a strategic capability investment plan for the public security and also derives from capability engineering development [80] models.

The Canada-United States Bi-National PSTP has used initially three key mission areas to address the security risks. The fourth mission is intended to examine overarching issues including the coordination of capabilities between mission areas and the conduct of the bi-national Coordinated Risk Assessment. The agreed mission areas are:

CBRNE*: the capability to prevent, prepare for and respond to CBRNE threats to public security, whether derived from terrorist or criminal activity, natural causes or accidents.*

Critical Infrastructure Protection (CIP)*: the capability to ensure the robustness, reliability and protection of physical and IT facilities, networks, services and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security, economic well-being or effective functioning of the nation.*

Disruption and Interdiction (DI)*: the capability to identify and stop terrorists/criminals and their activities, including surveillance, monitoring, disruption and interdiction of their activities through intelligence, law enforcement and border and transportation security.*

[79] PRICIE: Personnel, R&D/Ops Research, Infrastructure & Organization, Concepts, Doctrine & Collective Training, IT Infrastructure, Equipment, Supplies and Services.

[80] Defence R&D Canada. Collaborative Capability Definition, Engineering and Management (CapDEM), Defence R&D Canada Fact Sheet, http://www.ottawa.drdc-rddc.gc.ca/publications/factsheets/FFSE-234-capdem_e.asp; Internet; accessed 24 January 2005.

Systems Integration, Standards and Analysis (SISA)*: the performance, integration and interoperability of national and international public security and emergency management capabilities and supporting systems, including the enabling standards, and vulnerability and systems analyses.*

The four mission areas developed under the Binational program correlate well with other public security constructs such as that proposed by the European Group of Personalities as do the capabilities elements required in to address each mission area. These are shown in Table 2 where the four missions areas are compared to the Secure Europe report which identified how S&T and can contribute to public security. The comparison shows considerable agreement in missions as priorities and the requisite S&T capabilities. In some instances, the capability may already exist and simply require acquisition and implementation whereas in other areas where no satisfactory system is available, R&D will be needed to fill the gap.

Table 2: Comparison of Mission Concepts and Associated Capability Targets of the CA US Binational PSTP and the Secure Europe model.

Strategic Element	CA US PSTP	Secure Europe
Mission	• CBRNE • Disruption and Interdiction • Critical Infrastructure Protection • System Integration, Standards and Analyses	• Disaster Management (Conventional attack, CBRN attack Hostage) • Border Control • Protection of Critical Infrastructure
Capability	• Conduct effective, accurate and timely detection and alert of suspicious events • Improve S&T interoperability for operational reach back • Early event and critical point detection • Secure network architecture and management • Cyber event management; and • Network Analysis and Modelling • Immediate consequence management techniques for CBRNE hazards • Methodologies and protocols for recovery and long-term consequence management	• Detection • Protection • Surveillance and Monitoring • Systems Interoperability • Security Against Cyber Attacks • Secure Digital Communication • Protection of network hardware • Decontamination • Systems Interoperability

The most important aspects of taking a capability based planning approach is to use the model to ensure that the development addresses all factors for successful implementation.

The capabilities outlined in Table 3 consider very carefully the need for an all hazards approach and wherever possible dual use technologies or capabilities. By engaging all public security departments and associated science based departments and agencies, both the capabilities and the resources needed for their system wide development and successful implementation can be brought to bear. This capability planning-based approach is outlined in Figure 3. Characteristic scenarios are as the basis for the conduct of the risk assessment and for the examination of capability assessments and the identification of capability gaps. These can be addressed through a Capability Investment Plan that would identify where S&T is needed and where R&D is required to close capability gaps.

Table 3. Overarching Considerations for Possible NSP Capability Areas

Canadian NSP Capability Areas
An integrated national risk assessment, intelligence and surveillance capability to provide timely and accurate threat alert in support of interdiction of security threats
All-hazards, network-enabled national emergency management and response capability that provides decision makers and the public with timely, trusted situational awareness and decision support
Capability to rapidly identify and deliver the optimum effect both to mitigate risk and to provide effective response and recovery.
Effective and resilient public health capability to respond to terrorism and public health emergencies
Capability to rapidly identify vulnerabilities and to cost-effectively design and/or retrofit national critical infrastructure for all-hazards robustness.
Capability to ensure the safe, secure and efficient flows of people, goods and services across Canada's borders.
Effective national standards that enable performance objectives and interoperability across public safety and security organizations.

Key words such as "integrated", "network enabled", and "effective" address lessons learned from previous emergencies where these were found lacking in the measures taken or ignored and to the issue of "coordination". Anthony Cordesmann dedicates a significant portion his conclusions and recommendations in *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction* to the need for central coordination and in particular notes that "Technology offers major potential improvements in homeland defence, but it must be applied as a system of systems, rather than a series of uncoordinated increments, and analysis of the cost to deploy technology and means of defeating it needs a far more explicit analysis than it currently receives."

