

Canadian Foreign Policy, Terrorism, and Non-Traditional Security Threats: Temporary Aberration or Permanent Condition ?

By

David A. Charters

Introduction

It is too soon to say whether the recent ‘crisis’ in Canadian-American relations, over Canada’s refusal to support the American war in Iraq, will leave permanent scars or will prove to be merely one more temporary ‘bump’ in our complex relationship with the US. But it may be fair to suggest that the Canadian debate over the issue highlighted in stark terms the different threat perceptions of the two countries. Rightly or wrongly, the US administration regarded the Iraqi regime as a threat to regional and global stability; the Canadian government of the day did not share the American threat perception or the sense of immediate urgency to act.

This undoubtedly reflects the two very different experiences of 9/11. The United States was attacked, *directly and deliberately*; Canada was not. The United States suffered some 9,300 casualties, including 3,000 dead; Canada, only about two dozen, whose misfortune was simply the result of being in the wrong place at the wrong time. For the United States, 9/11 was “*The day the world changed*”. It opened the door to an uncertain, dangerous future, which placed the American homeland, indeed the American way of life itself, in a state of permanent *existential* threat. For Canada, it was a passing phenomenon, whose principal threat was actually the American *reaction* to 9/11, specifically the potential economic costs to Canada of stricter border security. After a flurry of legislative and budgetary activity designed to assure the US that we would do our part to keep the border secure - and thus open to trade - and a brief deployment of the army to the front lines of the War on Terrorism, Canadian political life has returned to normal.

But, although Iraq played no role in the 9/11 attacks, for the US the war in Iraq was a logical extension of the War On Terrorism. The US sees terrorism, WMD, and ‘rogue states’

(such as Iraq under Saddam Hussein) as all of a piece. Trans-national organized crime (TNOOC) and 'Cyber-terrorism' are sometimes grouped with these under the rubric of "Non-Traditional Security Threats", because they do not threaten the state or the international system with direct attack. Rather, the threats are *asymmetric*; they circumvent the state's military strength, and try to 'decapitate' or undermine government by using covert violence, corruption, and disruption to attack or exploit a country's 'centers of gravity' and Critical Infrastructures.' Unlike the Iraq situation, Canadian officials view these with genuine concern.

This essay will explore three of these - terrorism, cyber-terrorism, and trans-national organized crime - with a view to answering three questions. Are these threats genuine and serious, especially for Canada? Do they represent a permanent change or a temporary condition? And what are the security implications for Canadian foreign policy?

Terrorism

Terrorism is not a new problem for Canada. In the 1960s, the *Front de Liberation du Quebec* (FLQ) carried out a series of terrorist attacks in Quebec, culminating in the dramatic 1970 'October Crisis'. In the 1980s, international terrorist campaigns by Armenian and Sikh opposition movements spilled over into Canada. In 1985, the bombing of an Air India flight by Canadian-based Sikh terrorists killed 329 people - the largest death toll from a single terrorist incident prior to 9/11. Canada has supported and adopted all of the international conventions against terrorism. So, in light of this, what does 9/11 mean for Canadian foreign policy and national security?

First, 9/11 and *al-Qaeda* together may represent a 'Revolution Terrorism Affairs', or at least a 'paradigm shift' in terrorism. *Al-Qaeda* is clearly different from many terrorist groups, combining some of the features of an apocalyptic cult and of a multinational corporation. Its 'flat' structure and 'cutting edge' *modus operandi* is a product of the borderless, post-modern world. It uses the tools of 'Globalization' - the Internet, ATMs, cell phones, and air travel, the very things that make the modern western state livable and sustainable - to attack Globalization's

source: the West. It directs a ‘network of networks’, a series of subsidized ‘franchises’, with connectivity provided by the intertwined fibers of ideology and technology.¹ *Al-Qaeda is Terrorism.com*.

Furthermore, the 9/11 attacks could be seen as a ‘Breakthrough Event’ in terrorism. *Al-Qaeda* created and used weapons with destructive power equal to the major weapons of a state, to attack the ‘centers of gravity’ of a superpower. They killed some 3000 people, and injured 6,300. They inflicted physical damage in the tens of *billions* of dollars and economic damage in the *hundreds of billions* or more, hastening a global recession. Finally, 9/11 was the catalyst for two wars that have toppled regimes in Afghanistan and Iraq. In short, they caused catastrophic human, political, psychological, and economic damage, and major ripple effects on global security and stability. No sub-state terrorist group in history has ever achieved this degree of impact. *Al-Qaeda*’s success may inspire others to follow its example.

Thirty years ago terrorism analyst Brian Jenkins articulated the conventional wisdom that “Terrorists want a lot of people watching ... not a lot of people dead.” The primary terrorist motive now seems to be to strike overwhelming physical and psychological blows against their enemies. Mass casualty incidents began to increase in the 1980s, but 9/11 took lethality to a whole new level. So, now we have “a lot of people watching *and* a lot of people dead”.²

This is ‘Propaganda of the Deed’ in the age of McLuhan; the medium (the attack) *is* the message. Michael Dartnell asserts that the 9/11 attacks amounted to a ‘paradigm shift’ that demonstrated the new power and capabilities that Information Technology (IT) has given to non-

¹ Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002), pp. 1-2, 54, 56-57, 60-69, 76-77, 95-98.

