CONTEMPORARY THREATS, FUTURE TASKS: CANADIAN INTELLIGENCE AND THE CHALLENGES OF GLOBAL SECURITY

Martin Rudner
The Norman Paterson School of International Affairs
Carleton University, Ottawa

Canada's intelligence community consists of a complex web of functionally differentiated agencies for the collection, assessment and protection of security-relevant knowledge on behalf of this country's foreign policy, security and defence establishment. There are, as well, specialized organizations with mandates for the oversight of the intelligence services so as to ensure compliance with law. It is convenient for analytical purposes to characterize Canadian intelligence requirements by scope and function in terms of two distinct spheres of operations: security intelligence and foreign intelligence (Auditor-General, 1996). Security intelligence relates to activities that could threaten Canada' s domestic security, such as espionage, sabotage, foreign-influenced activities or politically motivated violence, and is collected to help maintain public safety and protect national security. Foreign intelligence addresses the capabilities, activities or intentions of foreign countries, organizations or individuals, and is required to serve Canadian national interests, including its geo-strategic, economic, military, scientific/ technological, environmental and social policy objectives. Intelligence informs many spheres of government decision-making and policy analysis, however what distinguishes intelligence from other information resources is its sensitivity and intrusiveness, which precipitates collection by clandestine means as well as from open sources (Herman, 2001).

In Canada, responsibility for security intelligence is assigned primarily to the Canadian Security Intelligence Service (CSIS), a civilian agency established under statute in 1984, which took over that function from the Royal Canadian Mounted Police (RCMP). Canada does not have (and never has had) a dedicated foreign intelligence service of its own, unlike most other NATO members and similarly situated middle powers like Australia or Sweden. Rather, the Canadian role in foreign intelligence is confined mainly to signals intelligence (SIGINT) collection by the Communications Security Establishment (CSE), to certain CSIS activities abroad relating to Canada's security, and to the defence intelligence function of the Canadian Forces. Canada's own efforts in the domain of foreign intelligence are significantly augmented by exchanges of intelligence product with allies and partners under various international arrangements.

The end of the Cold War yielded a peace dividend in terms of vastly reduced defence budgets and military establishments generally. Nevertheless, the past decade has witnessed a major upsurge in intelligence requirements and capabilities in response to a more challenging and more diffuse threat environment coupled with far-reaching technological advancements in information gathering and processing. The aftermath of the 11th September terrorist attacks on the United States prompted a sharply increased appropriation of resources, federal and even provincial, for security and intelligence. The study that follows examines the evolving role of the

---

This is a draft text of an article published in Norman Hillmer & Maureen Appel Molot, eds., *Canada Among Nations 2002: A Fading Power* (Toronto: Oxford University Press, 2002, pp.141-171.

Canadian intelligence community in terms of its policy direction, operational agenda, collection capabilities, intelligence assessment functions, international liaison, and oversight processes. A concluding section considers future challenges for Canadian intelligence policy.

THE DIRECTION OF INTELLIGENCE POLICY

The Canadian political system does not confer overall responsibility for security and intelligence on any single government department. By convention, the Prime Minister, as head of government, exercises broad high-level leadership in areas of major importance to the national interest, most notably international affairs, national unity and security, and economic and trade policy. The setting and coordination of policy directions for intelligence falls within this Prime Ministerial function (Privy Council Office [PCO], 2000). In particular, the Prime Minister chairs the annual Meeting of Ministers on Security and Intelligence and the cabinet decision-making process, appoints bureaucratic heads of the security and intelligence organizations, and from time to time takes personal charge of certain specifically sensitive issues. In October, 2001, in the aftermath of the terrorist attacks on the United States, the Government set up a high-profile Cabinet Committee on Security, chaired by the Minister of Foreign Affairs, John Manley, and given an unprecedented mandate to coordinate and supervise Canada's couinter-terrorism effort, including its intelligence component.[1]

The Prime Minister is supported in performing these responsibilities by the Privy Council Office (PCO), the central agency of the Government of Canada. The Clerk of the Privy Council chairs the Interdepartmental Committee on Security and Intelligence, a deputy-ministerial body that deliberates on strategic policy and resourcing issues, reviews national security affairs, and makes recommendations to ministers and Cabinet on intelligence matters, including the annual Meeting of Ministers on Security and Intelligence. The PCO Deputy Clerk, Counsel and the Security and Intelligence Co-ordinator supervises and co-ordinates the security and intelligence activities of all Canadian government agencies and departments and manages international intelligence relationships. The PCO houses two specialized intelligence-related secretariats reporting to the Deputy Clerk: a Security and Intelligence Secretariat dealing with policy matters and the Intelligence Assessment Secretariat which produces integrated all-source assessments of political, economic, and strategic intelligence for the Prime Minister, Cabinet, Ministers and senior officials.

Ministerial responsibility for the Security and Intelligence Community is divided among several departmental portfolios, sometimes in curiously intricate ways. CSIS comes under the ministerial jurisdiction of the Solicitor General, Canada's senior law officer. In February 2001, the Solicitor-General issued a revised compendium of Ministerial Directions to CSIS, a classified document setting out strategic guidelines and streamlining its policy and management framework (SIRC, 2001). CSE, for its part, has a bifurcated reporting relationship to the Deputy Minister of National Defence for financial and administrative issues and to the Deputy Clerk, PCO on policy and operational matters. The Minister of National Defence has ministerial responsibility for defence and military intelligence (J2) and for the Office of Critical Infrastructure Protection and Emergency Preparedness. Intelligence and security units of other federal departments and agencies, such as Foreign Affairs and International Trade, Transport, Citizenship and Immigration,

Canada Customs and Revenue Agency, and RCMP, report to their respective ministers.

