Senate Sénat
CANADA

SECURITY, FREEDOM AND THE COMPLEX TERRORIST THREAT: POSITIVE STEPS AHEAD

The Honourable Hugh Segal
Chair

The Honourable Serge Joyal, P.C.
Deputy Chair

Interim Report of the Special Senate Committee on Anti-terrorism

March 2011

Ce document est disponible en français.

****

Available on the Parliamentary Internet:
www.parl.gc.ca
(Committee Business – Senate – Reports)
40th Parliament – 3rd Session

TABLE OF CONTENTS

MEMBERS

The Honourable Hugh Segal, Chair
The Honourable Serge Joyal, P.C., Deputy Chair

The Honourable Senators:
George Furey
Mobina S.B. Jaffer
Elizabeth Marshall
Pierre Claude Nolin
David P. Smith, P.C.
David Tkachuk
Pamela Wallin

Ex officio members of the committee:
The Honourable Marjory LeBreton, P.C., (or Gérald Comeau) and James Cowan (or Claudette Tardif).

Other Senators who have participated from time to time in the study:
The Honourable Senators Roméo Dallaire, Michael Duffy, Fabian Manning, Grant Mitchell, Dennis Glen Patterson and Donald Neil Plett.

Parliamentary Information and Research Service, Library of Parliament:
Dominique Valiquet and Cynthia Kirkby, analysts.

Clerk of the Committee:
Barbara Reynolds

ORDER OF REFERENCE

Extract from the Journals of the Senate, Thursday, May 27, 2010:

The Honourable Senator Comeau moved, seconded by the Honourable Senator Di Nino:

That the Special Senate Committee on Anti-terrorism be authorized to examine and report on matters relating to anti-terrorism.

The question being put on the motion, it was adopted.

Gary W. O'Brien

Clerk of the Senate

THE COMMITTEE'S RECOMMENDATIONS

CHAPTER 1: THE CHANGING THREAT ENVIRONMENT

(1) That, given the lack of a strong research basis specific to the transition from radicalization into violence in Canada, the federal government provide support, including financial support, to enable others to conduct such research, in order to better understand and prevent violent extremism, and consider funding programs that have been proven to be successful that focus on countering radicalization leading to violence specifically.

(2) That the federal government work with relevant stakeholders, including private partners, and study the technology used in combating child pornography, to seek, through the application of existing laws, to counter the role of the Internet and other means of telecommunication in radicalization, not through censorship, but through such methods as limiting the circumstances in which potentially radicalizing material is automatically suggested to an audience that did not necessarily look for it and encouraging community leadership to respond to messages and websites that glorify and encourage violence or terrorist acts.

(3) That the Department of Justice publish and table a factual report on Canada's recent terrorism prosecutions on a routine and timely basis, both to inform the public with respect to the facts of these cases and to ensure that lessons learned are shared with all law enforcement agencies and prosecution services across Canada.

(4) That the federal government conduct a review of section 83.26 of the *Criminal Code* to determine whether amendments are required to provide better guidance to the courts with respect to the role of the "totality principle" in imposing consecutive sentences for terrorism-related offences, in a way that does not limit the Crown from seeking, or the judge from imposing, longer sentences as circumstances may require.

(5) That the federal government, in conjunction with its provincial and territorial counterparts, work with law enforcement and intelligence agencies involved in the fight against terrorism to develop policies and practices to ensure that, while necessary intelligence and policing should be robust, lawful and engaged, racial profiling is not used as a shortcut.

(6) That the federal government, in conjunction with its provincial and territorial counterparts, work with law enforcement and intelligence agencies to accelerate efforts to recruit employees who better reflect the diversity of the Canadian population, to achieve a workforce of approximately 16% visible minority employees within three years, so as to increase the likelihood that members of minority communities will be able to communicate with authorities in their own languages and in an atmosphere of cultural awareness.

(7) That the federal government reiterate its commitment to the Cross-Cultural Roundtable on Security (CCRS), and take steps to (i) increase its independence from the Department of Public Safety, (ii) ensure that information flows from communities to the

Government, as well as vice versa, (iii) ensure appointments to the CCRS are current, and (iv) when appointing new members to the CCRS, ensure the individuals appointed are representative of the communities most directly affected by national security policy.

CHAPTER 2: CHALLENGES ASSOCIATED WITH TERRORISM INVESTIGATIONS AND PROSECUTIONS

(8) That the role of the National Security Advisor (NSA) be expanded through legislation that clearly establishes the NSA's functions and powers with respect to coordinating national security activities, resolving disputes between agencies with national security responsibilities, and overseeing the effectiveness of government activities in national security. The National Security Advisor must also have the authority to transmit information received from an agency regarding a national security threat to other agencies responsible for national security.

(9) That the *Canadian Security Intelligence Service Act* be amended (i) to require that CSIS provide to the appropriate law enforcement agencies, or to the National Security Advisor, information that may be used in an investigation or prosecution regarding an offence constituting a "threat to the security of Canada" within the meaning of section 2 of that Act; (ii) when it is possible and reasonable to expect that the intelligence will be relevant to an investigation or criminal prosecution, to require that CSIS retain intelligence collected during an investigation into threats to the security of Canada (such as operational notes, tapes of interviews, and verbatim transcripts of intercepted communications); (iii) to require that CSIS collect and provide this material so as to comply with the rules of evidence and disclosure; and (iv) to clarify that the transfer of a human source from CSIS to a police service will not prevent the police service from invoking the police informer privilege. Disputes over the use of a human source could be resolved through the intervention of the National Security Advisor.

(10) That the federal government examine the importance of amending section 12 of the *Canadian Security Intelligence Service Act* in order to clarify and ensure CSIS's right to utilize lawful disruption as a method of preventing terrorist attacks, and that CSIS establish an official procedure and formal guidelines on the terms and conditions of utilizing such preventive activities. These should require CSIS to report all cases of disruption to the Minister of Public Safety, in a manner similar to that set out at section 25.1 of the *Criminal Code* and following, with respect to the requirements imposed on designated public officers.

(11) That the federal government examine whether it would be useful to amend the legislation governing national security agencies other than the Canadian Security Intelligence Service, such as the Royal Canadian Mounted Police, the Department of Foreign Affairs and International Trade, the Canada Border Services Agency and the Communications Security Establishment, to allow those agencies to transmit to the National Security Advisor information relating to national security that would be relevant to the NSA's proposed expanded mandate.

(12) That the federal government allocate appropriate resources to ensure the protection of Canada's critical infrastructure, for example with respect to the robust use of all available satellite technologies, and that it adopt, in a manner that is consistent with and reinforces the purposes of the *Emergency Management Act* and the new legislative framework expanding the mandate of the National Security Advisor, a proactive approach, notably in establishing secure information sharing systems and protocols with the private sector, provincial and territorial governments, and international partners.

(13) That the federal Minister of Justice consult with his or her provincial and territorial counterparts on the usefulness of amending sections 38 to 38.16 of the *Canada Evidence Act* so as to abrogate the two-court system in criminal law and to permit the trial judge to make decisions regarding confidentiality related to national security, to examine secret intelligence, to review his or her initial confidentiality orders, and to ensure due process of law through adequate safeguards, including, where applicable, through the assistance of a special advocate.

(14) That the federal government examine, particularly in anticipation of the statutory review mandated for 2011, the usefulness of amending the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations to reduce the $10,000 threshold for financial transactions related to terrorist financing, and to include, in the definition of "monetary instruments," prepaid cards and mobile communications devices that are used to transfer funds. To that end, the government shall carry out a "cost-benefit" analysis, giving consideration, for example, to costs for the private sector, protection of personal information, and the operational capacity of the Financial Transactions and Reports Analysis Centre of Canada.

(15) That the statutory mandate of the National Security Advisor include evaluating the integration and effectiveness of the Financial Transactions and Reports Analysis Centre of Canada.

CHAPTER 3: PARLIAMENTARY OVERSIGHT OF CANADA'S NATIONAL SECURITY

(16) That, consistent with the practices in the United Kingdom, Australia, France, the Netherlands, and the United States, the federal government constitute, through legislation, a committee composed of members from both chambers of Parliament, to execute Parliamentary oversight over the expenditures, administration and policy of federal departments and agencies in relation to national security, in order to ensure that they are effectively serving national security interests, are respecting the *Canadian Charter of Rights and Freedoms,* and are fiscally responsible and properly organized and managed.

The proposed committee of Parliamentarians shall have the same right to access information as the Security Intelligence Review Committee. Members of the Committee shall be appointed by the Governor in Council, and will hold office during periods of prorogation. Meetings of the Committee shall be held *in camera* whenever the Chair, a majority of members present or the Minister considers it necessary for the Committee to

do so. Members of the committee shall be required to swear an oath of secrecy similar to that found in the schedule to the *Canadian Security Intelligence Service Act* or to the Oath of a Privy Councillor, or both, and be permanently and statutorily bound to secrecy for purposes of application of the *Security of Information Act.* The committee shall report to the Prime Minister, who would make that report public within 60 days of receipt. When matters in the report need to be removed for national security reasons, the report, when made public, must indicate that this has transpired.

INTRODUCTION

The fight against terrorism requires striking a delicate balance. On the one hand, terrorism represents a unique and potentially devastating threat to national security, and the public must be protected through vigilant intelligence gathering and proactive law enforcement. On the other hand, Canada has a strong history of commitment to human rights and the rule of law, as evidenced by the *Canadian Bill of Rights*, the common law and the *Civil Code*, and the Canadian constitution, including the *Canadian Charter of Rights and Freedoms*, and the ratification of various international human rights agreements. Attempting to safeguard civil liberties and freedom while also keeping people safe from the threat of terrorism is not an easy feat. The purpose of detecting, preventing, acting lawfully against and prosecuting terrorist acts is to keep Canada and Canadians safe from those who would imperil our democratic freedom, core values and tolerant way of life, by harming Canadians through acts of violence. We must keep in mind what and who we are protecting, as well as how best to protect Canadians against a diverse and serious threat spectrum. The study undertaken by the Special Senate Committee on Anti-terrorism (the Committee) seeks to determine how best such a balance can be struck in this country and its resultant recommendations set out guidelines to help in achieving the end of keeping Canadians both safe and free.

BACKGROUND

In February of 2007, the Special Senate Committee on the *Anti-Terrorism Act* tabled *Fundamental Justice in Extraordinary Times*,[1] after reviewing the *Anti-Terrorism Act*, enacted in 2001 in the aftermath of the September 11 attacks in the United States, as well as the entire Canadian anti-terrorism framework. The Committee crafted a total of 40 recommendations, ranging in scope from amending specific aspects of Canadian legislation through to showing leadership in engaging the United Nations on the issue of how to properly deal with alleged or known terrorists.

[1] Special Senate Committee on the *Anti-Terrorism Act*, Main Report: Fundamental Justice in Extraordinary Times, February 2007. The Committee tabled a separate report on 28 March 2007, subsequent to the Supreme Court of Canada's decision in *Charkaoui* v. *Canada (Citizenship and Immigration)*, [2007] 1 S.C.R. 350, 2007 SCC 9.

In May 2010, the Special Senate Committee on Anti-terrorism (this Committee) was created and authorized, by Order of Reference from the Senate dated 27 May 2010, to examine and report on matters relating to anti-terrorism. To that end, the Committee held 11 hearings between 13 May 2010 and February 14, 2011, and heard from 32 witnesses, including scholars and members of the law enforcement and intelligence communities, from countries including Canada, the United States, the United Kingdom, and Australia. This report focuses on the broad themes that emerged from this study: the changing threat environment (Chapter 1), the challenges associated with terrorism investigations and prosecutions (Chapter 2), and Parliamentary oversight of Canada's national security (Chapter 3).