² Brian M. Jenkins, “International Terrorism: A New Mode of Conflict”, in David Carlton and Carlo Schaerf, eds., *International Terrorism and World Security* (London: Croom Helm, 1975), p. 15. According to John V. Parachini, “Comparing Motives and Outcomes of Mass Casualty Terrorism Involving Conventional and Unconventional Weapons”, *Studies in Conflict and Terrorism*, vol. 24, no. 5 (September-October 2001), p. 389, two NSC officials (Steve Simon and Daniel Benjamin) may have been the first to revise Jenkins’ original phrase.

state actors such as terrorists. In an web-based world, visual images reshape values, which in turn supplant the influence of the state. Terrorism is about sending messages; on 9/11 *al-Qaeda* shifted the message of political discourse from state-based 'management' values to the apocalyptic.³

Indeed, we can see in 9/11 the convergence of two trans-national forces: *Jihadism* and IT - the former challenging modernity, the latter embodying it. In *al-Qaeda*, they find symbiosis and synergy, a cult-like apocalyptic vision married to a capability that allows it to "Think Globally, and Act Locally." At the very least, it marks a change in the nature of strategic competition; the contested ground is no longer space, but values. Faith-based apocalyptic ideologies, Globalization, IT, social complexity, and non-state actors - terrorists among them - have driven that change, which is re-shaping the world. The process has been *evolutionary*, synergistic, and non-linear. These factors had *emerged* earlier, but they *converged* on 9/11.

This kind of terrorist capability levels the playing field; it puts such terrorist groups on a par with the states that are their enemies. It may have "raised the bar", setting a new standard by which all subsequent terrorist attacks will be measured. For if a terrorist group can now kill and injure nearly 10,000 people in one coordinated attack, then a much bigger attack - possibly using WMD to decapitate or paralyse a state - is no longer inconceivable. Indeed, as nuclear terrorism expert Gavin Cameron suggests, it may not be a question of "if" but "when".⁴ The threat to democracies now seems *existential* in a way not seen since the height of the nuclear standoff during the Cold War.

Even if the United States is likely to be the prime target of future attacks, this mutation of

³ Michael Dartnell, "Electronic 'Hearts and Minds': Web Activism and Global Security", paper presented at "Terrorism, Asymmetric Warfare and Homeland Security", Centre for Conflict Studies annual conference, 4 October 2002.

⁴ Gavin Cameron, "WMD Terrorism: No Longer a Question of If, But When?", paper presented at Conflict Studies conference, 4 October 2002.

terrorism could impact Canada directly or indirectly, in ways that have been elucidated in an earlier paper.⁵ Our close geographic, political, military, economic, and cultural relationship with the US makes Canada and Canadians potential targets. *Al-Qaeda* knows Canada joined the War on Terrorism. So, Canada's 'soft power' self-image, even its efforts to distance itself from the US war in Iraq, are no guarantees of immunity from attack.⁶ If the conflict with *al-Qaeda* is one of *values*, then ours place us in the same camp as the US. There is no room for smug complacency.

That said, neither should we dwell in a state of perpetual fear. It is possible that 9/11 may never be replicated. The war in Afghanistan that deprived *al-Qaeda* of its base, and the arrest of some 3,000 suspected members world-wide, including several of its key leadership figures, has dispersed and weakened the movement. But, the bombings in Bali, Saudi Arabia and Morocco, and the plots uncovered in Britain and Europe early in 2003 show that it has not given up and that it still intends to inflict mass casualties. Moreover, the American war on Iraq tends to validate *al-Qaeda*'s world-view and thus could draw more recruits to the movement. *Al-Qaeda* is not the only threat, but it is not clear whether other groups - domestic or foreign - would try or be able to emulate it. Few terrorist groups share *al-Qaeda*'s apocalyptic vision or its nihilistic will to fulfill that vision through self-immolation. Unless attacks on the 9/11 scale become the norm rather than the exception, then terrorism simply will remain a costly, dangerous, evolving and intractable problem of crisis and conflict management. However, we must accept that catastrophic attacks and outcomes are also possible, with or without WMD. The 9/11 experience

⁵ David A. Charters, "Terrorism and Response: The Impact of the War on Terrorism on the Canadian-American Security Relationship", in *Conference Publication: Canadian defence and the Canada-US Strategic Partnership* (Calgary: Canadian Defence and Foreign Affairs Institute, 2002), pp. 9-11.

⁶ Peter Cheney, "Terrorist Tape Names Canada", *Globe and Mail*, 13 November 2002. Syrian intelligence apparently helped thwart an *al-Qaeda* attack on Canadian government installations in 2001. See: Alan Sipress, "Syrian Reforms Gain Momentum In Wake of War. U.S. Pressure Forces Change In Foreign, Domestic Policy", *Washington Post* Foreign Service, 12 May 2003.

shows that we should anticipate innovation; terrorists are “thinking outside the box.” The only certainty at this stage is that 9/11 was a point of departure toward a terrorism future of great *uncertainty*.

Cyber-Terrorism

Does that future include “Cyber-Terrorism”? Gary O’Bright, Director of Operations for the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) observed in 2002 that the boundary-less world of globalized IT connectivity and interdependence has created a “target-rich environment” for cyber-*Hactivists*. The combination of fast computers and high bandwidth produces a higher potential threat, since one vulnerability can affect many users. Those vulnerabilities are multiplying at a faster rate, while cyber attacks are increasing in volume and sophistication, are spreading faster, and costing more. It is clear that terrorists are attracted to high-value critical infrastructures.⁷ However, this does not mean an “electronic Pearl Harbour” is possible or imminent. Posing the questions, “Why haven’t we seen any ‘cyber-terrorism’ in the wake of 9/11, and why are we unlikely to in the near future?”, Rand Corporation analyst David Mussington argues that cyber attacks may become *part* of the terrorist threat, but they are unlikely to cause ‘stand-alone’ terrorist attacks. The reason is simple; terrorism is associated with *physical destruction* and the *fear* that causes, and cyber attacks have yet to achieve either.⁸

This is not to suggest that there is no threat to our IT infrastructure. Many insurgent groups are using *cyberspace* for ‘*Hactivism*’, that is, to proselytize, to recruit, to generate funds, and to plan terrorist or other activities. ‘Hackers’ are also attacking and penetrating an increasingly wide range of government, military, business, and other sites, stealing information, defacing them or causing Denial of Service disruption. These frequently accompany or follow

⁷ Gary O’Bright, “Cyber Incident Management in the Canadian Government”, paper presented at Conflict Studies conference, 5 October 2002.