The primary forum for collective ministerial participation in intelligence policy-making is the annual Meeting of Ministers on Security and Intelligence, where intelligence priorities for the Security and Intelligence Community are determined. The newly created Cabinet Committee on Security is likely to play a key role in the overall direction of Canada's intelligence effort and in deliberations over policy, organizational and resource matters.

INTELLIGENCE AND THE POST-COLD WAR SECURITY AGENDA

In 1991, following the end of the Cold War, the federal Cabinet issued for the first time a directive on intelligence priorities setting out its urgent requirements for foreign intelligence collection (Auditor-General, 1996). These priority requirements have been updated almost annually since then. Among the current priorities are international terrorism, ethnic and religious conflict, proliferation of weapons of mass destruction, illegal migration, transnational organized crime, economic (counter-)espionage, and trade intelligence. These priority requirements have been given operational expression in **the tasking assigned to the Canadian intelligence community.** National Requirements for Security Intelligence are determined annually, including a general direction from Cabinet given direction as to where CSIS should focus its efforts and setting out guidelines for its intelligence collection, analysis and advisory functions. These priority requirements have been given operational expression in **the tasking assigned to the Canadian intelligence community.** As regards foreign intelligence collection, the contemporary priorities imply the targeting of neutral and friendly countries.

While the intelligence agencies never divulge operational targets or methods, various government reports, other disclosures, media accounts and information from foreign sources provide some indication of the direction and purpose of Canada's intelligence activities.

It is pertinent to note that the emergence of a "new" post-Cold War threat environment has not displaced the more traditional threats to Canada's homeland security so far as the intelligence community is concerned. Canada remains vulnerable to threats of espionage or menacing conduct on the part of former adversaries like Russia, or newly assertive powers like China or India, rogue states like Iran, Iraq or Libya, or even ostensibly friendly countries (CSIS, 1997). For instance, clandestine French activities in support of Quebec separatism were closely monitored and countered by Canadian intelligence services (Black, 1996). Incidents have occurred in which aggressive foreign agencies, like those of Iran, tried to procure illegal weaponry and military technology, evade internationally-mandated sanctions, and even foment civil unrest in Canada (Security and Intelligence Review Committee [SIRC], 2000). Canadian intelligence services also responded to security risks arising from attempts on the part of foreign governments to exercise improper influence on Canadian decision-making or public opinion, interfering with recent immigrants or homeland communities in Canada, or intruding upon Canada' s own communications systems (PCO, 2000).

The post-Cold War security agenda, for its part, has radically different implications for the functions of intelligence (Treverton, 2001). Whereas in responding to traditional threats the intelligence services are able to target specific countries or government, in new threat environment there are numerous, vaguely defined, mostly non-state targets. Intelligence regarding traditional threats is typically scarce and difficult to acquire, and the most reliable

sources tend to be privy to the intelligence community; by way of contrast, information about the newly emergent threats tends to be widely dispersed among a multitude of sources, little of which is either reliable or owned by intelligence services. There are relatively few consumers for traditional threat related intelligence, mainly security and defence officials, whereas intelligence about the new threats has many prospective consumers across the departments and agencies of Government.

Even prior to September 11th international terrorism figured prominently on the threat assessments of Canada's foreign and domestic security intelligence services (CSIS, 1997). Many of the world' s terrorist groups have established a presence in Canada, virtually all of them relating to ethnic, religious or nationalist conflicts elsewhere in the world (CSIS, 1999). Among the international terrorist organizations or fronts active in Canada are the Al-Qaeda network, Hezbollah and other Shiite Islamic terrorist organizations from the Middle East, the Palestinian Hamas, the Algerian Armed Islamic Group (GIA), Al-Jihad, the Provisional Irish Republican Army (PIRA), the Liberation Tigers of Tamil Eelam from Sri Lanka, the Kurdistan Workers Party (PKK) from Turkey, and virtually every significant Sikh militant group from India.

These international terrorist organizations typically maintain a presence in Canada in order to raise and transfer funds, procure weaponry and material, set up operational sanctuaries, and to support infiltration across the border to the United States or overseas. Cells of groups like Al-Jihad and GIA engage in financial fraud and theft, identity and document forgery, and people smuggling in support of their parent terrorist networks (Blatchford, 2001). Reported links between the Al-Qaeda network in North America and Montreal-based presence of the Algerian GIA exemplify this emergent globalized threat environment (Soloman, 2001; Sachs, 2001). Intelligence regarding terrorist threats will require new and challenging methods of penetrating tightly closed cells and loosely structured networks, and will have to depend on synergy with partners and allies, not all of which will be states (Treverton, 2001). The primary responsibility for counter-terrorist intelligence is vested in CSIS, working together with other pertinent government departments (*eg.* Citizenship and Immigration, Department of Justice), RCMP and local police forces.

Canadian foreign and security intelligence attention is also directed at the connection between trans-national criminality, on the one hand, and terrorist racketeering and criminal collaboration with insurgency movements elsewhere, on the other. International terrorist groups have taken over legitimate businesses and even Non-Governmental Organizations (NGOs) as a means of money laundering and in order to disguise their activities. Among the more notorious instances, the Liberation Tigers of Tamil Eelam established an underground network among Tamil sympathizers across Canada and also became extensively involved in racketeering to generate financing for their insurgency war in Sri Lanka (Porteous, 1996, Aryasinha, 2001). Intelligence sources were instrumental in uncovering Middle Eastern organized criminal groups involved in transferring funds and stolen equipment to Hezbollah in Lebanon, including stolen vehicles (Bell, 2000). Criminal-terrorist syndicates were reportedly active in drug trafficking, immigrant smuggling, commercial fraud, and extortion from homeland residents in this country and elsewhere.