CHAPTER 1: THE CHANGING THREAT ENVIRONMENT

1. Background

In *Fundamental Justice in Extraordinary Times*, the Committee noted that the terrorist threat had not abated since the attacks on 11 September 2001, and that in fact the war in Iraq seemed to be exacerbating the problem by radicalizing many Islamist ideologues. This Committee has since heard that Islamist extremism, as practised or inspired by Al Qaida, remains the pre-eminent terrorist threat to western countries, including Canada, and, according to Monik Beauregard, Director of the Integrated Threat Assessment Centre, Canada has been specifically identified by Al Qaida as a viable target on more than one occasion.[2]

The listing of an entity under section 83.05 of the *Criminal Code* is a public means in this country of identifying a group or individual as being associated with terrorism. The Governor in Council, on the recommendation of the Minister of Public Safety, may add an entity to the list if there are reasonable grounds to believe that the entity has knowingly been involved in a terrorist activity or is knowingly assisting a terrorist group. A review of the listed entities must be conducted every two years, to determine whether there are still reasonable grounds for an entity to be listed. The review completed on 23 December 2010 demonstrates the centrality of Islamist extremism as a threat to Canada and to Canadians. Following the review, all previously listed entities remained on the list, including Al Qaida, Al Qaida in the Islamic Maghreb,[3] and Al Shabaab, which, according to some recent news reports, is now considered to be the number one threat to national security. Al Qaida in the Arabian Peninsula has also been added as a listed entity, after claiming responsibility for the attempt to ship explosives hidden in ink cartridges on cargo planes destined to Chicago from Yemen.[4]

Although some experts believe that the jihadi movement is weaker today than it was five years ago, as demonstrated by the failure of Al Qaida to mount successful major attacks against

[2] Special Senate Committee on Anti-Terrorism, Evidence, 31 May 2010 (evidence of Monik Beauregard, Director, Integrated Threat Assessment Centre).

[3] Al Qaida in the Islamic Maghreb had previously been known as Salafist Group for Call and Combat.

[4] Public Safety Canada, The Government of Canada lists Al Qaida in the Arabian Peninsula as a terrorist entity, 23 December 2010.

the West and by the decline of popular support in the Muslim world for Al Qaida, this Committee is of the opinion that the threat of terrorism in Canada remains strong, and is evolving. This evolution includes, in recent years, the phenomenon of radicalization and "home-grown" terrorism, as part of "a global shift in terrorism toward decentralized, autonomously radicalized, violent jihadist individuals or groups who strike in their home countries."[5] Such attacks may be harder to detect and prevent because they can be planned and executed more quickly, by individuals who blend in due to their familiarity with local culture and customs, without the enhanced scrutiny that results from crossing international borders.

There is also some suggestion that, given this operational shift, the threat is evolving towards the goal of inflicting maximum economic damage, if not mass casualties. Al Qaida in the Arabian Peninsula is said to have boasted that expenses for the "supposedly 'foiled plot'" involving ink cartridges totalled $4,200 but costs to the U.S. and other Western countries would be in the billions of dollars in terms of new security measures, reflecting a new strategy of low-cost attacks designed to inflict broad economic damage.

Finally, the Internet plays an increasing role in the changing threat environment. Although there is less consensus on the likelihood of terrorist attacks against websites or Internet-based databases themselves or attacks via the Internet that cause damage to real-world infrastructure, this Committee heard that the Internet plays a growing role in the radicalization process, as will be discussed in further detail below, and also offers terrorists operational capabilities, for example by enabling terrorist groups to collect intelligence about their targets, communicate with one another, plot strategy and tactics, and raise funds. The potential also exists, however, to combat terrorism through the Internet, although as always, the appropriate balance between security and civil liberties must be sought, to ensure that the vast majority of individuals, who do not pose a threat to national security, are able to conduct their business without fear of being monitored without lawful reason.

[5] Jerome P. Bjelopera and Mark A. Randol, American Jihadist Terrorism: Combating a Complex Threat, Congressional Research Service, 7 December 2010, p. 7, citing Marc Sageman.

2. Radicalization

The RCMP has defined radicalization as "the process by which individuals — usually young people — are introduced to an overtly ideological message and belief system that encourages movement from moderate, mainstream beliefs towards extreme views."[6] While much of the current focus is on Islamist extremism, Canadian research notes that radicalization is not limited to any single ethnic or interest group; it has spanned the entire "left-right" political spectrum, from environmental and animal rights activists to neo-Nazis, as well as a range of ethnic and religious interests.[7]

2.1 From Radicalization into Violence

Research into the radicalization process has identified certain commonalities among individuals involved in terrorism, particularly in the context of Islamist extremism. The RCMP notes, for example, that although poverty and alienation are popular explanations for what drives people towards terrorism, "many dangerous extremists spring from the ranks of the privileged middle and upper-middle classes."[8] Similarly, in an influential report, the New York Police Department noted that "fifteen to thirty-five year-old male Muslims who live in male-dominated societies are particularly vulnerable" and that "[m]iddle class families and students appear to provide the most fertile ground for the seeds of radicalization."[9] Religious conversion may also play a key role in the radicalization of some individuals.

Other research has emphasized that these commonalities or indicators are not "root causes," since they are neither sufficient nor necessary conditions for terrorism, but are rather "permissive factors," in that they may help establish an environment in which terrorism is *more likely* to occur.[10] These permissive factors may be categorized as global factors, state factors, or sociocultural factors. Global factors include foreign policy decisions and military interventions, and, due to the globalised media, including the Internet, foreign grievances may resonate more

[6] Royal Canadian Mounted Police, Radicalization – A Guide for the Perplexed, June 2009, p. 1.

[7] Royal Canadian Mounted Police, Radicalization – A Guide for the Perplexed, June 2009, p. 2; Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, December 2010, p 13.

[8] Royal Canadian Mounted Police, Radicalization – A Guide for the Perplexed, June 2009, p. 5.

[9] New York Police Department, Radicalization in the West: The Homegrown Threat, 2007, p. 22.

[10] Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, December 2010, pp. 37-38.

strongly than they otherwise would. State factors include educational, professional and economic disadvantages, whether real or perceived, and recent reports indicate that Al Shabaab may be exploiting real or perceived discrimination in the employment context to recruit Canadian Muslim youth, arguing they will never get a job in this country, even if they have multiple degrees. Finally, sociocultural factors "are a complex mixture of characteristics relating to ideology, culture and identity," and the role of ideology and religion are particularly contentious.[11]

In particular, the Committee notes the impact of peer groups on the transition from radicalization into violence. Canadian research has found that a number of home-grown terrorists "have found the idea of violent jihad attractive for non-religious reasons: because they find it cool and exciting."[12] The firing of guns, including paintball guns, and the development of a sense of "brotherhood" are seen by some as fun and exciting, regardless of whether they constitute aspects of terrorist training or an adventure camp. Radicalization may also increase status within the peer group, in that higher status may be accorded to members demonstrating more defiant or violent tendencies and language.

The RCMP notes that, while radical thinking is not in itself a problem, "it becomes a threat to national security when Canadian citizens or residents espouse or engage in violence or direct action as a means of promoting political, ideological or religious extremism."[13] It is the movement from radical thinking to the consideration of violence that is a key watershed.

Although it has been subject to criticism, the "stage" model developed by the NYPD, and referred to by several witnesses, may be useful in illustrating this point. According to this model, which is focused on the context of jihadi-Salafi ideology and based on a review of nearly a dozen terrorist-related cases, there are four distinct stages to the process of radicalization. The first stage, Pre-Radicalization, describes an individual's world prior to the journey into radicalization, including his or her lifestyle, religion, social status, and education. The second stage, Self-Identification, involves the beginning of a "religious seeking," often following an economic,

[11] Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, December 2010, pp. 37-39.

[12] Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, December 2010, p. 99.

[13] Royal Canadian Mounted Police, Radicalization – A Guide for the Perplexed, June 2009, p. 1.

social, political, or personal crisis. At the third stage, Indoctrination, the individual wholly adopts jihadi-Salafi ideology and concludes that militant jihad is required to support and further the Salafist cause, and joins a cluster of like-minded individuals. It is the fourth and final stage, Jihadization, which is the critical stage that leads to a terrorist attack: members of the cluster accept their individual duty to participate in jihad, and begin planning for a terrorist attack. Not everyone who begins the process completes it or even necessarily proceeds in a linear manner, but, according to this theory, individuals who do pass through the entire process are "quite likely" to be involved in a terrorist attack.[14]

What is important from a public security standpoint is how to identify *which* radicals will become involved in violent extremism, since only "a handful" of radicals will go on to become terrorists.[15] With the exception of a 2010 report released by the UK-based think tank Demos, which contains significant primary research around extremism and radicalism in Canada that has been inspired by Al Qaida, there is little research on radicalization in Canada, and, as that report notes, "[i]t is possible for people to read or have read radical texts, be strongly and vocally opposed to Western foreign policy, believe in Sharia law, hope for the restoration of the caliphate, and even support the principle of Afghan and Iraqi Muslims fighting allied troops, while being extremely vocal in denouncing Al Qaida inspired terrorism in Western countries."[16] That is, existing research into "permissive factors" may be insufficient for distinguishing between radicals and terrorists, or for explaining why certain radicals progress to violent extremism while other similarly situated individuals do not.

2.2 Prevention Strategies

Canadian research notes that there are different tiers of "prevention" or "intervention" work, from the narrowest, which requires intervention by law enforcement with respect to individuals who are actively seeking to break the law, to the broadest, which involves the entire

[14] New York Police Department, Radicalization in the West: The Homegrown Threat, 2007.

[15] Brian Michael Jenkins, Would Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001, Occasional Paper, 2010, p. 7; Special Senate Committee on Anti-Terrorism, Evidence, 6 December 2010 (evidence of Brian Jenkins, Senior Adviser, RAND Corporation).

[16] Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, December 2010, p. 130.

community and focuses on ensuring equitable access to public services, social and economic integration and preventing discrimination.[17]

To the extent that such factors as a lack of social and economic integration contribute to radicalization, prevention work even at this broadest level may be a component of an anti-terrorism strategy. The Committee is aware, however, of research that advises against this approach. As noted in the Demos report, the primary focus of prevention work should be on targeted interventions where there is a clear, identified danger of radicalization to violence; "[i]ncluding issues of social concerns within an al-Qaeda inspired anti-terrorism agenda risks perpetuating the perception that radicalisation to violence is only a concern within Muslim communities and not others."[18]

The experiences of other countries may be instructive. The Committee has been advised about the United Kingdom's Prevent strategy, which was intended to tackle the root causes of radicalization and terrorism in the U.K., but which has suffered from confusion over whether funded programs constitute social work or security work. The U.K. Home Office notes that activity in the areas of race equality, multiculturalism and cohesion has led to accusations that the government's interest in Muslim communities is related only to the risk of terrorism.[19] That is, broad-based prevention work, intended to address permissive factors such as economic disadvantage, should be aimed at society in its entirety, and should be clearly distinct from counter-terrorism strategies.

At the same time, there may be a role for more targeted strategies, aimed at those who have displayed a tendency towards violent radicalization. The Committee heard from Sayyid Ahmed Amiruddin, Chairman of the Al Sunnah Foundation, that some community leaders in mosques are offering de-radicalization programs,[20] and believes that there may be a role for the Government in providing funding to help carry out these programs.