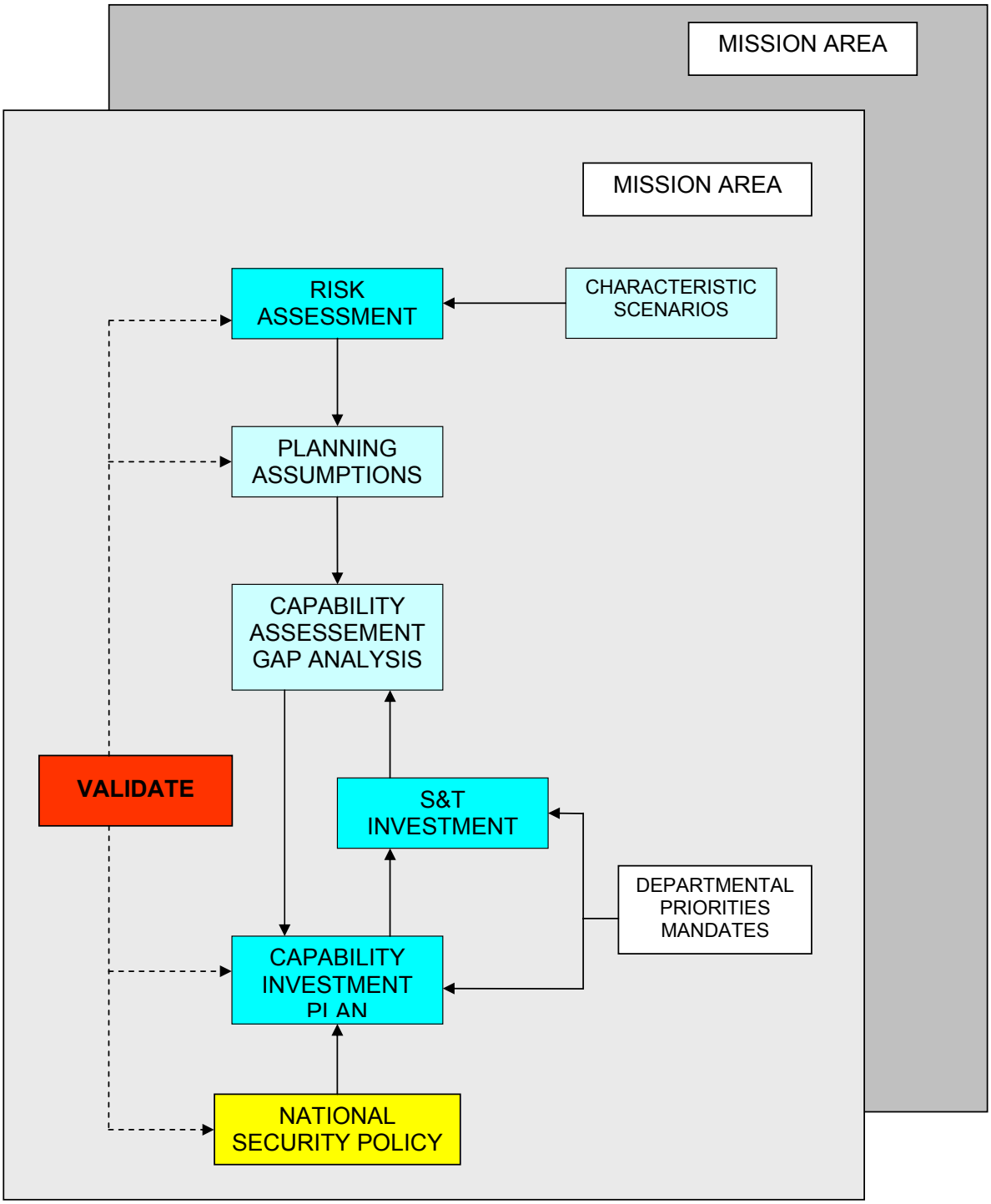


Figure 3: Outline of a Capability Based Planning Approach to Public Security

A distillation of published capability gaps, first responder needs, and government programs show how S&T can contribute to public security is given in Annex 3. This analysis allows for the identification of key S&T and R&D targets that contribute substantially to security

will be the requirement to manage data and communication challenges, such as the sensor-to-operator ratio where the number of sensors will exceed the number of operators or a decision support system's capability to manage data and information. Decision support and command and control systems will have to be able to adapt to the decision maker or users throughout the emergency management community by understanding the human dynamic, particularly at the level of cognitive and social domains. To achieve this, it will be necessary to exploit the potential of communications networks and knowledge management systems that enable distributed decision-making and coordinated action. Interoperability ensures that responders and response capabilities will be effective across the national and bi-national jurisdictions involved in an emergency response. S&T can identify where interoperability standards are required through system analysis or exercises and contribute to the development and implementation of appropriate standards.

Comment [CT2]: Have no idea what this phrase means. Suggest others may not, either

Public Security Science and Technology: Some Final Considerations

Public security science and technology has only very recently emerged as an area of public policy. In September 2004, the University of Manchester's PREST, an institute that examines science and technology management and policy convened a NATO Advanced Research workshop entitled "Science and Technology Policies for the Anti-terrorism Era."[81] The workshop examines the emerging issues of how to structure programs for best value and to encourage international cooperation and collaboration, and the engagement of the innovation system as broadly as possible to ensure that the best possible ideas could be utilized to counter the effects of terror.