Trans-national crime has been defined as a national security threat, thus warranting the attention of Canada's intelligence services. (Porteous, 1996). Organized criminal enterprises, which move money, people and contraband, including drugs, across borders, Canada' s included, seemed beyond the control of domestic law enforcement agencies alone. Moreover, some of the

more insidious attempts at major international fraud, corruption and financial manipulation were perceived as undermining the very foundations of legitimate governments, democratic institutions, and social order. By way of response, the governments of Canada and other allied countries decided to task their intelligence services with targeting trans-national crime (CSIS, 1997). CSIS took on a role in combating international criminal activity in Canada, primarily by providing access to international intelligence resources and producing analytical tools for law enforcement agencies (CSIS, 1995).

In order to facilitate international operations against trans-national criminality, the government of Canada, the United States, Australia and various European countries set up a consultative forum, the International Law Enforcement Telecommunications Seminar (ILETS), to coordinate intelligence collection with law enforcement requirements. One of their preeminent concerns was to ensure that design standards for telecommunications equipment and software remain accessible to legal surveillance. Trans-national commercial crime is especially vulnerable to SIGINT interceptions, given its inescapable dependence on electronic means of voice and data communications. Communications interceptions offered a unique window into illicit transactions and criminal activities that threaten the integrity of Canadian financial and commercial institutions (Porteous, 1996). At the same time, this implicit opening of global telecommunications to covert interception aroused much consternation in the European Union, which considered this to be a significant threat to commercial interests and privacy rights (Rudner, 2002).

Canada participates in virtually the entire array of global and regional initiatives to counter the proliferation of weapons of mass destruction and their delivery systems (CSIS, 1997). Canadian nuclear capabilities are devoted exclusively to peaceful purposes. Its non-proliferation foreign policy is aimed at ensuring that Canada' s nuclear exports are utilized solely for intended, non-military purposes, and to promote the evolution of a comprehensive and effective non-proliferation regime. By way of supporting this non-proliferation policy, Canada's Security and Intelligence Community aims at identifying attempts by countries of proliferation concern to acquire Canadian weapons-related technology and expertise. One of the more alarming aspects pertains to students and researchers from WMD-suspect countries enrolling in university programs in nuclear physics or other potentially militarized disciplines, a quarry calling for considerable dexterity and sensitivity in counter-intelligence operations (Smyth, 2002). Intelligence produced by Canadian agencies or obtained from their international sources helps keep the Government and its allies alert to proliferation threats.

THE STRATEGIC CONUNDRUM OF ECONOMIC INTELLIGENCE

Canada and many others countries, including major powers and smaller trade-dependent nations, have made the collection of economic intelligence an increasingly significant function of their respective foreign intelligence services. Governments collect economic intelligence in order to identify opportunities and warn of threats to national macro-economic, trade policy, commercial or scientific/technological interests. As early as 1970, a former Executive Director of the US Foreign Intelligence Advisory Board indicated that economic intelligence had been assigned a strategic priority equivalent to that of traditional diplomatic, military, and technological intelligence collection (Campbell, 1999; Porteous, 1995). Likewise, Canada' s post-Cold War intelligence directives identified economic intelligence among the priorities for targeting (Auditor-General, 1996).

Historically, Canadian operations in the domain of economic intelligence seem to have been primarily defensive in orientation. According to intelligence sources, Canada's chief concern has been to counter economic espionage, defined as "clandestine, deceptive, coercive or illegal activity carried out or facilitated by a foreign government aimed at obtaining access to Canadian proprietary information and/or technology for reasons of economic advantage" (CSIS, 1997). Among the industries which are considered especially vulnerable to foreign economic espionage are Canada's aerospace, biotechnology, chemicals, communications, information technology, mining and metallurgy, nuclear energy, oil and gas, and the environmental technology firms. CSIS has discerned that several foreign governments use visiting students, scientists, exchange personnel, delegations, business people and members of émigré communities to collect clandestine economic intelligence in Canada (CSIS, 2000).

Canada's own efforts at economic intelligence in this age of globalization appear to have concentrated somewhat more ambitiously on targets that improve this country's economic competitiveness and achieve commercial objectives in world markets. Media accounts claim that CSE provided Canadian policy- makers and negotiators with economic intelligence pertaining to international trade negotiations, including the plurilateral negotiations with Mexico on the North Atlantic Free Trade Agreement (NAFTA) of 1994; the 1995 multilateral ("Uruguay Round") trade negotiations; the Asia Pacific Economic Co-operation (APEC) Ministerial and Leaders' meetings in Vancouver in 1997; and bilateral negotiations with South Korea on their procurement of Candu nuclear reactors and with China on wheat sales (Livesey, 1998). The targeting of international economic and business affairs remains, of course, a highly delicate matter, all the more so in view of Canada's overwhelming trade dependence on the United States.

Notwithstanding these activities in the domain of economic intelligence, Canadian businesses do not seem to have had access to intelligence products. The Government of Canada has no departmental unit or agency which could handle the interface between economic and commercially-relevant intelligence and the private sector. Indeed, the highly internationalized structure of Canadian industry would greatly complicate any provision of government-sourced commercial intelligence to commercial enterprises. Much of Canada's large-scale industry consists of subsidiaries of foreign firms which would make the dissemination of commercial intelligence highly problematic. To be sure, there are important Canadian industrial enterprises in the telecommunications, aircraft, power generation and civil engineering sectors, industries that are generally dependent on government sponsored export markets, but there is no evidence that the Canadian intelligence community supplies these firms with commercial intelligence in support of their marketing ventures. It is more likely that products of economic intelligence are sometimes incorporated into the more general advice and counsel offered by government officials to help promote Canadian trade, without necessarily revealing their covert sources.