---

[17] Canadian Association of Chiefs of Police, Building Community Resilience to Violent Ideologies, p. 16; Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, p. 57.

[18] Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, pp. 132-133.

[19] U.K. Home Office, Review of the Prevent Strategy.

[20] Special Senate Committee on Anti-Terrorism, Evidence, 4 October 2010 (evidence of Sayyid Ahmed Amiruddin, Chairman, Al Sunnah Foundation).

The Committee also believes that Canada can again learn from the United Kingdom's experience with the Prevent strategy in that it is important to evaluate the success of such programs, so that it becomes clear what works and with what impact.

2.3 The Role of the Internet

This Committee has heard that the Internet facilitates the radicalization process in a variety of ways. The RCMP notes that the Internet is difficult to monitor and control but easy to access, and messages can be distributed to large numbers of people with relative anonymity.[21] The Internet can also function as a sort of "echo chamber," in that individuals may easily find other like-minded individuals to reinforce their beliefs, and legitimize their anger. This may again result in rhetorical one-upmanship, which, as Professor Stéphane Leman-Langlois argues, further complicates the task of distinguishing between those who would progress to a terrorist attack and those who are attracted to radical content but would remain law-abiding.[22]

The interactivity of the Internet may also make it particularly effective as a recruiting tool. Research notes that the Internet may blur the lines between readership and authorship, especially as compared to pamphlets or brochures. This interactivity may encourage those who interact on social networking sites and similar sites to more easily see themselves as part of broader jihadist movements, not just as casual readers or online spectators.[23]

Perhaps the biggest impact of the Internet on the radicalization process stems from the ability to generate an emotional response through the use of audio and video. In particular, this Committee is concerned that jihadi videos can make distant events, perceived as "Muslims under attack," seem local and immediate to would-be home-grown terrorists. Under some circumstances, the act of viewing jihadi videos may create the emotional urge to act in the face of injustice, including, perhaps, through violence.[24]

---

[21] Royal Canadian Mounted Police, Radicalization – A Guide for the Perplexed, June 2009, p. 10.

[22] Special Senate Committee on Anti-Terrorism, Evidence, 4 October 2010 (evidence of Stéphane Leman-Langlois, Professor, University Laval, Director, Terrorism and Counterterrorism Research Group, as an individual).

[23] Jerome P. Bjelopera and Mark A. Randol, American Jihadist Terrorism: Combating a Complex Threat, Congressional Research Service, 7 December 2010, pp. 18 – 19.

[24] Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, pp. 97 – 99.

This Committee has heard that it may be useful to distinguish between radical information that must be specifically sought on the Internet, and radical information that is automatically suggested to viewers who have viewed more moderate material.[25] Websites that automatically suggest jihadi material to visitors may inadvertently reach and radicalize a broader audience, and so consideration could be given to attempting to limit the situations in which such material is presented when it has not been specifically sought. As well, efforts could be made to counter the "echo chamber" effect through the presentation of reasoned arguments that challenge the legitimization of violence.

The Committee recognizes that this would be no easy task, but is nonetheless of the opinion that, given the potential scope of Internet-based radicalization, the federal government should work with relevant stakeholders, including private partners, to seek to develop methods to counter the Internet's role in radicalization, while respecting the right to privacy.

3. Homegrown Terrorism

"Homegrown" or domestic terrorism is not a new phenomenon. In the United States, for example, when measured by the number of terrorist attacks, the volume of domestic terrorist activity was 15 to 20 times greater in the 1970s than in the years following the 11 September 2001 attacks, although domestic terrorists in the 1970s tended to favour symbolic violence, avoiding casualties.[26] With respect to Al Qaida inspired terrorism specifically, the Demos report notes that Europe has been debating the appropriate policy response for the past decade. Canada also has a history of homegrown terrorism, including the attack against Air India Flight 182, which killed 329 passengers and staff on 23 June 1985. The threat is now changing, however, and it may be increasing.

Although a global study conducted in 2010 found Canada to be at "low risk" of terrorist attacks[27] and the data analysed in the Demos report suggested that many of those described as

---

[25] Special Senate Committee on Anti-Terrorism, Evidence, 6 December 2010 (evidence of Thomas Hegghammer, Research Fellow, Norwegian Defence Research Establishment).

[26] Brian Michael Jenkins, Would Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001, Occasional Paper, 2010, pp. 6 and 8; Special Senate Committee on Anti-Terrorism, Evidence, 6 December 2010 (evidence of Brian Jenkins, Senior Adviser, RAND Corporation).

[27] Maplecroft, Somalia overtakes Iraq, Afghanistan, Pakistan and Colombia to become world's terror capital – Global study, 15 November 2010.

violent were not seen as a particular threat to Canada itself,[28] the RCMP has estimated that as many as 50 terrorist organizations are present in some capacity in Canada, and, as of May 2010, CSIS was investigating over 200 individuals in Canada suspected of terrorism-related activities.

3.1 Recent Court Cases

Recent years have seen an increase in incidents of and persons charged with terrorism-related offences in Canada. In fact, one witness informed this Committee that "more Canadians have been indicted on terrorism-related crimes between September 2008 and September 2010 than used to face such charges over decades."[29] The Committee heard from Professor Kent Roach, however, that due to frequent publication bans, the public may not have a complete understanding of the evidence presented in terrorism-related cases,[30] which could, perhaps, result in cynicism or a sense of complacency. The Committee believes that the lack of concise, publicly available information on successful terrorism prosecutions in Canada may also result in the loss of valuable lessons that could assist in future terrorism prosecutions.

With respect to sentencing for terrorism-related offences, a series of decisions released by the Ontario Court of Appeal on 17 December 2010 emphasizes that sentences should reflect the uniquely devastating nature of terrorism. The Court of Appeal increased the sentence imposed on Momin Khawaja, the first person charged under the *Anti-Terrorism Act*, from a total of 10.5 years to life imprisonment with a period of parole ineligibility of ten years,[31] noting that "[w]hen terrorists acting on Canadian soil are apprehended and brought to justice, the responsibility lies with the courts to send a clear and unmistakable message that terrorism is reprehensible and those who choose to engage in it here will pay a very heavy price."[32] Similarly, the Court of Appeal declined to reduce the life sentence imposed on Zakaria Amara, the "mastermind and chief organizer" of a plot in which bombs were to be detonated at the Toronto Stock Exchange

---

[28] Jamie Bartlett, Jonathan Birdwell and Michael King, The Edge of Violence, Demos, p. 123.

[29] Alex Wilner, From Rehabilitation to Recruitment: Islamist Prison Radicalization in Canada, Macdonald-Laurier Institute, October 2010, p. 9; Special Senate Committee on Anti-Terrorism, Evidence, 13 December 2010 (evidence of Alex Wilner, Senior Researcher, Center for Security Studies, ETH Zurich, Switzerland).

[30] Special Senate Committee on Anti-Terrorism, Evidence, 13 December 2010 (evidence of Kent Roach, Prichard-Wilson Chair of Law and Public Policy, Faculty of Law, University of Toronto).

[31] *R. v. Khawaja*, 2010 ONCA 862, para. 3.

[32] *R. v. Khawaja*, 2010 ONCA 862, paras. 187 and 246. Mr. Khawaja has filed an application for leave to appeal to the Supreme Court of Canada.

Tower, the CSIS Headquarters on Front Street in Toronto and an unspecified military base east of Toronto;[33] and increased the sentences for co-conspirators Saad Khalid from 14 years to 20 years with delayed parole[34] and for Saad Gaya from 12 years to 18 years with delayed parole.[35]

The Supreme Court of British Columbia recently applied the same approach in sentencing Inderjit Singh Reyat for perjury, in relation to his testimony at the Air India trial of Ripudaman Singh Malik and Ajaib Singh Bagri. Justice McEwan noted that the *Khawaja* decision concerned terrorist crime rather than perjury, but he held that Reyat's testimony "bespoke a deep and abiding rejection of the values of Canadian society in a new context, in relation to the process of the Court itself."[36] Concluding that "[t]he Court simply cannot leave the impression with would-be terrorists or with the public at large that it will tolerate determined subversion of the premises upon which the whole justice system operates," Justice McEwan sentenced Reyat to nine years for perjury, although the cases introduced by the Crown and the defence suggested a range of penalties for perjury of up to six years.[37]

While this Committee is satisfied that courts are imposing sentences that send a strong message of denunciation and deterrence to terrorists and would-be terrorists, the Committee notes that there may still be some confusion, as discussed in *Khawaja*, with respect to how to reconcile certain provisions in the *Criminal Code.* In particular, section 83.26 of the *Criminal Code* generally requires sentences for terrorism offences to be served consecutively, while section 718.2(c) of the Code sets out the "totality principle," which requires the court to consider whether the combined effect of consecutive sentences would be unduly long or harsh. As a result, some courts may be inclined to impose shorter individual sentences for multiple terrorism-related offences than they otherwise would, so that the combined sentence is not unduly long. This Committee questions whether, as stated in *Khawaja*, this approach could neutralize the

[33] *R. v. Amara*, 2010 ONCA 858, para. 7.

[34] *R. v. Khalid*, 2010 ONCA 861, para. 8.

[35] *R. v. Gaya*, 2010 ONCA 860, para. 6.

[36] *R. v. Reyat*, 2011 BCSC 14, paras. 38 and 72.

[37] *R. v. Reyat*, 2011 BCSC 14, paras. 74 and 84. According to news reports, Mr. Reyat has filed an appeal.

impact of section 83.26,[38] and therefore is of the view that amendments to the Code to clarify the interplay of these provisions may be helpful for future terrorism-related prosecutions.

3.2 Racial Profiling

In *Fundamental Justice in Extraordinary Times*, the Committee noted that many witnesses had expressed concern about the possibility that law enforcement and intelligence agencies would engage in "racial profiling" by targeting individuals or selecting them for investigation solely on the basis of their race, national or ethnic origin, colour or religion, in the exercise of their duties in the fight against terrorism. In particular, concern was raised about the "motivation clause" in the definition of "terrorist activity" found at section 83.01 of the *Criminal Code*, which refers to an act or omission, committed in or outside of Canada, that is "committed in whole or in part for a political, religious or ideological purpose, objective or cause." The Committee recommended that this "motivation clause" be removed, noting that it could encourage racial profiling during investigations and that the Ontario Superior Court of Justice had, at that time, concluded that the clause was unconstitutional and should be severed from the rest of the definition of terrorist activity.[39]

The Ontario Court of Appeal has since ruled, however, that the "motive requirement" is not unconstitutional, although improper police conduct, such as profiling based exclusively on ethnicity or religious belief, could be.[40] That is, there is a distinction to be drawn between an unconstitutional law and the unconstitutional application of a constitutional law. While the Committee acknowledges this distinction, it remains imperative that security and law enforcement agencies not target or profile individuals for scrutiny or investigation based solely on their membership in a particular racial, religious or ethnic group. In addition to representing a disregard for guaranteed rights and liberties, racial profiling can also create a sense of over-policing in affected communities, resulting in distrust and resentment of authorities.

---

[38] *R. v. Khawaja*, 2010 ONCA 862, para. 210.