⁸ David Mussington, “Cyber Terrorism and Homeland Security”, paper presented at Conflict Studies conference, 5 October 2002 .

physical attacks. Currently, there are more than 50,000 Worms, Viruses and other electronic 'bugs' in circulation. Several of these, such as 'Code Red' and 'I Love You', have disrupted vital communications and data management systems, imposing financial, time, and other costs.⁹ So, cyber attacks are useful for delivering a political message, causing inconvenience, pushing up operating costs and diverting resources toward network security. But as bad as these things are, they are a far cry from the 'worst-case' scenarios hypothesized a decade ago.¹⁰ Indeed, the very concept "Cyber-Terrorism" is in my view problematic; 'cyber-sabotage' may be more appropriate. In any case, it is a threat which has yet to live up to its advance billing.

Trans-National Organized Crime

Organized crime is a familiar problem for Canada's law enforcement community. Most of its principal activities - drug trafficking, money laundering, extortion, and prostitution - have been going on for decades. Indeed, organized crime in Canada predates terrorism by a sizeable margin. So, why and how has it crept into the 'national security' debate? And does it even belong there?

Before going further, it is essential to clarify terminology. Organized crime (OC) by itself is not automatically a foreign policy issue or *security* threat. But '*trans-national*' [TN] OC, which by definition crosses borders in both directions, does enter the foreign policy realm because it affects more than one country. And certain activities and features of TNOC can have an impact on the functioning and stability of societies, making it a potential national security issue. So what sets it apart from 'traditional' OC?

First, the same tools and technologies of Globalization which allowed *al-Qaeda* to flourish have influenced the operations of TNOC. In 1999, the senior Australian police officer

⁹ The total cost inflicted by the Code Red, Love bug, NIMDA and SirCam viruses is estimated at \$ 13 billion.

¹⁰ See for eg., Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), pp. 12-18.

highlighted

the massive flow of so-called 'fast money' around.... a world in which ... A few key people located anywhere in the world can, through a series of strategic alliances, exercise control over substantial financial empires. Groups that hitherto would never have dealt with each other can now come together in a series of fluid alliances of convenience.... In such a turbo-charged environment, the job of locating illicit product or transactions is daunting.¹¹

¹¹ Dr. Sandy Gordon, Australian Federal Police, "The Emerging Features of Modern Transnational Crime", 1999, at: www.afp.gov.au/raw/publications/platypus/june99/emerging.htm

Second, some have suggested that the ‘securitization’ of the OC problem can be traced back to the 1980s when the Reagan administration re-defined the ‘War on Drugs’ as a national security issue and committed American military forces to it. At that time, terrorism and crime became linked in popular debate and political discourse through the now over-used cliché: “narco-terrorism”. However, the evidence of links and cooperation often has been less than conclusive.¹² The most frequently cited example of ‘narco-terrorism’ has occurred in Colombia. There, a large illicit coca production industry coexists with a prolonged, powerful Leftist insurgency, leading to a symbiosis between the *narcotraficantes* and the insurgents. The legitimacy and control of an ineffective and often repressive national government has been under challenge for decades by the drug lords, the insurgents, and right-wing para-military factions. The result has been a fusion of drugs and political violence. Only in Colombia have the crime cartels generated wealth and thus power sufficient to seriously challenge the government. That same wealth also drives their trans-national activities, giving them global reach and influence.¹³

The principal TNOG players in Canada are the Asian gangs and East European OC groups. Both are involved in the full range of traditional OC activities, and both rely on trans-national networks to conduct their ‘business’.¹⁴ Neither one poses a *direct* threat to Canadian security. Their TNOG activities stray into the national security realm only as *indirect* threats to social stability and to the integrity of national institutions. Of these, the illicit drug trade has the greatest impact on Canadian society. It fuels firearms smuggling, stimulates violence, increases

¹² On the problems with this phrase, see: Grant Wardlaw, “Linkages Between the Illegal Drugs Traffic and Terrorism”, *Conflict Quarterly*, vol. 8, no. 3 (Summer 1988), pp. 5-7. See also: Captain Dan C. Meyer, “The Myth of Narcoterrorism in Latin America”, *Military Review* (March 1990), pp. 64-70.

¹³ “Drugs and Insurgents in Colombia: A Regional Conundrum”, *RAND Research Brief*, no. 69 (2001).

¹⁴ Criminal Intelligence Service of Canada, *Annual Report on Organized Crime in Canada 2002* (Ottawa: CISC, August 2002) (on-line version at: www.cisc.gc.ca). See also: Ken Nyhuus, “Chasing Ghosts: Asian Organized Crime Investigation in Canada”, *RCMP Gazette*, vol. 60, nos. 9 & 10 (September-October 1998), pp. 46-55, 63.

social costs (such as health care and law enforcement), and has created a money-laundering industry that sustains OC and risks corrupting legitimate businesses and financial institutions. But, as bad as they are, these problems by themselves are unlikely to sunder the foundations of the state. So their relationship to national security is tangential at best.

By contrast, OC-driven illegal immigration activity, such as human smuggling, is - or ought to be - a major national security issue for Canada. BC-based Asian gangs have penetrated BC ports and work with other OC groups to smuggle contraband into and out of Canada. Thus they are ideally situated to exploit the trade in illegal immigrants. Human smuggling costs the federal and provincial governments \$ 120-400 million per year to support and process 8-16,000 migrants smuggled into Canada each year (over and above interception and enforcement costs). Moreover, the federal government is unable to keep track of many illegal migrants once they enter the country. This discredits and undermines support for national immigration policies.¹⁵ It also calls into question the integrity of Canada's borders and raises the spectre of terrorists slipping into the country undetected. Even though none of the 9/11 hijackers entered the US through Canada, the illegal immigration problem and Canada's immigration policies generally have been matters of great - if overstated - concern to the US since 9/11.