Canada's crown corporations present a somewhat different issue for the dissemination of economic intelligence. These enterprises, established by the federal and provincial governments, dominate important sectors of the Canadian export economy, including grain exports, energy exports, and export insurance and finance, where commercial intelligence can yield competitive advantages in government-to-government dealings. However, it is questionable whether any intelligence from clandestine sources has actually been shared with crown corporations like the Canadian Wheat Board or Atomic Energy Canada Limited, or whether government negotiators themselves have utilized this information to shape their bargaining positions on such public sector transactions as wheat sales to China or Candu sales to South Korea.

By implication, the collection of economic intelligence injects a competitive element, not to say conflicts of interest or mistrust, into the otherwise cooperative ethos of international intelligence alliances such as UKUSA, which will be described below. UKUSA, which includes Canada, evolved the practice that economic intelligence would be collected primarily by means of SIGINT, but decisions on whether to disseminate this economic intelligence to private companies would be taken by other governmental institutions and not by the intelligence organizations themselves. Thus, for example, Australia's DSD regularly remitted commercially relevant SIGINT to the Office of National Assessments, which in turn disseminated pertinent information to interested government departments and also to private firms (Campbell, 1999). Commercial firms do not in practice actually task government intelligence services for their own purposes nor do they receive intelligence product directly. Doing so could pose operational risks, and is anyway unnecessary since most large-scale enterprises have their own means of securing industrial information.

INTELLIGENCE COLLECTION

The Canadian Security and Intelligence Community deploys several specialized agencies for the collection and processing of intelligence of different types.[2] The principle agencies include CSE for SIGINT and communications security; CSIS for security intelligence and certain elements of foreign intelligence within Canada at the request of the Minister of National Defence; and J2 Division of DND for defence and military intelligence. The RCMP also fulfills certain intelligence collection and investigatory functions, and works in cooperation with CSIS against trans-national crime and in counter-espionage and counter-terrorism.

Communications Security Establishment (CSE)

Most of the foreign intelligence provided to the Canadian government by virtue of Canada's own intelligence collection capabilities derives from SIGINT collected by CSE or otherwise obtained through its international liaison arrangements. CSE collects signals intelligence by means of sophisticated, covert interception technologies designed to intercept terrestrial, microwave, radio, and satellite communications along with other electromagnetic emissions. These intercepts are then processed through technologically advanced computer systems programmed to search for specific telephone numbers, voice recognition patterns, or key words, and to decrypt text. In fulfilment of these foreign intelligence collection functions CSE participates in international SIGINT sharing arrangements with the United States, United Kingdom, Australia and New Zealand within the framework of the UKUSA alliance. CSE is also responsible for providing technical advice and guidance for protecting Canadian government communications and electronic data security. CSE is, arguably, the most secretive entity of the Government of Canada: for decades the very existence of this SIGINT agency was unconfirmed; it had no statutory mandate, at least until recently; and virtually all details of its resources, objectives and operations are still shrouded in official secrecy (Auditor-General, 1996; Rudner, 2001).

CSE operates a central SIGINT collection facility at Leitrim, Ontario, near Ottawa, which is linked to three other fully automated interception stations at Alert in the Northwest Territories., Gander, Newfoundland, and Masset, British Columbia. The personnel operating the interception installations at Canadian Forces Base Leitrim, and who service the remote stations at Alert, Gander and Masset, come from specialized military detachments of the Canad

ian Forces Information Operations Group (CFIOG), working under the overall direction of CSE (Robinson, www).

During the Cold War the Canadian signals intelligence effort was directed primarily at the Soviet Union and its Warsaw Pact allies. Canada' s geographic location provided particularly advantageous situations for intercepting radio-based telecommunications across the northern regions of the USSR and East Asia and the adjacent waters of the Atlantic, Pacific and Arctic oceans (Rudner, 2001). Canadian and allied SIGINT interceptions of in-country Soviet communications helped to acquire information needed to manage bilateral relations and to assess international behaviour and risks, which given the closed, secretive character of the Soviet Union could only be acquired though intelligence means. The monitoring of military, naval, and strategic rocket forces communications across the strategically vital polar region provided distant early warning of the Soviet order of battle and potential first strike capability, intelligence of primary significance during the Cold War for the defence of Canada and North America.

Canadian signals intelligence operations during and after the Cold War may be considered in terms of four types of interception operations: local in-country, external in-country, long-range, and satellite communications, in accordance with the location and technologies deployed. Local interception operations were mounted within Canada to target communications to or from this country on the part of Soviet Bloc diplomatic and consular missions,[3] trade and commercial offices, and organizations and individuals suspected of involvement in espionage or subversion (Cleroux, 1991). Radio transmissions from Soviet research stations in the Arctic were also intercepted, allowing intelligence analysts to monitor their scientific experiments (Bamford, 2001). By the early 1980s Canadian SIGINT was even targeting non-security related economic targets of opportunity as part of operation *Aquarian* aimed at foreign embassies and consulates, even those of friendly or indeed allied countries. CSE intercepts were said to have been instrumental in enabling Canada to out-compete the United States in a US$5 billion wheat sale to China in 1981 (Livesy, 1998). Following the collapse of Communism in Europe and the end of the Cold War, a more variegated and volatile post-Cold War security situation has had a far-reaching impact on Canadian foreign intelligence requirements.