[39] Fundamental Justice in Extraordinary Times, pp. 11-14 and 20, referring to *R. v. Khawaja*, [2006] O.J. No. 4245 (Sup. Ct. J.) (QL). For similar reasons, the Committee recommended that paragraph (c) of the definition of "threats to the security of Canada" in section 2 of the *Canadian Security and Intelligence Service Act*, R.S.C. 1985, c. C-23, be amended to replace the reference to a political, religious or ideological objective.

[40] *R. v. Khawaja*, 2010 ONCA 862, paras. 134 and 137.

Even where there is no distrust, there may be an *absence* of trust in intelligence and police agencies because those agencies are not well established in affected communities. When the investigation into the bombing of Air India Flight 182 got underway, there were few people in the RCMP who actually spoke Punjabi, in addition to a significant lack of understanding of the culture. This Committee has heard that law enforcement and intelligence agencies are now working hard to recruit members of minority communities as employees, in order to ensure the availability of language skills and cultural awareness. The Canadian Security Intelligence Service (CSIS), for example, advised the Committee that 13 percent of CSIS employees are visible minorities,[41] compared to 16.2 percent[42] of the Canadian population. This is constructive progress.

3.3 The Cross-Cultural Roundtable on Security

One promising Canadian practice is the Cross-Cultural Roundtable on Security (CCRS), created in 2005 to "engage Canadians and the Government of Canada in an ongoing dialogue on national security in a diverse and pluralistic society," by "[p]roviding a forum for Government to present policy initiatives and programs relating to national security and obtain the views of the CCRS as to how such national security measures may impact Canada's diverse communities" and "[f]acilitating a broad exchange of information between the government and communities on policy initiatives and programs relating to national security and the impact of such programs on Canada's diverse communities."[43]

An evaluation published in March of 2008 found that there continues to be a need for the CCRS, as "[n]ational security remains a key priority of the GoC [Government of Canada] and there are no other programs that provide a similar opportunity for dialogue between the GoC and Canada's multicultural communities on issues of national security."[44] Six meetings of the CCRS have been held since then, with themes including "Radicalization Leading to Violence,"

[41] Special Senate Committee on Anti-Terrorism, Evidence, 31 May 2010 (evidence of Charles Bisson, Deputy Director, Operations, Canadian Security Intelligence Service).

[42] Statistics Canada, *The Daily*, 2 April 2008.

[43] Public Safety Canada, Terms of Reference, 20 July 2009.

[44] Government Consulting Services, 2008-2009 Targeted Evaluation of the Cross-Cultural Roundtable on Security, March 2008, p. 28.

"Financing of Terrorism and Organized Crime," and, most recently, in June of 2010, "Border and Immigration."[45]

While the Committee believes the CCRS has great potential, it has not, to date, been an unmitigated success. The Committee is aware of concerns regarding the CCRS, including that there may be at least a perception that it lacks independence if it is seen merely as an extension of the Department of Public Safety; this could increase distrust in the process and decrease participants' willingness to express their perceptions, grievances, and concerns. The Committee has also heard that meetings of the CCRS may be seen less as a roundtable discussion and more as a one-way briefing from the Department, which would not appear to be in keeping with the mandate or intended scope of the CCRS. In addition, it is important to ensure that the right interlocutors are consulted; members of the CCRS must also be representative of the groups most directly affected by national security policy.

The Committee also notes that, under the Terms of Reference, meetings of the CCRS are to be held at least twice a year and no more than four times a year, that the CCRS averaged 2.5 meetings per year between 2005 and 2010, and that there are currently no upcoming meetings listed on the "Meetings" website. In addition, while members are appointed for a term of two years with a possibility of a one-year extension, the most recent notice of appointment on the website is dated 13 March 2008,[46] which raises the question of the mandate of the current members.

In light of these considerations, the Committee recommends:

(1) That, given the lack of a strong research basis specific to the transition from radicalization into violence in Canada, the federal government provide support, including financial support, to enable others to conduct such research, in order to better understand and prevent violent extremism, and consider funding programs that have been proven to be successful that focus on countering radicalization leading to violence specifically.

(2) That the federal government work with relevant stakeholders, including private partners, and study the technology used in combating child pornography, to seek, through the application of existing laws, to counter the role of the Internet and other means of

[45] Public Safety Canada, Meetings of the Roundtable, 5 November 2010.

[46] Public Safety Canada, Ministers Nicholson and Day appoint new members to the Cross-Cultural Roundtable on Security, 13 March 2008.

telecommunication in radicalization, not through censorship, but through such methods as limiting the circumstances in which potentially radicalizing material is automatically suggested to an audience that did not necessarily look for it and encouraging community leadership to respond to messages and websites that glorify and encourage violence or terrorist acts.

(3) That the Department of Justice publish and table a factual report on Canada's recent terrorism prosecutions on a routine and timely basis, both to inform the public with respect to the facts of these cases and to ensure that lessons learned are shared with all law enforcement agencies and prosecution services across Canada.

(4) That the federal government conduct a review of section 83.26 of the *Criminal Code* to determine whether amendments are required to provide better guidance to the courts with respect to the role of the "totality principle" in imposing consecutive sentences for terrorism-related offences, in a way that does not limit the Crown from seeking, or the judge from imposing, longer sentences as circumstances may require.

(5) That the federal government, in conjunction with its provincial and territorial counterparts, work with law enforcement and intelligence agencies involved in the fight against terrorism to develop policies and practices to ensure that, while necessary intelligence and policing should be robust, lawful and engaged, racial profiling is not used as a shortcut.

(6) That the federal government, in conjunction with its provincial and territorial counterparts, work with law enforcement and intelligence agencies to accelerate efforts to recruit employees who better reflect the diversity of the Canadian population, to achieve a workforce of approximately 16% visible minority employees within three years, so as to increase the likelihood that members of minority communities will be able to communicate with authorities in their own languages and in an atmosphere of cultural awareness.

(7) That the federal government reiterate its commitment to the Cross-Cultural Roundtable on Security (CCRS), and take steps to (i) increase its independence from the Department of Public Safety, (ii) ensure that information flows from communities to the Government, as well as vice versa, (iii) ensure appointments to the CCRS are current, and (iv) when appointing new members to the CCRS, ensure the individuals appointed are representative of the communities most directly affected by national security policy.

CHAPTER 2: CHALLENGES ASSOCIATED WITH TERRORISM INVESTIGATIONS AND PROSECUTIONS

1. Inter-agency Cooperation on National Security

A number of agencies in Canada are involved in combatting terrorism, most notably CSIS and the RCMP, but also the Department of Foreign Affairs and International Trade (DFAIT), the Canada Border Services Agency (CBSA) and the Communications Security Establishment (CSE). Each agency, however, has its own mandate and different legislative rules governing the execution of that mandate, particularly with respect to the collection and disclosure of information.

The mandate of CSIS is to collect, analyse, produce and share intelligence in order to inform the government of threats to national security. CSIS frequently invokes the need for secrecy to prevent the release of confidential information. The principal mandate of the RCMP is to prevent crime and to conduct investigations in order to collect evidence admissible in court. The RCMP therefore generally expects that the information it collects will be disclosed to the accused and referred to in public trials. As terrorism is both a crime and a threat to the security of Canada, both agencies exercise jurisdiction in this area. This overlap of mandates creates a constant tension between the desire to preserve the secrecy of security intelligence and the requirement to ensure that judicial proceedings are transparent. Ascribing too much importance to the preservation of secrecy can create an obstacle to the effective sharing of information, in that it fosters a "compartmentalized" approach to national security. The proper balance between these two objectives must be achieved.

1.1 Information Sharing

During this Committee's study, representatives from the organizations responsible for law enforcement and national security in Canada, Charles Bisson from CSIS and Monik Beauregard from ITAC in particular, said that they were relatively satisfied with the sharing of information and that the relationship between the agencies had "never been better than it is

today."[47] The Committee does not doubt their good faith and assumes that they cooperate and share information, but the changing nature of the terrorist threat demands an increasingly multidisciplinary approach which goes beyond traditional policing strategies. While these organizations have adopted new structures that facilitate information sharing – for example, the Integrated National Security Enforcement Teams (INSET), Integrated Threat Assessment Centre (ITAC), Secure Police Reporting Operating System (SPROS) and the CSIS-RCMP Joint Management Team – needless compartmentalization of information about terrorist threats and lack of coordination still seem to persist today, to some degree.[48]

According to Professor Martin Rudner, no one agency has an overview of the mosaic of intelligence collected by the various Canadian organizations, which would be necessary to implement an effective government-wide anti-terrorism strategy.[49] Although CSIS, the CBSA and the RCMP report to the Minister of Public Safety, the same is not true of other important stakeholders such as DFAIT, the Minister of National Defence, the CSE, anti-terrorist units of provincial and municipal police agencies, and the Attorney General of Canada, who is responsible for anti-terrorist prosecutions and for the protection of confidential information during court proceedings. It is the Committee's opinion that national security issues are too important to be entrusted to a single department or agency, and it should not be the role of a minister to be involved in the management of any national security investigation. That responsibility must fall instead to the National Security Advisor (NSA), as recommended by the Air India Commission of Inquiry and endorsed by various witnesses heard by the Committee.[50]

The NSA, one of the most senior officials of the Privy Council Office (PCO), was appointed in 2003 "to improve coordination and integration of security efforts among

---

[47] Special Senate Committee on Anti-Terrorism, Evidence, 31 May 2010 (Charles Bisson, Deputy Director, Operations, Canadian Security Intelligence Service).

[48] Special Senate Committee on Anti-Terrorism, Evidence, 7 June 2010 (evidence of John Thompson, President, Mackenzie Institute), and 21 June 2010 (evidence of Tom Quiggin, Senior Research Fellow, Canadian Centre of Intelligence and Security Studies, Carleton University).

[49] Special Senate Committee on Anti-Terrorism, Evidence, 21 June 2010 (evidence of Martin Rudner, Distinguished Research Professor Emeritus, Carleton University).

[50] Special Senate Committee on Anti-Terrorism, Evidence, 21 June 2010 (evidence of Martin Rudner, Distinguished Research Professor Emeritus, Carleton University); 15 November 2010 (Police services of Toronto, Vancouver and the City of Montreal); 13 December 2010 (Kent Roach, Prichard-Wilson Chair of Law and Public Policy, Faculty of Law, University of Toronto).

government departments."[51] The NSA has multiple policy, coordination and operational responsibilities.[52] His or her mandate is not well defined, however, and legislation to expand and clarify that mandate could be useful.

Given that a certain climate of distrust can exist between agencies responsible for national security, which, according to Professor Kent Roach, "is inherent in their mandates,"[53] the Committee believes that the NSA should have the power to resolve disputes between those agencies so as to establish a better balance between the confidentiality of security intelligence and its use as evidence in court. At the present time, national security legislation gives CSIS sole discretion to disclose or not disclose information to another agency.[54] Furthermore, the process of settling disputes between CSIS and the RCMP with respect to the circulation of information is set out in a 2006 Memorandum of Understanding (MOU), which is a non-statutory and non-binding document.

1.2 Protection of Critical Infrastructure

The protection of critical infrastructure – such as nuclear power plants, the electricity supply network, oil and gas infrastructure, the financial system, municipal water supply systems and telecommunications networks – is a priority of Canada's national security policy. Responsibility in this area is presently shared between the federal, provincial and territorial governments, local authorities, and owners and operators of critical infrastructure. According to evidence this Committee heard, this infrastructure would be a choice target for terrorists both because of its importance for national security and its vulnerability, a vulnerability possibly exacerbated by confidential information recently made public through such new media as WikiLeaks.[55] In 2009, the Auditor General of Canada also noted that "threats to computer-based critical infrastructure, including federal information systems, are evolving and growing."[56] This

[51] Government of Canada, Securing an Open Society: Canada's National Security Policy, April 2004, p. 9.