There is a paucity of direct evidence of the value of S&T for mitigating the effects of terrorism, due largely to the classified nature of many counter-terrorism operations but also because there are few instances where the intensity of terrorist attacks is sufficiently high as to measure the impact of an implemented technology or system. Isaac Ben-Israel, in a paper entitled *Science & Technology Priorities against Terrorism* considered the Israeli experience with an intense Intifada campaign of suicide terrorism over a four year period from 2000-

[81] University of Manchester. NATO Advanced Research workshop entitled "Science and Technology Policies for the Anti-terrorism Era. Program. http://les.man.uk/PREST/; Internet; accessed 8 April 2005.

2004 where there were 527 attempted attacks of which 132 successful suicide attacks killed 859 persons.[82] The suicide attack levels have since returned to pre-Intifada levels: "It will not be too exaggerated to say the "S&T played a major role in suppressing terrorism in Israel… The more technological the war against terrorism becomes, the better."[83] While specific technologies are not described, "intelligence technologies" that disrupt the terrorist network at key points in the planning stages are emphasized. The author offers other lessons on global terrorism:

> "*The "war" against terrorism is not a classic war (like the war between two rival state armies). It is more like the war against crime. And terrorism, like crime, will not disappear totally. Therefore, the goal of the "war" against terrorism should not be elimination of it, but reducing it to a bearable level."*[84]

Significant differences between the concepts of "national security" and "public security" emerged, particularly in the discussions surrounding the development of international collaboration models. In "national" security, considerations around the protection of defence technologies and knowledge, as well as the exchange of information, materials, weapons, and defence systems is very much tied to secrecy and national interests. In contrast, public security engages players and partners that have been outside of any traditional defence S&T collaborations and agreements. Technologies are actually intended for use by public responders and thus existing collaboration models were intended to protect and maintain control over knowledge rather than make these technologies available to a public response community that is outside of federal jurisdictions. As a result, the workshop recognised that even the existing international security collaboration models that were based on defence models require a paradigmatic shift if they are to provide value in the current public security environment with an anti-terrorism focus. The CA U.S. PSTP was the first example of a program that considered these issues.

---

[82] Isaac Ben-Israel. *Science and Technology Priorities against Terrorism*, Science and Technology Policies for the Anti-Terrorism Era, NATO Advanced Research Workshop, UK, 2004.

[83] *Ibid.,* 5.

[84] *Ibid*., 8.

CONCLUSIONS

The tragic events of September 11, 2001 only served to crystallize a growing need for enhanced public security that was apparent in the growth of fanatical religious terrorism, proliferation of CBRNE materials, and other national and global security threats The Government in Canada, the United States, and Europe have recognised the emerging security risks and threats and have embarked on significant transformational activities to ensure the

expands the capability targets beyond just CBRNE hazard. There is a lack of a comprehensive federal S&T program for public security within Canada is in sharp contrast to the United States, the United Kingdom, and European Union where S&T has been integral to the policies and strategies that have been that articulated and the importance of S&T to address current and future security requirements recognized.

The new public security construct allows an opportunity to engineer a sustainable and resilient business model *ab initio* rather than approach the problem as a re-engineering issue. As stated by John Garrick, past president of the Society for Risk Analysis, "The single biggest contribution of risk assessment to date . . . .has been the development of a meaningful basis for managing risks. The quantification of risk, including the uncertainties involved, provides the most effective knowledge base possible for the logical allocation of resources for effective risk management."[85] Dan Henstra, in comparing and contrasting emergency management in Canada and the U.S. since 9/11 notes "Canadian mitigation advocates should use the lessons learned from 11 September to promote the idea of *comprehensive* mitigation, to reduce the impact of all hazards natural and human-induced. Thus the Public Security Technical Program, as outlined in this essay, is very much in keeping with his call that " A compelling event like 11 September can have an enduring impact on the machinery of government and public policy. Such events can sometimes derail existing efforts in a policy area, but they can also provide the impetus for major change. In either case, policy entrepreneurs must adjust their strategies accordingly."[86]

The Canadian emergency response system is a "System-of-systems" comprised of the technologies and capabilities inherent in the "multi-agency" federal, provincial, and municipal departments and agencies. It requires an "All-hazards" approach to manage emergencies from criminal, accidental public health or natural disasters and as such is "first responder" focused to ensure that appropriate response occurs at the earliest possible moment. Finally it operates in the multi-jurisdictional, legislative framework inherent in the Canadian federal system. Every one of these attributes can only lead to the conclusion that a

[85] B. John Garrick, opcit, p 422.

[86] Dan Henstra. Federal Emergency Management in Canada and the United States after 11 September 2001. *Canadian Public Administration* 46, no.1 (Spring 2004): pp103-116.

well coordinated approach to any program conception, formulation or implementation is required.