The intersection of OC and terrorism would be a genuine, serious national security issue. In the post-9/11 threat climate, police and security intelligence have been watching for any major contacts between OC and terrorists. But recent public reports by the Criminal Intelligence Service of Canada and the Canadian Security Intelligence Service provide no evidence that OC groups and terrorist groups interact in Canada.¹⁶ In November 2002 Ward Elcock, the Director General

¹⁵ Samuel D. Porteous, *Organized Crime Impact Study* (Ottawa: Solicitor General Canada, 1998), pp. 3-6, 12-20; CISC, *Annual Report 2002*; Canada, Senate, *Canadian Security and Military Preparedness: Report of the Standing Senate Committee on National Security and Defence*, 1st Session, 37th Parliament, February 2002, pp. 43-48.

¹⁶ CISC, *Annual Report 2002*; CSIS, *Perspectives Report # 2000/07 Transnational Criminal Activity: A Global Context*, 17 August 2000 (online version at: www.csis-scrs.gc.ca); CSIS, *Background Series No. 8 Counter-Terrorism*, 9 August 2002 (online version at: www.csis-scrs.gc.ca).

of CSIS, explicitly downplayed any alleged links between criminals and terrorists. In his view, groups like *al-Qaeda*

are ... unlikely to expose themselves to investigation by participation in criminal endeavours.... the heightened vigilance on the part of authorities at all levels in North America in the wake of the US attacks has reduced ... the likelihood of such petty criminal activity. Moreover, if such individuals have a larger plan, they will not jeopardize it by engaging in petty crimes that would expose them to prosecution and visibility.¹⁷

That said, “Terrorists ... are also involved in other forms of crime - including money laundering, drug smuggling, identity fraud and people smuggling.” As the Nathanson Centre for the Study of Organized Crime and Corruption says, terrorist group activities “are linked to transnational crime” in two ways - the criminal nature of terrorist activities themselves, or a group engages “in other transnational crimes in order to advance the objectives of the ‘terrorist group’”. The links have always been there.... Rather than a long-term strategic alliance, the ‘linkage’ [if any] may be a short-term tactical move.” But there are significant differences [of motive/goal]: “Money is the *objective* for criminal groups - money is the *tool* for ‘terrorist’ groups....”¹⁸

These are sound assessments, and actual cases are rare. According to a 1995 study, to support their insurgency in Sri Lanka, Canadian-based members of the Liberation Tigers of Tamil Eelam (LTTE - aka the Tamil Tigers) engaged in: violent harassment and extortion of the Tamil emigre community, mainly in the Toronto area; illegal immigration; document fraud; and narcotics trafficking.¹⁹ A more recent RCMP report said that street violence connected to the LTTE

¹⁷ CSIS, *Speaking Notes for W. P. D. Elcock, Director General of the Canadian Security Intelligence Service*, 7 November 2002 (online version at CSIS website).

¹⁸ *Nathanson Centre Newsletter* no. 5 (Summer 2002), p. 17.

¹⁹ *Funding Terror: The Liberation Tigers of Tamil Eelam and Their Criminal Activities in Canada and the Western World. Mackenzie Briefing Notes* (Toronto, December 1995).

has increased in Montreal and Toronto.... outlaw gangs are funnelling money to support extremist activities in Sri Lanka ... although the proof is difficult to find.... Links have also been made to the organized crime activity of these street gangs in Canada, including ... producing false immigration documents for terrorists around the world.²⁰

The point is not that the LTTE has *'links'* to OC, but rather that the LTTE itself engages in serious organized crime in Canada. But this could include 'freelancers' using the LTTE banner to legitimize what is just crime for personal gain. And if the current peace process in Sri Lanka succeeds, the Tamil Tigers' criminal activities in Canada may simply cease. However, they are not alone. The trial of Mohamad Hammoud - a *Hizb 'Allah* cell leader - in North Carolina exposed a racketeering scheme involving cigarette smuggling and credit card fraud. Two alleged *Hizb 'Allah* members in Vancouver used the proceeds of the scheme to buy equipment (including night vision goggles, and blasting equipment) for the group in Lebanon.²¹ So, even if the terrorist/crime nexus is not large in Canada, neither is it non-existent.

The Implications: An Asymmetric Future ?

Nearly two years have passed since the 9/11 attacks, without a second attack on an equal scale. The US/UK war in Iraq was not accompanied by a single, significant terrorist incident, although the multiple bombings in Saudi Arabia and Morocco followed it by only a few weeks. American and allied intelligence agencies are increasingly confident that they have crippled *al-Qaeda*. But Bin Laden and other key figures remain at large, possibly along the Pakistani border, and the recent attacks show that it would be premature to suggest that *al-Qaeda* is finished. Although the US is withdrawing its military presence from Saudi Arabia, since Iraq is no longer a threat, the rest of Bin Laden's global vision lies unfulfilled. Even if it is unachievable, *al-Qaeda*

²⁰ Heather Hamilton, "The Hands of Terror", *RCMP Online* (June 2000), www.rcmp-grc.gc.ca

²¹ Stewart Bell, "Terrorists Plotted to Kill Prosecutor, US Court Told", *National Post*, 28 February 2003.

seems determined to pursue it. While many of the warnings of further attacks may be incorrect, after 9/11 no one can afford to ignore them. Until proven otherwise, we must assume that *al-Qaeda* will continue to pose some degree of threat for the foreseeable future.