[52] For more information on the current role of the NSA, see the report of the Air India Commission of Inquiry, volume 3, pages 26 to 34.

[53] Special Senate Committee on Anti-Terrorism, Evidence, 13 December 2010 (Kent Roach, Prichard-Wilson Chair of Law and Public Policy, Faculty of Law, University of Toronto).

[54] See subsection 19(2) of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23.

[55] Special Senate Committee on Anti-Terrorism, Evidence, 21 June 2010 (evidence of Martin Rudner, Distinguished Research Professor Emeritus, Carleton University); 6 December 2010 (Brian Jenkins, Senior Advisor, RAND Corporation).

[56] Report of the Auditor General of Canada, Chapter 7 – Emergency Management, 2009, para. 7.64.

is evidenced by the recent, sophisticated cyber-attacks against the Department of Finance and Treasury Board of Canada Secretariat.

The Air India Commission of Inquiry questioned whether the Canadian government was prepared to face the terrorist threat to critical infrastructure.[57] According to evidence heard by this Committee, steps taken to ensure its protection have been too slow and have suffered from a lack of resources.[58] While there are examples of structured response plans at the provincial and municipal levels,[59] according to Professor Martin Rudner, the national approach has been "essentially reactive and passive," and federal leadership is "fragmented,"[60] in spite of the coordination mandate assigned to the Department of Public Safety of Canada by the *Emergency Management Act* in 2007.

The Action Plan for Critical Infrastructure established in 2009 by the Department of Public Safety of Canada notes that "critical infrastructure protection is hampered by (i) uneven understanding of risks and vulnerabilities, (ii) insufficient sharing of information and (iii) limited integration of existing information into coherent situational awareness."[61]

In order to achieve a successful and effective protection strategy for our critical infrastructure, the various agencies responsible for public safety must collaborate and share information not only amongst themselves, but also with private-sector stakeholders, who, according to Michel Juneau-Katsuya, own over 80% of critical infrastructure.[62] Furthermore, this infrastructure is generally decentralized and linked to international networks, posing another formidable challenge for its protection. Memoranda of understanding must therefore be concluded between the agencies responsible for national security, the private sector, and

---

[57] Air India Report, Volume 2, Part 2, p. 532.

[58] Special Senate Committee on Anti-Terrorism, Evidence, 21 June 2010 (evidence of Martin Rudner, Distinguished Research Professor Emeritus, Carleton University).

[59] Special Senate Committee on Anti-Terrorism, Evidence, 21 June 2010 (evidence of Tom Quiggin, Senior Research Fellow, Canadian Centre of Intelligence and Security Studies, Carleton University, speaking about Alberta and New Brunswick); 15 November 2010 (Service de police de la Ville de Montréal).

[60] Special Senate Committee on Anti-Terrorism, Evidence, 21 June 2010 (evidence of Martin Rudner, Distinguished Research Professor Emeritus, Carleton University).

[61] Public Safety Canada, Action Plan for Critical Infrastructure, Annex D (Information sharing framework), 2009.

[62] Special Senate Committee on Anti-Terrorism, Evidence, 14 June 2010 (evidence of Michel Juneau-Katsuya, Chief Executive Officer, Northgate Group Corp.).

international partners, for example with respect to the granting of security clearances. The establishment of a secure information-sharing system is also a must.

This Committee recognizes that recent initiatives such as Canada's Cyber Security Strategy and the Canada-United States Action Plan for Critical Infrastructure[63] are a step in the right direction. However, given the significance of these issues for the health, safety, security and economic well-being of Canadians, and the status of the current terrorist threat, efforts must be undertaken to facilitate greater collaboration among the various stakeholders to effectively protect our critical infrastructure.

2. The Use of Intelligence as Evidence

The number of criminal prosecutions of terrorism offences requiring the disclosure or use, in one form or another, of security intelligence as evidence has increased since CSIS was created in 1984. This increase is due in part to the evolution of the terrorist threat, the extension of the obligation to disclose, and the creation, in the *Anti-Terrorism Act* of 2001, of new offences with respect to the support and financing of terrorism and preparation for terrorism, offences which occur before the terrorist act itself is committed.[64]

The use of security intelligence in investigations and criminal prosecutions will always be a complex issue. Like the challenges created by the collaboration between national security agencies, the difficulties relating to the use of intelligence before the courts arise from the difference between the agencies' mandates and the rules governing the collection and disclosure of information. The *Canadian Security Intelligence Service Act* permits CSIS to gather intelligence regarding threats to the security of Canada based on a lower threshold -- that of reasonable grounds to *suspect*[65]-- whereas the law enforcement agencies, which are governed by the *Criminal Code*, generally have to meet a higher threshold in order to make an arrest, conduct a search or engage in wiretapping -- that of reasonable grounds to *believe that an offence has*

[63] Public Safety Canada, Government of Canada launches Canada's Cyber Security Strategy, 3 October 2010; Public Safety Canada, Canada-United States Action Plan for Critical Infrastructure, 13 July 2010.

[64] Kent Roach, The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence, Research Studies for the Air India Commission of Inquiry, Volume 4, pp. 297-298.

[65] *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 12.

been or is about to be committed.[66] To obtain a criminal conviction, the prosecutor must prove guilt based on an even more demanding evidentiary threshold, namely beyond a reasonable doubt.

In addition, since court proceedings are public, intelligence services are generally reluctant to authorize the use in court of confidential information from their human sources or international partners. Moreover, using confidential information in support of criminal charges generally runs counter to the right to make full answer and defence which is entrenched in the *Canadian Charter of Rights and Freedoms*. Here again, a balance must be sought between the public interest in maintaining and respecting the rights and freedoms of Canadians and the public interest in the security of Canada. Many witnesses informed this Committee that the only way to protect our rights and freedoms without sacrificing security is to make use of the existing justice system for criminal offences.[67] This system is robust and flexible enough that certain offences, such as conspiracy or treason, could be adapted to respond to the current threat of terrorism.[68]

2.1 Disclosing Intelligence

In 1991, in *R.* v. *Stinchcombe*,[69] the Supreme Court of Canada imposed a constitutional duty on the Crown to disclose to the accused all relevant non-privileged information in its possession, whether inculpatory or disculpatory, and whether that information is introduced into evidence or not. Information is considered relevant if there is a reasonable possibility of its being used to support the Crown's case, to make full answer and defence, or to make a decision liable to influence the conduct of the defence.

This obligation on the Crown also applies to information obtained from police services. Therefore, in cases where the RCMP uses CSIS intelligence as the basis for applying for a wiretap order or search warrant, the RCMP might be legally obliged to disclose to the accused

---

[66] *Criminal Code*, R.S.C. 1985, c. C-46, ss. 495, 487 and 185 respectively.

[67] Special Senate Committee on Anti-Terrorism, Evidence, 31 May 2010 (Assistant Commissioner Gilles Michaud, National Security Criminal Investigations, RCMP); 7 June 2010 (Wesley Wark, Professor, Munk School of Global Affairs, University of Toronto); 22 November 2010 (Andrew Silke, Director for Terrorism Studies, University of East London).

[68] Special Senate Committee on Anti-Terrorism, Evidence, 14 February 2011 (James Renwick, Associate, Sydney Centre for International Law, University of Sydney Law School).

[69] *R. v. Stinchcombe*, [1991] 3 S.C.R. 326. A number of important decisions of the Court subsequently clarified and broadened the obligation to disclose (e.g. *R. v. O'Connor*, [1995] 4 S.C.R 411, *R. v. Mills*, [1999] 3 S.C.R. 668 and *R. v. McNeil*, [2009] 1 S.C.R. 66).

the information in its possession that came from CSIS. CSIS might, however, object to making this information public, in which case the success of subsequent criminal prosecutions could be compromised.

Furthermore, CSIS may have transmitted summaries of intelligence to the RCMP, but destroyed the original records (raw materials), such as operational notes, tapes of interviews, and verbatim transcripts of intercepted communications. Given that the obligation established in *Stinchcombe* also includes the obligation to preserve relevant information, a court may order a stay of proceedings in a particular case because records have been destroyed.[70] In 2008 in *Charkaoui*, the Supreme Court of Canada ruled that CSIS agents were obliged to retain their operational notes when conducting investigations targeting a particular person or group.[71]

Problems can also arise when intelligence has not been gathered by CSIS in accordance with applicable evidentiary standards for criminal investigations and prosecutions. Article 21 of the 2006 MOU between the RCMP and CSIS states that "CSIS does not normally collect information or intelligence for evidentiary purposes." In the United Kingdom and Australia, when intelligence agencies are conducting investigations that are likely to lead to criminal prosecution, they must keep in mind the requirements of both the law of evidence and the duty of disclosure.

While it is clear that police services are subject to the obligation to disclose set forth in *Stinchcombe*, the same has not been true with respect to CSIS. Canadian appeal courts are divided on this issue,[72] and the Supreme Court of Canada has not yet resolved the question, mentioning only the possibility that a state authority responsible for conducting investigations other than the police may be subject to the obligation to disclose.[73] The fact remains, however, that the Crown is obliged to make sufficient inquiries with other public agencies that might logically have relevant elements of evidence in their possession.[74] This caused the Air India Commission of Inquiry to comment that "[i]ncreased integration of the RCMP and CSIS may

[70] *R. v. La*, [1997] 2 S.C.R. 680.

[71] *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326, para. 43.

[72] *R. v. Arsenault* (1994), 93 C.C.C. (3rd) 111 (N.B.C.A.), and *R. v. Gingras* (1992), 71 C.C.C. (3rd) 53 (Alta. C.A.).

[73] *R. v. McNeil*, [2009] 1 S.C.R. 66.

[74] *R. v. McNeil*, [2009] 1 S.C.R. 66.

point to more frequent court findings that CSIS is subject to *Stinchcombe*," even if CSIS has sent no intelligence directly to the RCMP.[75]

However the Commission did not recommend new legislation governing the disclosure of intelligence during a criminal prosecution. In its view, the current limits on the obligation to disclose – privilege, the rule of relevance, and the procedure outlined in sections 38 to 38.16 of the *Canada Evidence Act* (CEA) - form, with a few adjustments, an appropriate framework permitting the courts to establish a balance between the basic right to a fair trial and the protection of confidential information.

Since the *Anti-Terrorism Act* made significant amendments to the CEA, it is now easier for the government to prevent the disclosure of certain information in court or during other proceedings on the basis that disclosure could injure international relations, national defence or national security. The Attorney General of Canada may also issue a certificate prohibiting the disclosure of information for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity, or to protect national defence or national security. Such a certificate, which must be published in the *Canada Gazette*, expires after 15 years but may be reissued.[76]

Under sections 38 to 38.16 of the CEA, all applications for non-disclosure must be settled by the Federal Court *ex parte* (that is, in the absence of the accused), although the substantive issue of the guilt or innocence of the person charged with a terrorism offence will be decided by the trial judge sitting, for example, in a provincial superior court. Trial judges must comply with the Federal Court's orders of non-disclosure, but may dismiss the charges if they find that non-disclosure would prejudice the accused's right to a fair trial.

However trial judges will generally have to make decisions without having access to the undisclosed confidential information, and this places them in a difficult position. It has even

[75] Air India Report, Volume 3, pages 98 (discussing the RCMP philosophy of "the less we receive from CSIS, the better") and 119.