The approach is consistent with Canadian S&T policy frameworks that prefer horizontality in S&T to address a national priority. In order to deliver the most relevant and highest impact S&T results, the nations' S&T communities must improve their ability to:

- Anticipate risks and vulnerabilities in order to allow a shift from reactive to proactive S&T delivery;
- Inform, enable and respond to national public safety and security strategies that establish future direction,
- Provide direct S&T operational support; and
- Deliver to users the technical capabilities that anticipate and address the most critical gaps in operational effectiveness.

National Security is what Canadians expect from Canada's National Security Policy. Articulating a policy however is only the first step towards a lasting, robust, and resilient, public security system and capabilities that requires the full engagement of Canada's innovation system will be needed to keep up with emerging risks, terrorist threats, and other emergencies. To paraphrase Basil Liddell Hart, we can now arrive at a shorter definition of public security science and technology strategy as the art of distributing and applying *science and technology* to fulfil the ends of policy.[87]

[87] Basil H. Liddell Hart. Strategy 2nd Ed. (New York: Frederick A. Praeger Publisher): 1967: p 335.

Annex 1: High Consequence Natural and Deliberate Attack Scenarios

The following is an unclassified list of high consequence vignettes that serve as the basis for the development of scenarios for risk assessment within the CA US Binational Public Security Program. They are intended to be illustrative, not exhaustive, and are used in combination with lists of chemical, biological, radiological, or explosive materials to assess vulnerabilities, gaps and to develop capabilities.

BIOLOGICAL ATTACKS:

- An attack on unprotected civilian populations using a highly contagious viral disease (e.g. smallpox)
- An attack on unprotected civilian populations using a non-contagious bacterial agent (e.g. anthrax)
- An attack on the agricultural/food production chain at the livestock level using a contagious pathogen (e.g. foot & mouth disease)
- Contamination of food at the production or distribution stage using a pathogen (e.g. salmonella)
- An attack on the agricultural/food production chain at the crop level (e.g. wheat, soybean rusts)
- An attack using a novel emerging pathogen (e.g., engineered organisms) that is resistant to antimicrobial therapy, vaccination, or has enhanced virulence.

CHEMICAL:

- The deliberate release of a Toxic Industrial Chemical/Material causing wide area contamination (e.g. chlorine, ammonia)
- The release of a Chemical Warfare Agent internal to facility such as a mall, airport, or sports arena
- The release of a toxin in water supply system

RADIOLOGICAL or NUCLEAR EVENTS:

- The non-explosive dispersal or release of a radioactive source or clandestine placement of a source in a public space
- A Radioactive Dispersal Device – RDD (explosive dispersal)
- An Improvised Nuclear Device
- The use of a Nuclear weapon

EXPLOSIVES:

- Small clandestine charges (e.g. mail/letter bombs)
- Bomb on person (suicide bomber)
- Bomb in vehicle (roadside placement, suicide bomber, remotely piloted vehicle)
- Projectile with charge (RPG, mortar, small rocket, MANPAD, etc)
- Incendiary devices

CYBER:

- Disruption or denial of service (can be localized or widespread, and can be done in a variety of ways)
- Epidemic-style attacks (virus or worms)
- Attacks on protocol infrastructure (widespread disruption could be accomplished by attacks on Internet naming infrastructure (DNS) or routing infrastructure (BGP).
- Attacks on electronic control systems (SCADA)
- Malicious code (compromise via stealthy insertion of malicious code in software)

- Compromise of data (theft, corruption, destruction or release of data, can be stealthy or overt)
- Misrepresentation and misdirection (covers a wide variety of things, that could be done through a variety of means, to achieve a variety of objectives)

PHYSICAL ASSAULT:

- Small team with weapons (less than 10 people)
- Large team with weapons (10 or more people)
- Vehicle

INSIDER ATTACKS:

- Support staff (janitor, landscaper, etc)
- Security staff
- Technical or Administrative staff
- Executive staff

EMERGING HAZARDS:

- EMP, high-power microwave, directed energy devices

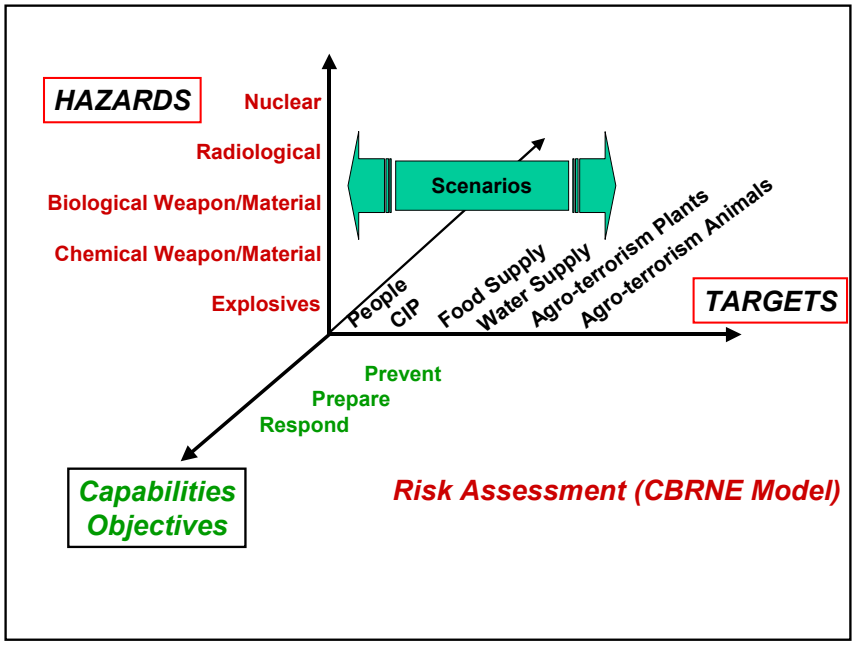
NATURAL DISASTERS AND OTHER EMERGENCIES:

- Major storm (major hurricane, set of major tornados, massive snow/ice storm)
- Firestorm, Forrest fires (natural or manmade)
- Major earthquake
- Major accident (power plant, chemical plant, etc)

Annex 2: Consolidate Risk Assessment Model: CBRN Terrorism[88]

The CRTI Consolidated Risk Assessment was originally produced in 2002 and updated in 2003. The annual CRA is classified Secret, CA UK US AUS NZ Eyes Only and the distribution is controlled at source (CSIS) and unclassified summary is provided here to illustrate the outcomes and information that is derived to guide S&T investments. The following is taken directly from the CRTI unclassified bulletin.

The assessment of the risk of CBRN terrorism examines several dozen characteristic scenarios that covered three hazard areas (chemical, biological, and radiological/nuclear) and targets such a people, critical infrastructure, food and consumer products and the agricultural systems; examples of these characteristic scenarios can be found in Annex 1.



Risk Assessment Process

The analysis of each characteristic scenario involves two steps. First, the Relative Technical Feasibility is evaluated, considering the technical and aspects of material availability, deployment, production and or dissemination equipment, technical expertise and knowledge, leading to a rating scale of high, medium, low, or very low. Impact is then evaluated, considering the potential number of dead or injured, intensity of response required, disruption of capability or capacity including critical infrastructure, critical services or the environment, and economic losses. This results in a rating scale of catastrophic, critical, moderate, or low. From this, Vulnerability is assigned based on the following matrix (Table 1):

[88] Canada. CBRN Research and Technology Initiative. Assessing the Risk to Canadian Public Safety and Anti-Terrorism. (2004-04-02); http://www.crti.drdc-rddc.gc.ca/about/assessing_e.html#1; Internet; accessed 3 April 2005.

Table 1: Vulnerability Matrix

IMPACT	RELATIVE TECHNICAL FEASIBILTY			
	High	**Medium**	**Low**	**Very Low**
Catastrophic	Extreme	Extreme	High	Moderate
Critical	Extreme	High	High	Low
Moderate	High	Moderate	Moderate	Low
Low	Moderate	Low	Low	Low

Second, an intelligence judgement is assigned according to the categories of likely, emerging, possible, or unlikely, with the results of the Vulnerability Matrix being brought forward. This judgement is not based on specific threat or intent information but is holistic examination of all contributing information. A preparedness prioritization level is then obtained based on the following matrix where Risk is the product of Vulnerability and Intelligence Judgment, which in the context of the Consolidated Risk Assessment is considered to be the best measure of probability usually employed in risk assessment. The matrix identifies scenarios and prioritizes investment from immediate through high, emerging, and finally discretionary (Table 2).

Table 2: Investment Prioritization

VULNERABILITY	INTELLIGENCE JUDGEMENT			
	Likely	**Emerging**	**Possible**	**Unlikely**
Extreme	Immediate	Immediate	High	Emerging
High	Immediate	High	High	Discretionary
Moderate	High	Emerging	Emerging	Discretionary
Low	Emerging	Discretionary	Discretionary	Discretionary

Scenario are then ranked and analyzed to identify prevention, preparedness or response gaps.

Annex 3: Overview of Science and Technology Capability Targets[89]

CA CRTI Investment Priorities[90]	**US DHS S&T** Strategic Objectives[91]	**US NAS** Making the Nation Safer[92]	**US MIPT** Project Responder [93]
Develop and Implement laboratory cluster (networks) in support of S&T response Collective command, control, communications, coordination and information (C4I) capabilities for CBRN planning and response S&T for equipping and training first responders Prevention, surveillance, and alert capabilities Immediate reaction and near-term consequence management capabilities Long-term consequence management capabilities Criminal investigation capabilities S&T dimensions of risk assessment Public confidence and psychosocial factors.	Technical Stds and certified laboratories to evaluate security and emergency responder technologies State of the art to prevent, detect, and mitigate the consequences of CBRNE attacks Equipment, protocols, and training procedures for response and recovery to CBRNE attacks Methods and capabilities to test and assess threats and vulnerabilities, and prevent technological surprise and anticipate emerging threats	Treatments and preventatives for known and emerging pathogens Develop, test and implement an intelligent, adaptive electric power grid Data fusion and data mining for intelligence analysis Information security against cyber-attacks Technologies (protective gear, sensors, communications) for emergency responders Advanced engineering technologies and fire rating stds for blast- and fire-resistant buildings Sensor and surveillance systems (for a wide range of targets) emergency officials and decision makers Methods and stds for filtering air against chemicals and pathogens Methods and stds for Decontamination	Unified Incident Command, Decision Support and Interoperable Communication Crisis Evaluation and Management Personal Protection and Equipment Logistics Support Detection, Identification, and Assessment Medical response Response and Recovery Mitigation and restoration for Plant and Animal Resources Criminal Investigation and Attribution