External in-country interception operations targeted communications in foreign countries from Canadian diplomatic posts, using US-supplied technologies. Microwave systems in most countries converge on their capital cities, rendering some of their most sensitive communications traffic vulnerable to embassy-based interception operations. Embassy-based SIGINT stations were also effective for intercepting official car phone communications transmitted by short-range radio. The first such interception operation, *Stephanie*, was mounted from the Canadian embassy in Moscow beginning in the autumn of 1972, and ran for about three years (Frost & Gratton, 1994). A subsequent operation, *Sphinx*, was run in the late 1980s. Other external interception operations were reportedly conducted in Abidjan (operation *Jasmine*), Beijing (*Badger*), Bucharest *(Hollyhock),* Rabat (*Iris*), Kingston, Jamaica (*Egret*), Mexico City (*Cornflower*), New Delhi (*Daisy*), Rome, San Jose, Warsaw and possibly Tokyo. All the intelligence collected by Canadian external-based interceptions was actually remitted to NSA for deciphering and analysis, since at the time Canada lacked a capacity to do this. It was ironic that for the want of cryptanalytical capability Canada was unable to process the take from its own external SIGINT collection efforts, but had to rely on partners for this intelligence product (Robinson, www; Rudner, 2001).

Long-range interceptions targeted communications and electromagnetic emissions abroad from interception facilities in Canada. Later, specialized facilities were installed to also monitor satellite communications links.

Apart from the Soviet bloc, the Canadian SIGINT effort also sometimes targeted the communications of other countries whose foreign policy behavior was considered inimical to Canada, and those whose embassies or representatives were suspected of engaging in illegitimate political activities, inappropriate dealings with Canadian residents, support for subversive or terrorist groups, or illicit arms procurements. After the election of a separatist government in the Province of Quebec, CSE reportedly began monitoring communications traffic between the governments of Quebec and France (Black, 1996; Arnold, 1992). Such operations were ostensibly mounted by CSE itself, some say with support from SIGINT allies in Norway and the United States.

The development of space based technologies since the 1960s led to the deployment of sophisticated satellite systems for intelligence collection. Imagery satellites, for photographic and radar intelligence, were deployed first by the US and later by other countries, including France[4] Le Point, 20 June 1998. See also Jerome Thorell, Frenchelon - France has Nothing to Envy in Echelon , *Echelon Special*, ZDNET, 30 June 2000 [URL: www.zdnet.com][5], Russia, China, India, Israel, and Italy. However, the Americans and French are still the only countries to have developed a capability to intercept communications from space. Whereas Canada does not possess either imagery or SIGINT satellite capabilities of its own, the UKUSA arrangement allowed CSE to share in satellite based SIGINT collection and also to task - within certain parameters - US satellites to respond to specific Canadian foreign intelligence requirements.

The rapid expansion of satellite based telecommunications traffic since the 1970s prompted the UKUSA partners to build a network of six satellite communications (SATCOM) interception stations in strategic locations so as to achieve global coverage. One of these operated under CSE aegis at Leitrim, Ontario, ostensibly targeted on Latin American PanAmSat communications links. To deal with the ensuing surge in raw intelligence collection, CSE undertook a revitalization and enlargement of its intelligence processing capacity and cryptanalytic capabilities. Early in 1985 CSE acquired its first supercomputer for cryptanalysis, a Cray X- MP/11. By the late 1990s there were four satellite dishes operating at Leitrim. Staffing likewise had to be augmented and trained to analyze and disseminate the ensuing intelligence product. CSE staffing grew from around 600 personnel in the late 1970s to some 720 in the mid-1980s, and to about 900 by the end of the decade (Robinson, www; Rudner, 2001).

By the 1990s, extensive refinements to UKUSA satellite interception technologies had made possible a virtually seamless global intelligence collection capability for the various modalities of signals intelligence collection: local in-country, external, HF long distance and space based. This quantum leap forward towards a convergence and meshing of SIGINT technologies reached its zenith in the tightly integrated and networked interception and processing system known as *Echelon*[6] (Campbell, 1999). At the operational heart of this integrated SIGINT processing and networking system is the *Echelon* "Dictionary", a specialized, powerful computer system having the capacity to store a comprehensive database on designated organizations or individuals, including names, topics of interest, addresses, telephone numbers and other criteria for target identification (Bamford, 2001). Highly secret still, the *Echelon* system is able to process and sort through vast flows of telecommunications traffic to or from most parts of the world and identify specifically targeted messaging. The great challenge

confronting CSE and its partners has been the tremendous influx of intercepts which can overwhelm existing capacity to synthesize and analyze raw communications intelligence into readily usable product.

While CSE may not have its own *Echelon* Dictionary computer, according to reports, this networking infrastructure enables Canada to readily access other UKUSA partners' facilities. Available information indicates that each SIGINT partner can only access the *Echelon* system for its own "watch list" and is not obliged to share any of the intelligence gathered with other partners (Bamford, 2001). The reciprocal sharing arrangement under UKUSA gives each partner SIGINT organization virtually automatic access to interception modalities, but not necessarily to particular intelligence products.

In the wake of the 11 September attack, Canadian intelligence reportedly intercepted encrypted communications among international terrorist networks warning of renewed terrorist assaults on the United States (Seper, 2001). This intelligence was forwarded this to the American authorities who subsequently invoked a heightened state of alert. Although publicly credited to CSIS, it seems likely that the interception operation originated with CSE, probably through the *Echelon* network (Simmie, 2001). Under the new counter-terrorism legislation enacted in 2001, Bill C-36, CSE has been empowered, subject to authorization by the Minister of National Defence, to monitor communications to or from Canada specifically for the collection of foreign intelligence.