[76] Special Senate Committee on the *Anti-Terrorism Act*, Main Report: Fundamental Justice in Extraordinary Times, February 2007.

provoked some criticism at the international level, [77] although, in the February 2011 decision of *R. v. Ahmad*, the Supreme Court of Canada recognized the constitutional validity of the sections of the CEA creating this two-court process. The Court interpreted the provisions as conferring a broad discretion on the Federal Court and the Attorney General of Canada, including the power to disclose sensitive information to the trial judge in certain circumstances, such as by providing a summary.[78] Trial judges will still not be able, however, to order that material withheld pursuant to section 38 be disclosed or produced for their own inspection.

From the outset, the Supreme Court emphasized that the underlying wisdom of the section 38 scheme was not a matter for the Court to assess: "It will ultimately be for Parliament to determine with the benefit of experience whether the wisdom of the bifurcated scheme should be reconsidered."[79] According to some of the testimony heard by this Committee, this process involving two different courts which have to rule on similar, closely related questions can result in long delays and the fragmentation or disruption of criminal trials.[80] The Supreme Court echoed this point of view: "the legislative division of responsibilities does have the potential to cause delays and to pose serious challenges to the fair and expeditious trial of an accused, especially when the trial is by jury."[81]

This bifurcated scheme, which is unique to Canada, leads the Committee to believe that we are lagging behind countries such as Australia, the United Kingdom and the United States, which, as noted by Professor Kent Roach, allow the trial judge to decide issues of non-disclosure, to examine secret intelligence and to review his or her own initial confidentiality orders in cases where new evidence is subsequently brought to light during the criminal trial.[82]

---

[77] See the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights, Assessing Damage, Urging Action, December 2008, p. 153, and the UN Human Rights Committee, Concluding observations on Canada, CCPR/C/CAN/CO/5, 20 April 2006, para. 13.

[78] *R. v. Ahmad*, 2011 SCC 6, paras. 37, 41 to 44, and 50

[79] *R. v. Ahmad*, 2011 SCC 6, para. 80; see also paras, 2, 3 and 75.

[80] Special Senate Committee on Anti-Terrorism, Evidence, 13 December 2010 (evidence of Kent Roach, Prichard-Wilson Chair of Law and Public Policy, Faculty of Law, University of Toronto).

[81] *R. v. Ahmad*, 2011 SCC 6, para. 76.

[82] Kent Roach, The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence, Research Studies for the Air India Commission of Inquiry, Volume 4, p. 292.

These countries also allow special advocates, in the United Kingdom, or defence counsel who have obtained appropriate security clearance in Australia and the United States, to examine the confidential information and challenge the government's applications for non-disclosure. During its in-depth review of the provisions and application of the *Anti-Terrorism Act*, the Committee recommended the appointment of such a special advocate, with access to the confidential information held by the government, in proceedings in which the disclosure of information is denied to one party on grounds of national security, in order to represent the interests of that party as well as the public interest in disclosure.[83] The Supreme Court of Canada recently confirmed that "the assistance of a special counsel might be of considerable help (depending on the circumstances) to the judge presiding at a criminal trial."[84]

The Committee nonetheless recognizes that members of the Federal Court possess significant expertise with respect to the confidentiality of national security information, and that the current two-court system, as discussed by the Supreme Court in *Ahmad*, is flexible and can be adapted to respond to a particular case, in order to protect both the national security interest and due process.

2.2 Protection of Human Sources

The cooperation of communities and human sources is one of the most effective ways of investigating terrorist plots. It is for this reason that intelligence services jealously guard the confidentiality of their human sources. In his evidence before the Air India Commission of Inquiry, Jack Hooper, former Assistant Director of Operations at CSIS, explained that exposing the identity of a human source could "chill an entire community" and CSIS would then have to start over "from ground zero."[85]

Even if all national security agencies managed to build a relationship of trust amongst themselves based on good faith, CSIS may remain legitimately fearful that the identity of its human sources could be compromised during subsequent investigations or criminal prosecutions,

[83] Special Senate Committee on the *Anti-Terrorism Act*, Main Report: Fundamental Justice in Extraordinary Times, February 2007, Recommendation 7.

[84] *R. v. Ahmad*, 2011 SCC 6, para. 47.

[85] Air India Report, Volume 2, Part 2, p. 394.

since, as discussed earlier, police officers (and probably CSIS itself in certain cases) who use information from CSIS sources are subject to the obligation to disclose set forth in *Stinchcombe*.

There are nonetheless certain protective measures that are applicable to human sources, such as orders of non-disclosure under section 38 of the *Canada Evidence Act* and witness protection programs. The government can also remove information liable to reveal the identity of a human source from the affidavit used to issue a search warrant or wiretap order. There is also the privilege relating to police informers, which protects the name of the informer and all information liable to permit him or her to be identified. This is an absolute privilege, meaning that the judge *must* see that this information is protected in all cases, except where the innocence of the accused is at stake. Unfortunately, it is not clear at the present time whether the privilege for police informers could be applicable to CSIS sources.[86]

Non-publication orders and testimony under pseudonyms provide only partial anonymity, since the accused can see the witness. The law as it stands in Canada does not authorize anonymous testimony, in particular because of the accused's *Charter* rights to know the case against him or her, to make full answer and defence, and to conduct a full cross-examination in order to assess the credibility of witnesses. Certain European countries, such as France, Finland, the Netherlands and the United Kingdom, allow anonymous evidence in criminal proceedings, but only in exceptional circumstances which are tightly controlled and in compliance with European human rights law.

2.3 Disruption

Some witnesses noted that the prevention of a terrorist act is often more important than criminal prosecution, and should take priority. For example, it may be more advantageous to keep the identity of a human source secret in order to secure intelligence that will serve to disrupt a plot than to use such a person as a witness in a subsequent trial. The challenges faced by those agencies responsible for national security are substantial, in terms of both criminal prosecution and the prevention of terrorism, particularly given the domestic evolution of this threat. There is no single profile of a homegrown terrorist, indicators of radicalization are often non-criminal,

[86] Special Senate Committee on Anti-Terrorism, Evidence, 15 November 2010 (evidence of Gordon Sneddon, Inspector, Intelligence Division, Integrated National Security Enforcement Team, Toronto Police Service).

and once the final stage of the radicalization process is reached (violent extremism), the likelihood of the police or intelligence agencies preventing the attacks is low.[87]

Nonetheless, the evidence this Committee heard suggests that one of the main reasons for the absence of major attacks in recent years is that intelligence agencies have been able to thwart plots before they materialize as actual attacks,[88] for example by letting the targets know that their activities are being investigated. Disruption activities can, in fact, be very effective in combatting terrorism – consider the example of the prior terrorist networks before the arrest of the "Toronto 18," which was raised by way of example before this Committee.[89]

The independent agency responsible for the civil review of CSIS' operations, the Security Intelligence Review Committee (SIRC), has pointed out that these disruption activities, although necessary to adapt to the new nature of terrorism, stray from the customary mandate of CSIS. In its most recent report, SIRC points out that "although CSIS' mandate under Section 12 [of the *Canadian Security Intelligence Service Act*] does not explicitly prohibit the use of disruption, neither does the authority to collect and analyse intelligence and report to and advise the Government of Canada thereon, appear to capture such activities."[90]

3. Terrorist Financing

Combatting the financing of terrorism is part of the broader objective of preventing terrorist acts, by such means as detection, disruption, and also deterrence.[91] It is, however, very difficult to get an accurate picture of the extent of terrorist financing, both internationally and in Canada. In Canada, in 2006-2007, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) identified 41 cases involving nearly $2 billion in suspect transactions which could have concealed money laundering, terrorist financing or other threats to the security of

[87] New York Police Department, Radicalization in the West: The Homegrown Threat, 2007, p. 46.

[88] Special Senate Committee on Anti-Terrorism, Evidence, 21 June 2010 (evidence of Martin Rudner, Distinguished Research Professor Emeritus, Carleton University).

[89] Special Senate Committee on Anti-Terrorism, Evidence, 14 June 2010 (evidence of Dwight Hamilton, Author, *Terror Threat: International and Homegrown Terrorists and Their Threat to Canada*). See also Brian Michael Jenkins, Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001, 2010, p. 10.

[90] Security Intelligence Review Committee, Annual Report 2009-2010: Time for Reflection: Taking the Measure of Security Intelligence, tabled 30 September 2010, p. 16.

[91] Special Senate Committee on Anti-Terrorism, Evidence, 4 October 2010 (Guillermo R. Aureano, Internship Coordinator, Department of Political Science, University of Montreal, Associate Researcher, CIPSS).

Canada.[92] According to ITAC, numerous terrorist groups are engaged in criminal activities in support of their operations and as a means to generate funds. Those activities vary in complexity: examples include fraud, smuggling (including human trafficking) and drugs and weapons trafficking.[93] Certain groups have even established ties to organized crime[94] or founded legitimate businesses.

After the events of September 11, most countries, including Canada, chose to combat terrorist financing by adopting the model used to fight money laundering, which generally involves staggering amounts of money. While terrorists do use techniques related to money laundering, the campaign against terrorist financing differs in certain respects from that against money laundering.

Contrary to the laundering of proceeds of crime, money that may be used to finance terrorist activities is not necessarily generated from the commission of a separate criminal offence, and in many cases is relatively modest. For instance, the operational cost of the Air India bombings was estimated at around $3,000.[95] More recently, meagre operational costs have been linked to the attempt against Northwest Airlines Flight 253 to Detroit on 25 December 2009 and the parcel-explosives aboard cargo planes from Yemen in October 2010. According to Charles Bisson, Deputy Director of Operations with CSIS, future attacks will likely continue to be characterized by their more or less improvised and opportunistic nature, a low level of organization, and the need for "much less investment to carry out," in particular given the reduced capacity of core Al Qaida.[96]

The Canadian model for combatting terrorist financing is presently based on the approach used for money laundering, which in particular targets cash financial transactions and electronic funds transfers of $10,000 or more. The Committee feels that this threshold, provided for in the

[92] Financial Transactions and Reports Analysis Centre of Canada, Annual Report 2007, p. 8.

[93] Special Senate Committee on Anti-Terrorism, Evidence, 31 May 2010 (Monik Beauregard, Director, Integrated Threat Assessment Centre).

[94] Special Senate Committee on Anti-Terrorism, Evidence, 14 June 2010 (Michel Juneau-Katsuya, Chief Executive Officer, Northgate Group Corp.).

[95] Air India Report, Volume 5, p. 34.

[96] Special Senate Committee on Anti-Terrorism, Evidence, 31 May 2010 (Charles Bisson, Deputy Director, Operations, Canadian Security Intelligence Service).

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), will result in too many transactions related to terrorist financing going undetected. Other countries have set their threshold lower, as in the United States, where money services businesses[97] have to report transactions of $2,000 or more, or, in some cases, $5,000 or more.[98] While the Air India Commission of Inquiry made no formal recommendations concerning terrorist financing, it did suggest that "[t]he time may have come to use distinct legislative schemes to deal with money laundering and TF [terrorist financing]".[99]

3.1. FINTRAC

FINTRAC is the linchpin of the Government of Canada's strategy against terrorist financing. Created in 2000, FINTRAC is the Canadian Financial Intelligence Unit (FIU), which receives financial information from government agencies as well as persons and entities in the private sector such as banks, money services businesses, casinos and accountants. It analyses and distributes financial intelligence to national security agencies in Canada and to foreign FIUs with which it has signed memoranda of understanding. To date, FINTRAC has concluded 71 MOUs with various countries.[100]

FINTRAC is an independent agency that acts at arm's length from law enforcement and intelligence agencies.[101] Consequently, it cannot transmit financial intelligence to agencies responsible for national security unless there are "reasonable grounds to suspect"[102] that the intelligence would be relevant to the investigation or prosecution of a money laundering or terrorist financing offence or to a threat to the security of Canada. The reason for this is to ensure the protection of the privacy rights of persons and entities in the private sector that must report

[97] Money services businesses include alternative money remittance systems (such as Hawala, Hundi or Chitti), etc.