[89] There are two UK reports addressing science and technology for countering terrorism. The House of Commons examined primarily system wide and organizational considerations of the scientific response to terrorism. The Royal Society more narrowly assessed requirements for detection and decontamination of chemical and biological agents. House of Commons Science and Technology Committee. *The Scientific Response to Terrorsim*. London, UK: The Stationery Office Limited, 6 November 2003. The Royal Society. *Making the UK Safer. Detecting and Decontaminating Chemical and Biological Agents.* London, UK: The Royal Society (April 2004).

[90] Canada. CBRN Research and Technology Initiative. *CRTI Framework*. (May 2002). http://www.crti.drdc-rddc.gc.ca/about/framework_e.html; Internet; accessed 3April 2005.

[91] United States. Department of Homeland Security. Science and Technology Directorate Strategic Objectives; http:/www.dhs.gov/dshpublic/; Internet; accessed 18 March 2005.

[92] United States. Committee on Science and Technology for Countering Terrorism. *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism.* National Research Council of the National Academy of Sciences. Washington, D.C, National Academic Press (2002). The report also identifies 7 areas where the immediate application of existing technologies can substantially improve security. http://www.nap.edu/openbook/0309084814/html/R1.html, Internet, accessed 3 April 2005.

[93] Thomas M. Garwin, Neal A. Pollard, and Robert V. Tuohy, *Project Responder: National Technology Plan for Emergency Response to Catastrophic Terrorism*, Oklahoma: National Memorial Institute for the Prevention of Terrorsim, (April 2004).

Annex 4: Canada - U.S. Binational Public Security Technical Program

CA US PSTP Mission Area Priorities

CBRNE	Disruption and Interdiction	Critical Infrastructure Protection Physical/Cyber	Systems Integration, Standards and Analysis
Improve S&T interoperability for operational reach back Develop technologies for early event and critical point detection Progress immediate consequence management techniques for CBRNE hazards Deliver methodologies and protocols for recovery and long-term consequence management	Reduce vulnerability of people, conveyances and cargo from deliberate harm or compromise while ensuring flow of commerce Enhance officer safety; Improve surveillance and domain awareness capability aimed at knowledge discovery and dissemination from data and information Conduct effective, accurate and timely detection and alert of suspicious events Determine intent Disrupt human threat through assessment of alternatives and selection of most appropriate course of action Ensure seamless communications interoperability between authorities to support disruption and interdiction functions Conduct effective targeting and intervention.	**PHYSICAL** Develop, assess and deploy tools for: CIP decision-support systems Standardized vulnerability and risk assessment/analysis New design architectures and retrofits for increased security and protection (enhanced robustness and resiliency) **CYBER** Develop, assess and deploy tools for: Secure network architecture and management Cyber event management; and Network Analysis and Modelling	Advance the evolution towards Public Safety and Security integrated capabilities Improve national risk and vulnerability assessment capabilities Champion new and emerging methodologies for Public Safety and Security decision making; Enable interoperability of bi-national Public Safety and Security capabilities; Facilitate the integration and uptake of S&T solutions delivered by the PSTP Mission Areas.

BIBLIOGRAPHY

TERRORISM

Periodical Articles

Betts, Richard K. The New Threat of Mass Destruction." *Foreign Affairs* 77, no. 1 (January/February 1998): 26-41.

Byman, D. "Scoring the War on Terrorism." *National Interest,* Issue 72 (Summer 2003): 75.

Carter, Ashton, John Deutch, and Philip Zelikow. "Catastrophic Terrorism: Tackling the New Danger." *Foreign Affairs* 77, no. 6 (November/December 1998): 80-94.

Cronin, Audrey Kurth. "Terrorist Motivations for Chemical and Biological Weapons Use: Placing the Threat in Context." *Defense and Security Analysis* 20, no. 4 (December 2004): 313-320.

Franck, Raymond E., and Francois Melese. "Exploring the Structure of Terrorists' WMD Decisions: A Game Theory Approach." *Defense and Security Analysis* 20, no. 4 (December 2004): 355-372.

Garrick, B. John. "Perspectives on the Use of Risk Assessment to Address Terrorism." *Risk Analysis* 22, No.3 (2002): 421-423.

Giddens, A. "Scaring people maybe the only way to avoid the risks of new-style terrorism." *New Statesman* 134, iss. 4721 (2005): 29.