Canadian Security Intelligence Service (CSIS)

CSIS is a civilian security intelligence agency, created by an Act of Parliament (CSIS Act) in 1984. Historically, the primary concerns of Canadian security intelligence related to Communist subversion and espionage, and to perceived threats of separatist violence in Quebec The Cabinet intelligence directive of 1991 led to a refocusing of CSIS efforts more towards counter-terrorism, economic espionage, weapons of mass destruction, and foreign influenced activities deemed detrimental to the national interests of Canada. In fulfilling its mandate, CSIS investigates, analyzes and advises government departments and agencies on activities which are suspected of constituting threats to Canada's national security.

International terrorism is perceived to be the dominant threat to Canada's domestic security. Canada's open society and presence here of large, identifiable homeland communities from societies in conflict create a distinctly attractive arena for international terrorist networks. Whereas most acts of political violence in Canada have been extensions of foreign conflict, however Canada has itself been targeted for terrorist attack. International terrorist organizations and rogue states have targeted individuals and institutions in this country in order to intimidate adversaries or gain public attention for their cause (Bell, 2001a; Edwards, 2001; Landy, 2001). Al-Qaeda reportedly plotted a bomb attack on Jewish neighbourhoods in Montreal (Matas, 2001). Other Islamicist militants set up Internet sites registered in Canada for recruiting and promoting a violent "jihad" (Bell, 2001d). Efforts to monitor and control such activities in Canada seem to have been impeded by lax immigration, citizenship and passport procedures, as demonstrated by the Ahmed Ressam case (Bell, 2001b).

CSIS legislation allows the Service the targeting authority to investigate the activities of any group, organization or person suspected of constituting a threat to the security of Canada in relation to the stipulated issue, eg. terrorist fund-raising (SIRC, 2000). This targeting authority is governed by policies procedures that control the operational methods and investigatory techniques to be utilized. CSIS also investigates foreign government activities deemed

detrimental to Canadian national interests or public safety, such as interference with ethnic and dissident communities in Canada. There have been instances where foreign operatives, like those of Iran, attempted to intimidate dissidents in this country, threatened ethnic groups, or orchestrated public demonstrations to gain attention for their cause (SIRC, 2000). CSIS operations try to prevent such external homeland issues from becoming domestic security problems or international incidents. By way of responding to emergent terrorist threats, CSIS is taking steps to improve and expand its analytical skills, knowledge resources and investigatory capabilities regarding distant conflict situations in the Middle East, East and Central Europe, Asia and Africa.

Large scale mass movements of people, sometimes involving political, religious or economic refugees, and sometimes combined with the growth of transnational criminal activity, brings with it social, economic, political and, by implication, security challenges. Migrant smuggling has become a lucrative commodity for transnational criminal groups. While the intelligence component of Citizenship and Immigration Canada has the responsibility to forewarn of attempts at illegal migration, CSIS plays a role in the security screening of prospective immigrants and refugee claimants. Staff shortages and work overload has meant that CSIS can take as long as two years to complete these background checks on new arrivals, leaving a chink in the armour of Canada's security. (SIRC 2001). Even when alerts are indicated, the record suggests that the refugee determination process has not worked adequately in checking and excluding suspected terrorist operatives from Canada (Blatchford, 2001).

The Security and Intelligence Community has devoted increased attention to the phenomenon of illicit trans-national fund-raising and money laundering in support of international terrorism. At the Halifax summit of the Group of 8 (G-8) countries commitments were made to combat international terrorism by curbing the misuse of charitable, social and cultural organizations for fund-raising. However, Canada was slow to enact legislation proscribing international terrorist organizations and criminalizing their fund-raising activities (SIRC, 2000). Finally, prompted by the terrorist attacks of 11 September, the Government announced in October 2001 new regulations to block money transfers to terrorist organizations, in anticipation of further changes to the law regarding the suppression of terrorist financing. The intelligence capabilities of the Canada Customs and Revenue Agency are also being reinforced in order to counteract abuses of charitable status for financial resource mobilization by international terrorist networks.

More recently, the anti-globalization violence that accompanied meetings of multilateral trade and financial institutions and regional economic organizations posed radically new challenges for security intelligence in Canada and elsewhere. The violent protests surrounding the Summit of the Americas in Quebec City exemplified this phenomenon. CSIS concern was aroused by the presence and actions of militant extremists from the trans-national anarchist and other radical movements, who melded with a broad spectrum of opponents of globalization (CSIS, 2001). The amorphous and extremely violent character of these protests blurred any distinctions between legitimate dissent, law enforcement and security intelligence (*Financial Times*, 2001). While CSIS insists that it does not investigate lawful dissent or advocacy, security intelligence and law enforcement agencies have had to direct increasing efforts at monitoring protestors, groups and individuals (Pugliese and Bronskill, 2001). In May, 2001, the RCMP set up a new specialized unit, the Public Order Program, to liaise with other police agencies,

exchange intelligence information and strengthen its capacity to control large, combative political demonstrations.

Cyber-based threats to Canada's communications and information infrastructure are among the increasingly complex challenges to critical national infrastructure which CSIS must contend, in conjunction with the Office of Critical Infrastructure Protection and Emergency Preparedness (CSIS, 2000). CSIS identified a looming threat from information warfare waged through "weapons of mass corruption" at the disposal of rogue countries and international terrorist organizations like the Provisional IRA, the Spanish Basque ETA, the Kurdish PKK, and militant Islamicists (Bell, 2001c).