[98] United States, Department of the Treasury, Financial Crimes Enforcement Network, Money Services Business (MSB) Suspicious Activity Reporting.

[99] Air India Report, Volume 5, p. 273.

[100] For example, there are MOUs with Egypt and certain countries considered to be tax havens, although FINTRAC has no agreements with Tunisia or Switzerland. However, the absence of an MOU does not prevent FINTRAC from *receiving* voluntary reports from those countries. FINTRAC must have a MOU and meet the criteria of "reasonable grounds to suspect" if it wants to *transmit* intelligence to foreign FIUs.

[101] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17, ss. 40, 55 and 55.1.

[102] The legal threshold of "reasonable grounds to suspect" is not defined in the PCMLTFA. According to FINTRAC, this threshold is lower than "reasonable grounds to believe," but more than simply a suspicion. FINTRAC conducts a case-by-case analysis to determine whether the threshold is met (Special Senate Committee on Anti-Terrorism, Evidence, 7 February 2011 (Yvon Carrière, Senior Counsel, Legal Services, Financial Transactions and Reports Analysis Centre of Canada)).

certain financial transactions to FINTRAC. The vast majority of these transactions are legitimate. In this regard, this Committee notes that the Privacy Commissioner of Canada, in the two-year review required by the PCMLTFA, concluded that "the Centre's use and disclosure practices respect privacy."[103] That being said, the Commissioner stated that certain financial information reported to security agencies did not clearly demonstrate that there were reasonable grounds to suspect cases of money laundering or terrorist activity financing. What is more, the memoranda of understanding lacked "a number of key clauses: namely, a requirement for both parties to notify the other in the event of a breach [of privacy]."[104]

Another effect of FINTRAC's position of independence is that it does not have the power to force other government agencies to provide access to intelligence in their possession, or to force reporting entities to forward information over and above what is provided for in the PCMLTFA; for example, it does not track the transfer of funds using prepaid cards or mobile communications devices.[105]

The disadvantage with that position of independence is that FINTRAC may be operating in its own silo. In her November 2004 report, the Auditor General noted that law enforcement agencies were reluctant to share information with FINTRAC.[106] This Committee is pleased to learn, however, that, according to Denis Meunier, Assistant Director of FINTRAC,[107] this is no longer the case: in practice, relations among the agencies are now based on more effective mutual cooperation. In fact, according to the recent evaluation conducted for the Department of Finance Canada, "FINTRAC has enhanced its expertise and capabilities" and has provided partners "with names of individuals previously unknown to them."[108]

---

[103] Office of the Privacy Commissioner of Canada, Audit of the Financial Transactions and Reports Analysis Centre of Canada, 2009, para. 117.

[104] Office of the Privacy Commissioner of Canada, Audit of the Financial Transactions and Reports Analysis Centre of Canada, 2009, paras. 50, 73, and 78.

[105] Department of Finance Canada, 10-Year Evaluation of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, December 2010, in section 4.2.1, "Gaps in Coverage of the PCMLTFA and Other Legislation."

[106] 2004 Report of the Auditor General of Canada to the House of Commons, Chapter 2, para. 2.25.

[107] Special Senate Committee on Anti-Terrorism, Evidence, 7 February 2011 (evidence of Denis Meunier, Assistant Director, Financial Analysis and Disclosures, FINTRAC).

[108] Department of Finance Canada, 10-Year Evaluation of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, December 2010, section 4.2.4, Achievements in Intelligence Gathering and Analysis.

Nonetheless, certain problems seem to persist with regard to the integration and evaluation of the effectiveness of FINTRAC. Firstly, the Committee believes that, as noted in the ten-year evaluation conducted for the Department of Finance Canada,[109] FINTRAC's work against terrorist financing must be more integrated with that of the other agencies so as to provide them with the most useful financial intelligence and to avoid duplication of effort. Under the PCMLTFA, FINTRAC cannot currently, of its own accord, disclose its own analyses of financial intelligence in specific cases, or written explanations justifying disclosure, to national security agencies.[110] As a result, law enforcement agencies and CSIS must re-analyse the intelligence received and essentially repeat any analysis that FINTRAC has already done.

Secondly, even though it is still a relatively new organization, the effectiveness of FINTRAC in terrorist financing investigations, prosecutions and convictions appears at first glance to be rather modest. According to Professor Guillermo Aureano, it is not possible to identify any particular case in which the money trail served to prevent an attack,[111] even though national security agencies indicate that they find the intelligence provided by FINTRAC very useful in carrying out their mandate, especially since the improvements introduced by Bill C-25 in 2007-2008.[112] As for the number of actual charges and convictions (there have been only two convictions to date: *Khawaja*[113] and *Thambithura*[114]) for a terrorist financing offence, FINTRAC's internal evaluation system makes it difficult to determine the extent of FINTRAC's contribution. In fact, this lack of precise data and statistics – especially with respect to the number of charges laid – is an issue for the entire anti-money laundering and anti-terrorist financing regime.[115] The Committee notes, however, that two years ago FINTRAC implemented a process to improve feedback and tracking of its disclosures to national security agencies.

---

[109] Department of Finance Canada, 10-Year Evaluation of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, December 2010, Executive Summary, Conclusion 5.

[110] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17, s. 55 and 55.1.

[111] Special Senate Committee on Anti-Terrorism, Evidence, 4 October 2010 (evidence of Guillermo Aureano, Internship Coordinator, Department of Political Science, University of Montreal, Associate Researcher, CIPSS).

[112] Special Senate Committee on Anti-Terrorism, Evidence, 7 February 2011 (evidence of Denis Meunier, Assistant Director, Financial Analysis and Disclosures, FINTRAC).

[113] *R. v. Khawaja* (2008), 238 C.C.C. (3d) 114 (Superior Court, Ont.); *R. v. Khawaja*, 2010 ONCA 862.

[114] British Columbia, Supreme Court, Justice Robert Powers, Vancouver, 14 May 2010 (unpublished decision).

[115] Department of Finance Canada, 10-Year Evaluation of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, December 2010, Executive Summary, Recommendations 2c and 2d.

Considering that investigations in these areas can go on for years, this evaluation tool should provide a more accurate picture of FINTRAC's effectiveness in these cases.

Furthermore, over 80% of presumed cases of terrorist financing are brought to FINTRAC's attention through voluntary reports by national security agencies and foreign financial intelligence units.[116] One might therefore wonder whether FINTRAC in fact has the capacity to detect new cases of terrorist financing through sources other than current investigations. According to the evaluation by the Financial Action Task Force (FATF), this lack of effectiveness might be explained by the relatively small number of employees assigned to analysing terrorist financing cases at FINTRAC compared with the number of reporting entities (approximately 300,000) and the number of reports it receives (nearly 25 million last year).[117] Furthermore, the percentage of FINTRAC's activities devoted to terrorist financing is small (20%) compared with those devoted to money laundering (80%).[118] The Committee notes, however, that the Government of Canada has recognized the importance of FINTRAC's functions by increasing its permanent funding by $8 million per year in Budget 2010.

In light of these considerations, the Committee recommends:

(8) That the role of the National Security Advisor (NSA) be expanded through legislation that clearly establishes the NSA's functions and powers with respect to coordinating national security activities, resolving disputes between agencies with national security responsibilities, and overseeing the effectiveness of government activities in national security. The National Security Advisor must also have the authority to transmit information received from an agency regarding a national security threat to other agencies responsible for national security.

(9) That the *Canadian Security Intelligence Service Act* be amended (i) to require that CSIS provide to the appropriate law enforcement agencies, or to the National Security Advisor, information that may be used in an investigation or prosecution regarding an offence constituting a "threat to the security of Canada" within the meaning of section 2 of that Act; (ii) when it is possible and reasonable to expect that the intelligence will be relevant to an investigation or criminal prosecution, to require that CSIS retain intelligence collected during an investigation into threats to the security of Canada (such as operational notes, tapes of interviews, and verbatim transcripts of intercepted communications); (iii) to

[116] FINTRAC, Annual Report 2010, p. 9.

[117] FINTRAC, Annual Report 2010, p. 15; Financial Action Task Force, Third Mutual Evaluation of Canada, 29 February 2008, p. 297.

[118] Special Senate Committee on Anti-Terrorism, Evidence, 7 February 2011 (evidence of Denis Meunier, Assistant Director, Financial Analysis and Disclosures, FINTRAC).

require that CSIS collect and provide this material so as to comply with the rules of evidence and disclosure; and (iv) to clarify that the transfer of a human source from CSIS to a police service will not prevent the police service from invoking the police informer privilege. Disputes over the use of a human source could be resolved through the intervention of the National Security Advisor.

(10) That the federal government examine the importance of amending section 12 of the *Canadian Security Intelligence Service Act* in order to clarify and ensure CSIS's right to utilize lawful disruption as a method of preventing terrorist attacks, and that CSIS establish an official procedure and formal guidelines on the terms and conditions of utilizing such preventive activities. These should require CSIS to report all cases of disruption to the Minister of Public Safety, in a manner similar to that set out at section 25.1 of the *Criminal Code* and following, with respect to the requirements imposed on designated public officers.

(11) That the federal government examine whether it would be useful to amend the legislation governing national security agencies other than the Canadian Security Intelligence Service, such as the Royal Canadian Mounted Police, the Department of Foreign Affairs and International Trade, the Canada Border Services Agency and the Communications Security Establishment, to allow those agencies to transmit to the National Security Advisor information relating to national security that would be relevant to the NSA's proposed expanded mandate.

(12) That the federal government allocate appropriate resources to ensure the protection of Canada's critical infrastructure, for example with respect to the robust use of all available satellite technologies, and that it adopt, in a manner that is consistent with and reinforces the purposes of the *Emergency Management Act* and the new legislative framework expanding the mandate of the National Security Advisor, a proactive approach, notably in establishing secure information sharing systems and protocols with the private sector, provincial and territorial governments, and international partners.

(13) That the federal Minister of Justice consult with his or her provincial and territorial counterparts on the usefulness of amending sections 38 to 38.16 of the *Canada Evidence Act* so as to abrogate the two-court system in criminal law and to permit the trial judge to make decisions regarding confidentiality related to national security, to examine secret intelligence, to review his or her initial confidentiality orders, and to ensure due process of law through adequate safeguards, including, where applicable, through the assistance of a special advocate.

(14) That the federal government examine, particularly in anticipation of the statutory review mandated for 2011, the usefulness of amending the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations to reduce the $10,000 threshold for financial transactions related to terrorist financing, and to include, in the definition of "monetary instruments," prepaid cards and mobile communications devices that are used to transfer funds. To that end, the government shall carry out a "cost-benefit" analysis, giving consideration, for example, to costs for the private sector, protection of personal

information, and the operational capacity of the Financial Transactions and Reports Analysis Centre of Canada.