Gunaratna, Rohan. "Defeating Al Qaeda-The Pioneering Vanguard of the Islamic Movements." *Defeating Terrorism: Shaping the New Security Environment*. R.D. Howard and R.L. Sawyer, eds., Guilford, CT: McGraw-Hill, , 2004.

Henry, Terrence. "Al-Qaeda's Resurgence," *The Atlantic Monthly*, June 2004, 54-55.

Hoffman, Bruce. "Terrorist Targeting: Tactics, Trends, and Potentialities." *Terrorism & Political Violence* 5, Issue 2 (Summer 93): 12-30.

Hoffman, Bruce. "The Changing Face of Al Qaeda and the Global War on Terrorism." *Studies in Conflict & Terrorism* 27, Issue 6 (Nov/Dec 2004): 549-560.

Hoffman, Bruce. "The Logic of Suicide Terrorism, in Defeating Terrorism: Shaping the New Security Environment." R.D. Howard and R.L. Sawyer, eds., Guilford, CT: McGraw-Hill, , 2004, 103-113.

Hoffman, Bruce, "Plan of Attack," *The Atlantic Monthly*, July/August 2004, 42

Kay, J. "Outmanoeuvring Terror: Redefining the Terrorist." *National Interest* Issue 75 (Spring 2004): 87-94

McMillan, J. “Apocalyptic Terrorism: The Case for Preventive Action.” *Strategic Forum* No. 212 (November 2004): 1-6.

McAllister, Brad. “Al Qaeda and the Innovative Firm: Demythologizing the Network.” *Studies in Conflict & Terrorism* 27, Issue 4 (July/August 2004): 297-319.

Nacos, Brigitte L. “The Terrorist Calculus behind 9-11: A Model for Future Terrorism?” *Studies in Conflict & Terrorism* 26, Issue 1 (January 2003): 1-16.

Quillen, Chris. “Mass Casualty Bombings Chronology.” *Studies in Conflict & Terrorism* 25, Issue 5 (September 2002): 293-302.

Quillen, Chris. “A Historical Analysis of Mass Casualty Bombers.” *Studies in Conflict & Terrorism* 25, Issue 5 (September 2002): 279-292.

Robbins, James S. “Defeating Networked Terrorism.” in *Defeating Terrorism: Shaping the New Security Environment*, R.D. Howard and R.L. Sawyer, eds., Guilford, CT: McGraw-Hill, 2004.

Rubbelke, Dirk T.G. “Differing Motivations for Terrorism,” *Defence and Peace Economics* 16, no. 1 (February 2005): 19-27.

Schbley, Ayla. “Religious Terrorism, the Media, and International Islamization Terrorism: Justifying the Unjustifiable.” *Studies in Conflict & Terrorism* 27, Issue 3 (May/June 2004): 207-233.

Terrence, Henry. “Al-Qaeda’s Resurgence,” *The Atlantic Monthly*, June 2004, 54.

Books

Hoffman, Bruce. *Inside Terrorism.* London: Victor Gollancz Publisher, 1998.

Laqueur, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction.* New York: Oxford University Press, 1999.

Laqueur, Walter. *A History of Terrorism*. New Brunswick, NJ: Transaction Publishers, 2002

Laqueur, Walter. *No End to War: terrorism in the twenty-first century.* London: Continuum, 2003.

Pyszczynski, Tom, Sheldon Solomon, and Jeff Greenberg. *In the Wake of 9/11: The Psychology of Terror*

Periodical Articles

Delvoie, L. A. "A Not So Benign New Century: Conventional Security Challenges To Canadian Interests." *International Journal* 57, Issue 1 (2002): 19-35.

Coffin, Bill. "Forecasting Terrorism Loss." *Risk Management* 49, no. 11 (November 2002): 8-9.

Coffin, Bill. "Terrorism in 2005", *Risk Management*, (January 2005): 34-39.

Covello, Vincent T., Richard G. Peters, Joseph G. Wojtecki, and Richard C. Hyde. "Risk Communication, the West Nile Virus Epidemic, and Bioterrorism: responding to the Communication Challenges Posed by the Intentional or Unintentional Release of a Pathogen in an Urban Setting." *Journal of Urban Health: Bulletin of the New York Academy of Medicine*, 78, no.22 (2001): 382-391.

Durodie, Bill and Simon Wessely. "Resilience or Panic? The public and Terrorist Attack." *The Lancet*, 360 (December 14, 2003): 1901-2.

Falkenrath, Richard. "Analytic Models and Policy Prescription: Understanding Recent Innovation in U.S. Counterterrorism." *Studies in Conflict & Terrorism* 24, Issue 3 (May 2001): 159-181.

Faria, Jaoa Ricardo. "Terrorist Innovations and Anti-terrorist Policies, University of Texas at Dallas Political Economy Working Paper 09/04, September 2004.

Garrick, B. John. "Perspectives on the Use of Risk Assessment to Address Terrorism." *Risk Analysis* 22, no.3 (2002): 421-423.