While there are many terrorist groups in the world, only the other *Jihadist* groups, such as *Hamas* and *Hizb'Allah* and similar groups, are motivated to the same extreme degree as *al-Qaeda*, and most lack its resources. They operate mainly in the Middle East, but in certain circumstances, such as a joint Israeli-Palestinian crackdown on such groups as a pre-condition for a peace agreement, it is conceivable that they could shift their operations to the international arena and attack those states that support the peace process or the on-going War on Terrorism. Clearly, the US would be the prime target of their wrath, but its major allies might be attacked as well to 'punish' them for supporting the US position or to dissuade them from doing so. Given the predilection of *Jihadist* groups for '*Islamikaze*' attacks, it seems reasonable to conclude that we have not seen the end of mass-casualty terrorism.

Cyber threats will continue to multiply, in frequency, scale, and disruptive capacity. Even if they fall short of being 'The Big One' that takes down the entire Internet and the whole national Critical Infrastructure with it, they will exact financial and possibly human costs. These, and the consequent search for security solutions, will be among the endemic costs of e-business and of electronic interdependence generally. Likewise, trans-national organized crime is here to stay. TNOG by itself does not pose a *significant direct* challenge to Canada's national security. But it will remain a foreign policy issue because affects Canada's relations with other countries.

All of this suggests that these emerging non-traditional 'Asymmetric' threats are not a temporary phase. They will play a part in Canada's foreign policy and national security futures on a permanent basis - at least for the foreseeable future. But their intensity and relative importance may vary over time, both at home and overseas. What, then, are the implications of this for Canadian foreign and national security policy ?

Of the three non-traditional threats, only terrorism has the potential for mass casualties and destruction. This suggests that it should automatically have the highest priority. But unlike

cyber-sabotage and organized crime, which are constants, terrorism combines low likelihood with high consequence. This poses something of a conundrum for Canada. It may be politically difficult to justify allocating scarce resources to the least likely problem, but the consequences of failing to do so could be so serious that there may be no alternative. How, then, can Canada maximize the return on its investment in national security ?

First, it should give top priority to intelligence, the first line of defence against terrorism. *All* successful counter-terrorism campaigns and operations have been based on good intelligence. If effective, it can anticipate threats (allowing security forces to prevent them), provide ‘early warning’ of imminent attacks (allowing the government to avoid surprise and thus minimize the impact of attacks), facilitate investigation, arrest and prosecution of terrorists and penetration and destruction of terrorist groups.²² British general Frank Kitson said it best in his book *Low Intensity Operations*, published more than thirty years ago: “The problem of defeating the enemy consists very largely of finding him.”²³ Money, time, and people invested and used wisely in counter-terrorism intelligence will pay dividends beyond all other measures. Good intelligence allows governments to manage risk and to allocate scarce resources appropriately. It helps political leaders to deal with the problem in a well-informed manner rather than in a reactive, crisis-driven mode. Thus, intelligence is essential to maintaining democratic processes and values while countering terrorism effectively. It provides the direct link between *understanding* the problem and *responding* to it. However, it must be noted even the most capable intelligence services *cannot* anticipate and prevent *all* terrorist attacks. Surprise can only be *minimized*, not eliminated.

For Canada, giving priority to counter-terrorism intelligence has a number of

²² David A. Charters, “Counterterrorism Intelligence: Sources, Methods, Process and Problems” in David A. Charters, ed., *Democratic Responses to International Terrorism* (Ardsey on Hudson, NY: Transnational Publishers, 1991), p. 227.

²³ Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peacekeeping* (London: Faber, 1971), p. 95.

implications. First, it must confront squarely the question of whether or not Canada needs a foreign intelligence service. Such a service would collect intelligence by clandestine means abroad, in a manner similar to the espionage operations of the CIA or MI6. In the wake of 9/11, the issue has regained saliency, but thus far, the government has not “grasped the nettle”. This is not surprising; it is a politically-charged issue, and in the absence of a direct attack on or threat to Canada, the need for it does not appear to be pressing. The fact that there have been no attacks in Canada since 9/11 could mean that CSIS has been effective in preventing them, or that the threat has been minimal. If so, then perhaps the issue is moot. But if not and there is a need for clandestine foreign intelligence collection to counter terrorism, then it would be best to address the question in a time of relative calm, rather than in the heat of reaction to a major incident.

Canada has two options in this regard. One may be to expand the remit of CSIS. It already has some capacity to collect information abroad, so it might be feasible to add a foreign espionage branch. That has a number of political, legal, organizational, and civil liberties ramifications. The alternative is to create a separate foreign intelligence service ‘from scratch’. Whatever approach is chosen, there should be public debate, inside and outside parliament. Discussion must be realistic. The government would have to be clear about what its foreign intelligence needs are. Likewise, the intelligence community will have to be forthright about what a foreign service can and cannot deliver, and what the ‘price’ will be. A new service would require a substantial investment of resources: people, training, installations, and above all, money. It would take time to develop expertise, to cultivate sources, to generate useful products, and thus to prove its value. For its part, government would have to demonstrate long-term political and fiscal commitment.

This would demand patience on the part of Canada’s political leaders, and a willingness to accept the inevitable errors and ‘growing pains’. Moreover, in the current climate, even in the wake of 9/11, creating a foreign intelligence service would be ‘hard sell’ politically. For any Canadian government, it would require an extraordinary act of political courage.