(15) That the statutory mandate of the National Security Advisor include evaluating the integration and effectiveness of the Financial Transactions and Reports Analysis Centre of Canada.

CHAPTER 3: PARLIAMENTARY OVERSIGHT OF CANADA'S NATIONAL SECURITY

The term "oversight" here refers to various forms of scrutiny and review by a permanent parliamentary body to deal with security and intelligence issues. Although permanent parliamentary committees on national security currently exist in both chambers of Parliament (the Anti-terrorism Committee, being a special committee, was formed only for a temporary period), the longstanding absence in Canada of appropriate and in-depth parliamentary oversight remains a real concern. In fact, the Committee has repeatedly identified the need for such oversight. In *Fundamental Justice in Extraordinary Times*, the Committee recommended that a parliamentary committee be established, "to monitor, examine and periodically report on matters relating to Canada's anti-terrorism legislation and national security framework on an ongoing basis."[119]

After conducting the first parliamentary review of the *CSIS Act* in 1989 and 1990, a special committee of the House of Commons recommended the creation of a permanent parliamentary subcommittee charged, among other things, with examining the work of the agencies responsible for national security.[120] During its review, the special committee was unable to access certain important information because of its confidential nature. Its recommendation that any members of the subcommittee have "Top Secret Special Activity" security clearance was designed to address this shortcoming. This Committee strongly believes that parliamentarians must be fully informed about national security activities so that they can more effectively defend the interests of Canadians.

With the coming into force of the *Anti-Terrorism Act* in 2001, the powers of national security agencies were extended, thereby heightening the risk of infringement of human rights and freedoms. In 2002, the House of Commons Standing Committee on Foreign Affairs and International Trade therefore recommended increased parliamentary oversight of intelligence

[119] Special Senate Committee on the *Anti-Terrorism Act*, Main Report: Fundamental Justice in Extraordinary Times, February 2007, p. 122.

[120] Report of the Special Committee on the review of the CSIS Act and the Security Offences Act, *In Flux But Not in Crisis*, 1990 (Recommendations 107 to 116).

agencies.[121] The same opinion was then expressed by the Privacy Commissioner of Canada.[122] A detailed study of the issue was conducted by the Interim Committee of Parliamentarians on National Security, which in 2004 recommended the creation of a parliamentary intelligence committee to ensure that the security and intelligence community effectively serves Canada's interests, respects the *Canadian Charter of Rights and Freedoms,* and remains fiscally responsible, properly organized and well managed.[123] Its members would have had the same right to access confidential intelligence as SIRC.[124] SIRC has access to all the information held by CSIS, with the exception of confidential Cabinet information.

In November 2005, a National Security Committee of Parliamentarians was proposed in Bill C-81, which died on the *Order Paper* with the dissolution of the 38th Parliament. The mandate of the Committee, which would have had access to classified information, would have been to review the legislative, regulatory, policy and administrative framework for national security in Canada, the activities of federal departments and agencies in relation to national security, and any other matters relating to national security referred to it by the government. The Committee would have been comprised of Senators and Members of the House of Commons but would have reported to the Prime Minister.

A number of mechanisms are already in place for the review of national security and intelligence activities, including SIRC, the Inspector General of CSIS, the CSE commissioner, and the Commission for Public Complaints Against the RCMP – which Bill C-38 proposes to replace with a new, more effective commission. However, these review mechanisms and parliamentary oversight are not mutually exclusive. The role of Parliament in this area is widely recognized, as the Committee noted in its review of the *Anti-Terrorism Act* from 2005 to 2007: "While duplication of effort should be avoided, it is necessary, given Canada's constitutional framework, to have parliamentary review and scrutiny that complements the policy and

[121] House of Commons, Report of the Standing Committee on Foreign Affairs and International Trade, December 2002, recommendation 10.

[122] Office of the Privacy Commissioner of Canada, Rights and reality: enhancing oversight for national security programs in Canada, May 2009.

[123] Privy Council Office, Report of the Interim Committee of Parliamentarians on National Security, 2004.

[124] The importance of a right to access classified information was underscored by the Council of Europe in the Report on the Democratic Oversight of the Security Services, June 2007, para. 163.

operational decisions of the government."[125] Parliamentarians have the advantage of having an overview of the various federal departments to which the many national security agencies are accountable. Furthermore, the creation of a joint committee of parliamentarians from the Senate and the House of Commons would retain significant corporate memory thanks to the greater continuity of the Senators' mandate.

On the international stage, the Committee would like to emphasize that Canada now lags significantly behind its allies on the issue of parliamentary oversight, as the only country that lacks a parliamentary committee with substantial powers of review over matters of national security. In the United Kingdom, for example, an independent reviewer has been appointed to monitor the operation of that country's anti-terrorism legislation. The United Kingdom also has a Security and Intelligence Committee, made up of parliamentarians from the two chambers who oversee the operations of the relevant agencies and report to the Prime Minister. The Prime Minister is charged with appointing its members, after consulting with the Leader of the Opposition. As in other countries, there are rules governing members' access to secret intelligence and their obligation of confidentiality.

Australia has had a joint committee providing parliamentary oversight of the administration and spending of national security agencies since the coming into force of the *Intelligence Services Act 2001*. This committee can also review the operation and effectiveness of security legislation. While it has access to certain confidential information, it cannot, for example, inspect sources of information (e.g. raw material) or a particular secret operation of an agency. On the other hand, the committee can count on the assistance of the Inspector-General of Security and Intelligence, who is able to examine not only every Australian intelligence agency but also any kind of national security function within different departments of the Australian government. Unlike in the United Kingdom, this committee reports directly to Parliament. The executive may suggest candidates, but it is up to Parliament to appoint the members. More recently, Australia has also created the position of National Security Legislation Monitor, who will be required to report annually to the Prime Minister and to Parliament. In November 2010, a parliamentary committee with extended powers was established to oversee the broad operation

[125] Special Senate Committee on the *Anti-Terrorism Act*, Main Report: Fundamental Justice in Extraordinary Times, February 2007, p. 120.

and effectiveness of law enforcement agencies. The committee can convene *in camera* and receive confidential information. In exceptional cases, however, the minister responsible may refuse access to this type of information if he or she considers that the public interest in a full review by the committee is outweighed by the prejudicial consequences of its disclosure. This measure is similar to what is provided for in Norway.

The United States also has a Senate Select Committee on Intelligence and a House Permanent Select Committee on Intelligence which have extended powers to review and obtain classified information. The committees of Congress may also be charged with approving certain types of covert actions. In France, Bill 2007-1443 created a "special parliamentary delegation" composed of four members of Parliament and four senators. The delegation holds all its hearings *in camera* and its proceedings are subject to national defence privilege. It may also make recommendations to the Prime Minister and the President.

In addition to those countries where parliamentarians themselves exercise an oversight role through a parliamentary committee, other countries allow for the creation outside Parliament of expert bodies or committees whose members are not parliamentarians and yet still report to Parliament (examples are Belgium, the Netherlands and Portugal). Certain states such as Germany have both parliamentary committees and expert bodies. Parliamentary oversight committees are sometimes chaired by the opposition, as is the case in Hungary.

(16) That, consistent with the practices in the United Kingdom, Australia, France, the Netherlands, and the United States, the federal government constitute, through legislation, a committee composed of members from both chambers of Parliament, to execute Parliamentary oversight over the expenditures, administration and policy of federal departments and agencies in relation to national security, in order to ensure that they are effectively serving national security interests, are respecting the *Canadian Charter of Rights and Freedoms,* and are fiscally responsible and properly organized and managed.

The proposed committee of Parliamentarians shall have the same right to access information as the Security Intelligence Review Committee. Members of the Committee shall be appointed by the Governor in Council, and will hold office during periods of prorogation. Meetings of the Committee shall be held *in camera* whenever the Chair, a majority of members present or the Minister considers it necessary for the Committee to do so. Members of the committee shall be required to swear an oath of secrecy similar to that found in the schedule to the *Canadian Security Intelligence Service Act* or to the Oath of a Privy Councillor, or both, and be permanently and statutorily bound to secrecy for purposes of application of the *Security of Information Act.* The committee shall report to

the Prime Minister, who would make that report public within 60 days of receipt. When matters in the report need to be removed for national security reasons, the report, when made public, must indicate that this has transpired.

APPENDIX I: WITNESSES

Meeting Date	Agency and Spokesperson
May 31, 2010	**Canadian Security Intelligence Service** Charles Bisson, Deputy Director, Operations **Integrated Threat Assessment Centre** Monik Beauregard, Director **Royal Canadian Mounted Police** Assistant Commissioner Gilles Michaud, National Security Criminal Investigations **National Defence** Linda Goldthorp, Director General, Director General Intelligence Production
June 7, 2010	**Mackenzie Institute** John Thompson, President **As individuals** Wesley Wark, Professor, Munk School of Global Affairs, University of Toronto Jez Littlewood, Director, Canadian Centre of Intelligence and Security Studies, Carleton University
June 14, 2010	**As an individual** Dwight Hamilton, Author, *Terror Threat: International and Homegrown Terrorists and Their Threat to Canada* **Northgate Group Corp.** Michel Juneau-Katsuya, Chief Executive Officer **As an individual** Ronald Crelinsten, Senior Research Associate, Centre for Global Studies, University of Victoria
June 21, 2010	**As individuals** Martin Rudner, Distinguished Research Professor Emeritus, Carleton University

	Tom Quiggin, Senior Research Fellow, Canadian Centre of Intelligence and Security Studies, Carleton University Steven Hutchinson, Assistant Professor, Department of Criminology, University of Ottawa
October 4, 2010	**As individuals** Guillermo R. Aureano, Internship Coordinator, Department of Political Science, University of Montreal, Associate Researcher, CIPSS Stéphane Leman-Langlois, Professor, Laval University, Director, Terrorism and Counterterrorism Research Group **Al Sunnah Foundation** Sayyid Ahmed Amiruddin, Chairman
November 15, 2010	**Toronto Police Service** Gordon Sneddon, Inspector, Intelligence Division, Integrated National Security Enforcement Team Tom Fitzgerald, Superintendent, Unit Commander, Intelligence Division **Vancouver Police Department** Robert Stewart, Inspector, Criminal Intelligence Section **Service de police de la Ville de Montréal** Philippe Pichet, Commander Robert Chartrand, Chief Inspector
November 22, 2010	**As an individual** Andrew Silke, Director for Terrorism Studies, University of East London (by videoconference) **Royal United Services Institute** Tobias Feakin, Director, National Security and Resilience Department (by videoconference)
December 6, 2010	**Norwegian Defence Research Establishment** Thomas Hegghammer, Research Fellow (by videoconference) **RAND Corporation** Brian Jenkins, Senior Advisor

December 13, 2010	**Center for Security Studies, ETH Zurich, Switzerland** Alex Wilner, Senior Researcher (by videoconference) **As an individual** Kent Roach, Prichard-Wilson Chair of Law and Public Policy, Faculty of Law, University of Toronto (by videoconference)
February 7, 2011	**Financial Transactions and Reports Analysis Centre of Canada** Denis Meunier, Assistant Director, Financial Analysis and Disclosures Gina Jelmini, Manager, Terrorist Financing Analysis Yvon Carrière, Senior Counsel, Legal Services
February 14, 2011	**As individuals** James Renwick, Associate, Sydney Centre for International Law, University of Sydney Law School (by videoconference) George Syrota, Associate Professor, University of Western Australia (by videoconference)