Defence Intelligence (J2)

The institutional centrepiece of Canada's Defence Intelligence capability is the J2 Division at the Department of National Defence (DND). J2, with a staff of approximately 500, is responsible for providing the Canadian Forces (CF) with all-source strategic, military and security intelligence, imagery (in cooperation with the CF Photographic Unit) and counter-intelligence (in conjunction with the CF National Counter Intelligence Unit). Activities include the provision of political, strategic and tactical intelligence to CF commanders, and the deployment of Intelligence, Geomatics and Imagery detachments for CF operations, the dispatch of Intelligence Response Teams to support peacekeeping missions; and the provision of Counter-Intelligence force protection to operational missions. Defence Intelligence products are also shared with other components of Canada's Security and Intelligence community and Government Departments, as well as with selected Allies.

The *Strategy 2020* strategic capability plan for the Canadian Forces (CF) assigns high value to Information and Intelligence capabilities among its "capability goals" (DND, 2000). The future scenarios being contemplated stipulate that the CF must be capable of operating alongside allied or coalition partners in international operations, while retaining an autonomous capability to function domestically. Information and Intelligence capabilities for peace support and other operations other than war must relate to situations of far greater complexity and indeed ambiguity compared to the tradition combat operations for which these systems were designed.

The military intelligence functions of the CF in operational contexts will generally be subordinated to Allied, and especially American, systems. This especially true as regards information and surveillance capabilities, particularly sophisticated sensors, processors, automated analysis tools, and supporting dissemination networks. DND is developing a Canadian Electronic Warfare Command and Control Program, an automated architecture for information processing and distribution designed for interoperability with the US and other allied systems and capable of offering commanders a common understanding of their mission environment.

The experience of peace support operations suggests that the CF military intelligence architecture will also have to interact with and accommodate the information-gathering capabilities and other activities of local authorities and non-governmental organizations. This will require the creation and maintenance of human intelligence (HUMINT) and analytical capabilities as regards regions and conflict situations in which Canada may become involved. As well, the CF will have to continue supporting other Government departments and agencies in security and intelligence-related matters, such as Canadian Forces Information Operations Group support for CSE.

INTERNATIONAL ALLIANCES AND LIAISON

Intelligence alliances are among the most intimate, enduring and secretive of international security arrangements. The Canadian Security and Intelligence community is highly dependent on its alliances and international liaison for access to foreign intelligence sources, in particular, given the absence of a dedicated foreign intelligence service. International partnerships have proven to be especially relevant to SIGINT, where collaboration among allies has been of great value for extending the scope and depth of geographic coverage. Other international arrangements been put in place for sharing intelligence on a more specialized issue-oriented or institutional basis. The architecture of these intelligence alliances has generated significant operational synergies and cost-sharing advantages, however these arrangements have profound implications for Canadian foreign policy and security and defence planning.

The UKUSA Alliance

For more than fifty years, the little-known United Kingdom-United States Security Agreement on communications intelligence cooperation, the UKUSA alliance, has been the keystone of Canadian intelligence policy and its single most important asset (Bamford, 2001; Andrew, 1994; Richelson & Ball, 1985). As early as 1945 Canada's intelligence chiefs were determined that the country's independent SIGINT effort should be enhanced in order to gain a place in post-war cooperation among allies in the realm of communications intelligence (Wark, 1997). Initially, however, the American Communications Intelligence Board would not countenance sharing communications intelligence with Canada except on a 'need to know' basis (Aldrich, 2001).

As the Cold War intensified, however, earlier bilateral arrangements with the US and Great Britain culminated in 1948 in the formation of a closely-knit, plurilateral Anglo-American SIGINT alliance, UKUSA, involving the US, UK, Canada, Australia and New Zealand. The existence of this UKUSA alliance is still an official secret. Its architecture reportedly provided for a geographic division of responsibilities for regional coverage among the five partner countries' SIGINT agencies, coupled with a collaborative arrangement for intelligence collection, processing and product sharing. This robust, tightly networked alliance of SIGINT agencies cooperated in global intelligence targeting, in operational procedures, in transfers of SIGINT technologies, and provided full exchanges of intelligence product. Later, certain other countries were included in a somewhat looser, more limited association as so-called "Third Parties" to UKUSA, usually by virtue of bilateral arrangements with Britain (*e.g.* Sweden) or the US (*e.g.* Norway).(Richelson & Ball, 1984; van Buuren, 2000).

UKUSA is not a single treaty but rather a set of Anglo-American agreements, Memoranda of Understanding and exchanges of letters which have been acceded to also by Canada, Australia and New Zealand (Andrew, 1994; Richelson & Ball, 1985; Bamford, 2001). It has become an underlying principle of UKUSA that the partner countries do not target one another or their respective nationals. As an expression of the intimacy of their cooperation these otherwise highly secretive organizations, both GCHQ and NSA exchanged liaison officers with all their UKUSA counterparts. This asymmetric pattern of liaison exemplified the hub-and-spokes configuration of the UKUSA operations, with the US and, to a lesser degree the UK serving as core contributors and other partners like Canada comprising auxiliaries at the periphery of the global SIGINT effort. This implicit division if labour enables CSE to gain access to a shared global capacity to collect and deliver real-time SIGINT on targeted foreign intelligence targets as tasked by the Government of Canada.