Which brings us to the second point: changing attitudes toward intelligence. As academic

Martin Rudner has observed, Canada does not have a “national security culture.”²⁴ In private, senior officials acknowledge that, as a consequence, “We don’t have an ‘intelligence culture’ at the highest levels of government in Canada.” Since Canada is usually a follower rather than a leader in international affairs, Canadian political leaders don’t see the need to make immediate decisions. So they don’t display any urgency to have and to use intelligence. The decision-makers who do use intelligence prefer short digests without much detail; the result is a product that doesn’t appear to be very different from what they read or see in the news media. So, it is not ‘impressive’, and therefore, doesn’t generate a ‘must have’ attitude on the part of consumers. Insofar as policy- and decision-making is concerned, they tend to see intelligence as confirming what they’ve already decided or what they think they know, rather than a ‘value added’ asset. Finally, intelligence usually does not provide the level of ‘proof’ that political leaders expect; there is rarely ‘a smoking gun’. More often it offers a lot of circumstantial evidence that adds up to a conclusion in the mind of a knowledgeable analyst, but that leaves a politician unpersuaded. Since 9/11, however, attitudes have changed somewhat; more senior officials are beginning to realize that they need intelligence to stay on top of situations. But, there is still a major ‘education’ job to do among our political leaders about the value, utility, and limitations of intelligence for decision-making. That is why an open and *informed* debate on a foreign intelligence service is so essential.

Third, and closely related to the first two points is the question of intelligence management and direction. National security and intelligence missions are shared among some sixteen agencies and departments, including: Privy Council Office (PCO), Solicitor General Canada (responsible for RCMP, CSIS, and Criminal Intelligence Service of Canada), National Defence (which administers OCIEP and the Communications Security Establishment, the SIGINT service), Treasury Board Secretariat (responsible for government-wide security policy),

²⁴ Martin Rudner, “The Threat of Global Terrorism: Canada’s Security and Intelligence Community Responds”, *RCMP Gazette*, vol. 64, no. 4 (2002), p. 24.

and the Financial Transactions and Reports Analysis Centre, which tries to track terrorist and criminal finances.²⁵ The sheer number of these bodies and their different roles and functions makes inter-agency and cross-jurisdictional cooperation essential. “We are trying to create a new club - the counter-terrorism club”, one official told the author. “We are trying to determine what the rules are, how you become members. Counter-terrorism *has* to be multi-agency, but the implications of that are not fully understood. The national security *community* doesn’t quite exist yet. Everyone is in ‘a state of becoming’.” The RCMP and CSIS now cooperate effectively on national security, but elsewhere much remains to be done. To ensure that intelligence-sharing works, the government needs to resolve: technological standardization and inter-operability problems; jurisdictional responsibilities; and information security issues: access, security standards, privacy and disclosure.

The management and direction problem this poses is quite simple; to paraphrase then Foreign Affairs Minister John Manley’s remarks in the wake of 9/11, “There is no one person in government who wakes up in the morning and says ‘I am responsible for the security of Canada’.” In a formal sense, this is the Prime Minister’s responsibility. But in fact, the Solicitor General probably comes closer than anyone to filling that role. Yet, clearly it is not that minister’s job alone. Indeed, it is doubtful that it could be any single *person’s* responsibility.

The most senior intelligence body is the Security and Intelligence Secretariat in the PCO, which provides intelligence advice on national security and foreign intelligence issues to the Prime Minister and cabinet. The PCO’s Intelligence Assessment Secretariat (IAS) provides a central analytical capability that draws upon government-wide inputs and produces assessments of developments in foreign countries. The IAS Executive Director chairs the Intelligence Assessment Committee (IAC), which brings together representatives from all departments and agencies that produce, assess and consume intelligence. The IAC produces long-range

²⁵ Privy Council Office, *The Canadian Security and Intelligence Community: Helping Keep Canada and Canadians Safe and Secure* (2001).

intelligence assessments of immediate interest to policy/decision-makers. The IAS and IAC are quite small, but were given additional analytical resources in the wake of 9/11. If Canada chooses not to create a foreign intelligence service, thus retaining its considerable dependence upon its allies, a central analysis function will gain increased importance to ensure a 'Canadian' product. That capability might be strengthened, for example, by moving the DND's Directorate of Strategic Analysis to the IAS.

However, the PCO's S&I Secretariat does *not* provide central *direction* for the national intelligence community. In the absence of a single person or agency in this leading role, there is no way of ensuring at present that *all* of the 'players' are working *cooperatively* and *effectively* toward the common purpose of national security. Much depends on informal, personal working relationships, which take time to develop and require constant 'maintenance'. This appears to leave an awful lot to chance. Thus, it seems reasonable to suggest that an examination of the foreign intelligence issue should include options for improving national intelligence *coordination*.

Fourth, given the centrality of 'messages' to terrorism and of Information Operations (IO) generally to other forms of low-intensity conflict (including peacekeeping), the government needs to address the 'Information Warfare' (IW) issue. The CF has a limited military IW capability in its IO Group, which is used to support CF operations. But does Canada need a 'national IW service', in the same sense that CSE serves as the national SIGINT service? This raises a host of other important questions. What could such a service be expected to achieve? Would it be limited to the IW dimension of countering terrorism, or should it have a wider remit across the full spectrum of low-intensity conflict, including 'cyber-war' and cyber-security? Should it be purely defensive or does Canada require an offensive (or at least proactive) IW capability? What sorts of messages would it be permitted to convey? How would these be coordinated with other national-level information programs and themes? Should it be operate only within Canada, or should it be 'deployable' to support foreign policy initiatives and military operations abroad? In that regard, is it a strategic or a tactical asset? How should it be organized

and where should it reside - under an existing department or as a 'stand-alone' agency ? All of these questions need to be answered.

Finally, the government must decide how it will exercise the limited military power it has at its disposal, i.e., what it wants the armed forces to do. Does it require armed forces for internal security and continental defence, and if so, what form should that take ? Does it need or want an 'expeditionary' capability ? If so, for what kinds of missions and on what scale ? Three factors will impact on this. First, the nature and sources of the 'Non-Traditional' threats discussed above mean that Canada's *internal* security cannot be separated from its *trans-border* and *continental* security responsibilities. Second, in the internal/continental arena they put a premium on policing and intelligence, rather than military operations. Finally, as a result of prolonged budgetary shortfalls, the Canadian Forces (CF) now have only limited capabilities for either internal/continental security or expeditionary missions. With regard to the latter, at present the CF are capable only of small-scale, short-duration, low-intensity operations.