Giddens, Anthony. "Scaring People Maybe The Only Way to Avoid the Risks of New-Style Terrorism," *New Statesman* 134, Issue 4721 (January 2005): 29-31.

Kunreuther, Howard. "Risk Analysis and Risk Management in an Uncertain World." *Risk Analysis* 22, no. 4 (2002): 655-664.

Larrabee, F. S., J. Gordon IV, and P.A. Wilson. "The Right Stuff." *National Interest* Issue 77 (Fall 2004): 50-59.

Major, John A. "Advanced Techniques for Modeling Terrorism Risk." *The Journal of Risk Finance* (Fall 2002): 15.

Seebeck, Lesley. "Cadence, War and Security." *Australian Journal of International Affairs* 58, Issue 4 (Dec 2004): 494-510.

Slovic, Paul, "Terrorism as Hazard: A New Species of Trouble." *Risk Analysis* 22, no. 3, (2002): 425-426.

Woo, Gordon. "Quantitative Terrorism Risk Assessment." *The Journal of Risk Finance* (Fall 2002): 7-14.

Zelikow, Philip. "The Transformation of National Security." *National Interest* (Spring 2003): 17-28.

Books

Bullock, J.A., G.D. Haddow, D. Coppola, E. Ergin, L. Watterman, and S. Yeletaysi. *Introduction to Homeland Security.* Burlington, Massachusetts: Elsevier Butterworth-Heinemann, 2005.

Howard, R.D. and R.L. Sawyer, eds. *Defeating Terrorism: Shaping the New Security Environment.* Guilford, CT: McGraw-Hill, 2004.

Viscusi, W. Kip, ed. *Risks of Terrorism*. Boston: Kluwer Academic, 2003.

Davies, J.L. and T. R. Gurr, eds. *Preventive Measures: Building Risk Assessment And Crisis Early Warning Systems*, Lanham, Maryland: Rowan and Littlefield Publishers Inc., 1998.

Cordesman, A. H. *Terrorism, Asymmetric Warfare And Weapons Of Mass Destruction: Defending The U.S. Homeland*, Westport, Connecticut: Center for Strategic and International Studies, Praeger Publishers, 2002.

Hough, Peter, *Understanding Global Security*, London: Routledge, 2004.

CAPABILITY AND SCENARIO BASED PLANNING

Periodicals

Schoemaker, Paul J.H. "Scenario Planning: A Tool for Strategic Thinking." *Sloan Management Review* 36, no. 2 (Winter 1995): 25-39.

Wack, Pierre. "Scenarios: Shooting the Rapids." *Harvard Business Review* 63, no. 6 (November/December 1985): 139-150.

Wack, Pierre. "Scenarios: Uncharted Waters Ahead." *Harvard Business Review* 63, no. 5 (September/October 1985): 73-89.

Books

Cronin, Patrick M. *2015, Power and Progress,* Washington, D.C. National Defence University Press, 1996.

Davis, Jacquelyn K. *Strategic Paradigms 2025: U.S. Security Planning for a New Era,* Washington, D.C. Brassey's Institute for Foreign Policy Analysis, 1999.

PUBLIC DOCUMENTS

Canada. Privy Council Office, *Securing an Open Society: Canada's National Security Policy*. Ottawa: 2004)

Canada. Department of National Defence. *1994 Defence White Paper*. Ottawa: Canada Communications Group Publishing, 1994.

United Kingdom. House of Commons Science and Technology Committee. *The Scientific Response to Terrorsim*. London, UK: The Stationery Office Limited, 6 November 2003.

United States. The White House. *The Department of Homeland Security*. Washington, D.C.; June 2002; available from http://whitehouse.gov/homeland/book/nat_strat_hls.pdf; Internet; accessed 2 April 2005.

United States. Department of Defence. *Quadrennial Defense Review Report*. Washington: Government of the United States of America, September 30, 2001; available from http://www.defenselink.mil/pubs/qdr2001.pdf; Internet; accessed 14 March 2005.

United States. The White House. *National Strategy to Combat Weapons of Mass Destruction*. Washington, D.C.: July 2002; available from http://www.whitehouse.gov/news/releases/2002/12/WMDStrategy.pdf; Internet; accessed 2 April 2005.

United States. The White House. *National Security Strategy of the United States of America*. Washington, D.C.: September 2002; available from http://www.whitehouse.gov/nsc/nss.html; Internet; accessed 2 April 2005.

United States. The White House. *National Strategy for Combating Terrorsim*. Washington, D.C.: February 2003; available from http://www.whitehouse.gov/news/releases/2003/02/counter_terrorism_strategy.pdf; Internet; accessed 2 April 2005.

United States. The White House. *Securing the Homeland Strengthening the Nation*. Washington, D.C.: 2003; available from http://www.whitehouse.gov/homeland/homeland_security_book.html; Internet; accessed 2 April 2005.

United States. Department of Homeland Security. *Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan*. Washington, D.C.: 2004; available from http://www.dhs.gov/interweb/assetlibrary/DHS_StratPlan_Final_spread.pdf; Internet; accessed 2 April 2005.