The CF roles in counter-terrorism for internal and continental defence are quite limited. Even if *al-Qaeda* or a similar group attacked a target in Canada, their preference for mass casualties probably would make a hostage/siege or situation the least likely scenario. But, however remote the eventuality, Canada's obligation to protect foreign missions and high-value Critical Infrastructures (eg., nuclear power plants), from attack or seizure, and to be able to terminate airliner hijackings means that the CF must retain JTF2 for those purposes. Likewise, there is probably only a remote possibility that some rogue state or terrorist group might try another 9/11-style airliner attack or launch a cruise missile from a cargo ship offshore against North American targets. This means there is still a requirement for air/seaspace control, including surveillance systems, interceptor aircraft, naval vessels (with detection, tracking and interdiction capabilities), and low-level air defence artillery/missile systems. The scale of investment required and specifics of systems and locations lie beyond the scope of this paper. It must be acknowledged that this could involve considerable cost. However, if Canada does not provide this, the US will - with or without the consent of the Canadian government. Therefore, Canadian

participation in NORAD remains relevant in the 21st Century. Without it, we lose not just access to a whole range of bilateral defence forums, but also a say in our own defence. In sum, the CF cannot eliminate its continental security role, however small, without surrendering sovereign control of Canadian air/seaspace to the United States.²⁶

A Canadian military contribution to internal and continental security is *the necessary minimum*. But is that sufficient? Michael Ignatieff argues that in the international realm Canada cannot have it both ways - “talking the talk” of commitment to multi-lateralism, peacekeeping and protection of universal human values, while refusing to “walk the walk”, that is to “put its money where it’s mouth is”.²⁷ The gap between Canada’s words and its deeds has eroded the confidence and trust of our allies and undermined our credibility in every international forum that matters. If Canada is to regain that trust and credibility, then it will have to restore a capability in the CF to conduct sustained expeditionary operations, at least in the low-intensity spectrum, including both peacekeeping and counter-terrorism missions. It should be able to do them well, on a scale that will have a ‘value-added’ impact on the ground and among our allies, the UN, or in a coalition

If the government accepts that an *effective* expeditionary capacity is necessary to restore Canada’s influence among its allies, then what should it consist of? Recent experience from operations in Afghanistan, the Balkans, and Africa suggests that a battalion-based battle group should be the *baseline*. But, realistically, to demonstrate commitment the CF should have the resources to deploy overseas up to a brigade to a single theatre of operations, or two battle groups on simultaneous but separate operations in different theatres. In either case, the formation should comprise the full, appropriate mix and balance of combat and support elements. This would

²⁶ Canada, Senate, *Defence of North America: A Canadian Responsibility. Report of the Standing Senate Committee on National Security and Defence*, 1st Session, 37th Parliament (September 2002), p. 24.

²⁷ Michael Ignatieff, “Time to Walk the Walk: Canada’s Faith in Multilateralism Must be Defended - by Force if Necessary”, address to Institute for Research on Public Policy, 15 February 2003.

include full-strength infantry battalions, armoured reconnaissance, anti-armour, light artillery and air defence (if needed), *combat* engineers, armed and transport helicopters, headquarters staffs, C4I and IO support, and all the necessary surface transport and logistical capabilities to sustain the formation in-theatre for a *minimum* of six months or up to a *year* if necessary.

The implications of this are significant, in terms of resources and cost. First, the capacity to deploy a brigade overseas implies the need to maintain two brigades at home; one engaged in post-operation rebuilding and retraining, the other ‘working up’ for deployment. Each of the brigades should comprise at least two full-strength infantry battalions (ideally three), plus the other elements noted above, as well as augmentation and reinforcement ‘surge’ capacity in the reserves.

Second, to deploy these forces overseas, it would be unwise to be wholly dependent on allies or on chartered ships and aircraft. Circumstances may arise where our allies choose not to join specific operations, commercial carriers are unavailable in a timely manner, or are inadequate for CF needs. Therefore, to ensure that Canada retains the capacity for independent action the CF must have some modern strategic airlift and sealift. Again, the specific numbers and types cannot be addressed here, but some general principles can be established. It should give Canada ‘global reach’. It should be self-sustaining in remote, difficult, and hostile terrain/waters /airspace. It must have the capacity to move all types of CF vehicles and cargo; the sealift, in particular, should have ‘roll-on, roll-off’ and amphibious capability. Finally, there should be sufficient capacity to support prolonged overseas operations with minimal dependence on allies.

Third, it will have to re-invest in the CF Intelligence Branch. The Branch is of high quality, with experienced personnel and some up-to-date, interoperable, IT and ISTAR systems. However, it is small and spread too thin. It lacks surge capacity and sustainability, and its technological edge is aging and diminishing. If the CF is to regain a capacity for expeditionary operations, then it will need more personnel (regular and reservist), better intelligence skills (languages, analysis), new organization (all-source ‘fusion’ centers), and ‘cutting edge’

technology appropriate to low-intensity operations. This does not mean that the CF must be able to field *all* of the ‘state of the art’ RMA systems, such as surveillance satellites, but it should have *some* remote-sensing ability. Equally, if not more important, the CF needs the technology that would allow it to share/receive intelligence with the most capable RMA-driven forces, ie., the US military. And since low-intensity operations put a premium on ‘Contact Intelligence’, CF intelligence doctrine will have to instill the mindset that everyone is a potential source and every soldier is an intelligence collector.²⁸

The final capability that must be reviewed further is the role of Joint Task Force 2 (JTF2). The wars in Iraq and Afghanistan have highlighted the utility of Special Operations Forces (SOF). They are capable of a wide range of missions in the low-intensity environment. These include: counter-terrorism; direct action; covert reconnaissance; IO and Psyops; and civil affairs, among others.²⁹ JTF2's original mandate has been expanded to include SOF missions and they have been used in that regard in Afghanistan. The government has decided to increase the size of JTF2 so that it can maintain its domestic counter-terrorism role and conduct special operations overseas. However, before DND assigns more of its limited resources to a larger SOF unit, it needs to consider carefully two important points. First, at current army personnel levels, the CF cannot afford a larger JTF2, as it can come only at the expense of units which are already under-strength and over-tasked.³⁰ Expanding the unit now will reduce Canada's already limited capacity to conduct other low-intensity operations. Nor can it be done ‘on the cheap’; it must be done well. Therefore, expansion of JTF2 should be contingent on an expansion of the army as a whole.

²⁸ David A. Charters, “The Future of Military Intelligence Within the Canadian Forces”, *Canadian Military Journal*, vol. 2, no. 4 (Winter 2001-2002), pp. 47-52.

²⁹ Lieutenant-Colonel Bernd Horn, “A Self-Evident Truth: Special Operations Forces and Intelligence in Asymmetric Warfare”, paper presented at Conflict Studies Conference, 5 October 2002, since published in *Canadian Military Journal*.

³⁰ House of Commons, Standing Committee on National Defence and Veterans Affairs, *Facing Our Responsibilities: The State of Readiness of the Canadian Forces*, May 2002, pp. 42-43.

Second, special operations are inherently 'high risk', both militarily *and* politically. If operations are exposed or go wrong, the unintended consequences can be severe and 'ugly'. They cannot always be 'plausibly deniable'. So, the political, departmental, and military leadership need to ask themselves whether they can live with the risks and consequences. If they cannot, and if the army itself is not substantially increased, then JTF2's roles should be restricted and its growth curbed.

Given the fact that the terrorist threat to Canada is uncertain, it would be politically difficult to 'sell' a significant re-investment in the Canadian Forces on the counter-terrorism mission alone. But that is not necessary; all of the foregoing could be justified honestly on the basis that these capabilities are essential to restore Canada's pre-eminence in peacekeeping.

Conclusions

Canada faces a future of considerable uncertainty in the foreign policy and national security arenas. It confronts a number of non-traditional asymmetric threats whose intensity, scope, scale, targets and timing cannot be known with any precision. The risk of terrorist attack in Canada or against Canadian interests or citizens overseas may be remote, but the possibility can't be ignored. And the nature of these threats means that Canada cannot address them in isolation; threats to us are also threats to our neighbours and allies. That applies as much to trans-national organized crime and cyber crime as much as it does to terrorism. This imposes on Canada obligations to ensure that it is not the 'weak link' in collective security. Nor can we simply leave it to the US and other nations to expend their 'blood and treasure' to ensure our security without being prepared to do so ourselves. Not only would that cost us credibility and influence; ultimately, it could cost us our sovereignty. Finally, we need to recognize that terrorism presents a fundamental challenge to values that Canada claims to uphold at home and abroad. Words alone will not protect them. So, Canada must re-invest in national security in the non-traditional arena as well as in familiar areas. This will make policy-making, planning, and resource allocation very difficult. It also could be very expensive. Asymmetric threats may fall within the low-intensity spectrum, but that does not mean that the counter-measures are low-cost. At a time

when there are many legitimate demands on the national treasury, making the case for these commitments will be politically difficult. It will require patience, wisdom, and the courage to show that making the investment and using it is consistent with Canadian values. To fail to address these issues and to invest accordingly will be to trust the fate of Canadians and of our allies to chance, luck, and wishful thinking. In the post-9/11 world, that would be as unwise as it is immoral.

Summary of Implications

Non-Traditional Threats

1. Terrorism is the primary 'non-traditional' security threat to Canada. However, the degree of threat is uncertain. Canada could be affected by attacks against the United States.
2. 'Cyber-Terrorism' has *not yet* become the problem it was expected to be a decade ago. But hacking and sabotage will be constant challenges for cyber-security.
3. There is no evidence that terrorists and organized crime are collaborating in Canada. However, some terrorist groups engage in organized criminal activity on their own to support themselves.
4. These three problems are likely to remain 'permanent' fixtures for the foreseeable future.

Canadian Responses

1. The government should give top priority to counter-terrorism intelligence.
2. Canada needs to engage a serious public debate about creating a foreign intelligence service.
3. The government needs to enhance national intelligence coordination and national-level strategic analysis, and to educate senior political leaders in the use of intelligence.
4. There is a need to examine Canada's Information Operations requirements.
5. Canada requires some capabilities for surveillance, control, and defence of Canadian and North American territory, air and sea space against terrorist-type attacks. Therefore, the Canadian roles in NORAD and other continental defence arrangements with the US remain relevant. Our role need not be large, but if Canada does not do it, the US will do it at the cost of our sovereignty.
6. Canada should maintain a capability to undertake sustained expeditionary low-intensity military operations, including both peacekeeping and counter-terrorism missions. It should be

able to make ‘value-added’ contributions to allied (eg., NATO), UN, or other coalition operations.

7. Battalion-based battle group formations should be the *baseline*, but the CF should be able to deploy a brigade-size, all-arms force. This calls for a full-strength, three-brigade regular army.

8. Canada must have some modern strategic airlift and sealift, with the range, sustainability, and capacity to support prolonged expeditionary operations without depending on other sources.

9. The government will have to re-invest in the CF Intelligence Branch to support CF operations.

10. Any expansion of the size, capabilities and missions of JTF2 should not be at the expense of the under-strength army, but should be contingent on the re-building of the army as a whole.

Endnotes