Canada's role in the UKUSA alliance was valued not so much for this country's inherent capabilities in intelligence production, as for the distinct geographic advantage that this country offered by way of SIGINT coverage of the Soviet Union, especially its Arctic and Far Eastern regions, and the adjacent Atlantic, Pacific and Arctic Oceans (Rudner, 2001). This contribution was of great strategic significance to UKUSA during the Cold War. Nevertheless, the alliance mechanism provided Canada with substantially more intelligence product from its allies, and especially from the US, on a far wider array of issue areas, than this country itself generated. Indeed, Canada's lamentable terms of trade in intelligence product was at times deprecated by its UKUSA allies (Aid and Wiebes, 2001). Yet, despite its meager capacity to produce tradable intelligence, Canadian geography sustained its role in this most powerful of international intelligence alliances. This in turn provided Canada's Security and Intelligence community with intimate access to the highest level policy councils of it American and British allies, and with privileged recourse to the most sophisticated technologies for intelligence and defence generally, and to a shared capability for global intelligence coverage as well.

Intelligence for Multilateralism: NATO and UN

The UKUSA connection also had implications for Canada's intelligence role in other international security contexts. The alliance provided the impetus for Canada to further become involved in a tripartite Canada-UK-US (CANUKUS) intelligence grouping within NATO. NATO, as an organization, does not possess an intelligence collection capability of its own, and has only a limited capacity for analysis. Ordinarily, all of NATO's intelligence requirements are met from intelligence products supplied by member countries for the exclusive use of the Alliance itself and for its constituent governments. During the Cold War, the CANUKUS grouping was said to have contributed the bulk of the input into the annual NATO Military Committee assessments of Soviet military power (Urban, 1996). The CANUKUS grouping furnished a preponderant share of NATO's overall intelligence requirements, mostly derived from SIGINT, including CSE product.

Since the end of the Cold War NATO has taken upon itself 'peace support' missions in the Gulf, in Somalia and in the former Yugoslavia. These missions were not only 'out of theater' but also involved NATO in new kinds of operations aimed at conflict prevention, peace-making, peace-keeping, humanitarian aid, peace-enforcement and peace-building (Nomikos, 2000). NATO has recognized that peace support implies a requirement for robust Information and Intelligence capabilities at operational and strategic levels, a task that imposed severe tensions on the traditional principles underpinning the Alliance's intelligence system.

It has been a fundamental principle of NATO intelligence sharing up until now that none of the intelligence supplied to the Alliance can be made available to non-member countries or to any international organization composed of non-member countries (Nomikos, 2000). This principle is also applicable to peace support missions involving NATO in coalition with other countries or international organizations, notwithstanding operational requirements for intelligence sharing (*NATO, Peacekeeping and the UN*, 1994). Indeed, some of the highest value elements of intelligence collected by sophisticated American surveillance technologies are not even shared with other NATO forces on the same Alliance-led peace support missions. However, Canadian Forces reportedly have enjoyed privileged access to this intelligence.

As a result of these tensions and conflicting requirements, the intelligence architecture for NATO-led peace support missions has become compartmentalized into a three tier, differentiated access arrangement. The top tier is restricted to US forces and their most intimate UKUSA allies

who share full access to American intelligence, surveillance and reconnaissance capabilities as well as NATO resources. This includes Canadian Forces. A second tier consists of other NATO allies who may acquire intelligence made available through the Alliance mechanism, but without having access to reserved American-generated products. A third tier is composed of all other countries or international components who are denied access to either NATO or American intelligence resources. This trifurcation of NATO's intelligence architecture militates against effective command and control of peace support operations and humanitarian missions involving coalitions with non-NATO countries, and impeded the availability of tactical and operational intelligence even for Canadian participants.

Although NATO membership and UKUSA connections have benefitted Canada in terms of intelligence access, this country's frequent involvement in peace support operations in coalition with non-NATO/non-UKUSA partners can sometimes place Canadian Forces on the fault lines between the three tiers of Alliance intelligence compartmentalization.

UN peace missions, for their part, were historically ambivalent regarding intelligence requirements (Johnston, 1997; Smith, 1994). In as much as the UN considers itself an essentially neutral, multilateral organization, "intelligence systems" were not countenanced as part of UN mandated peace operations, ostensibly due to their covert, sinister connotations (International Peacekeeping Academy, 1984). So far as the UN was concerned, intelligence was equated with espionage, and therefore considered a betrayal of the "trust, confidence and respect" deemed necessary for effective UN peacekeeping. Reflecting this view, Canadian military doctrine rejected the term "intelligence" as being "negative and covert", insisting instead that peacekeeping operations rely on a more principled access to "information" that was "impartial, trustworthy and overt" (Canadian Forces, 1992).

The operational consequences of this aversion to intelligence has proved to be very problematic for Canadian Forces on UN peace support operations. UN peace support operations in Bosnia in 1992 were impeded by intelligence deficiencies. In the words of General Lewis Mackenzie, commander of UN Forces in Bosnia: "we had absolutely no intelligence" (Nomikos, 2000).

The Report of the Brahimi panel, a review of UN peace-keeping doctrine undertaken at the behest of the Secretary-General and published in August, 2000, recommended that UN peace operations acquire a more robust and realistic mandate to achieve their objectives (United Nations, 2000). As a result the UN established an Information and Strategic Analysis Secretariat within the Department of Political Affairs (United Nations General Assembly, 2000) top collect and manage "strategic information", an acceptable euphemism for intelligence. It remains to be seen whether and how this new found acceptability of Information and Analysis at the strategic policy level will percolate down to the intelligence requirements at the tactical and operational levels of UN peace support missions.

International Liaison and Cooperation

Canada has engaged in bilateral intelligence liaison with many countries and cooperates with certain plurilateral groupings on a functional basis, in relation to specific threats. Canada's intelligence services have working relationships with counterparts in most countries, and formal liaison relations exist with countries with whom there are common security interests (PCO, 2001). International liaison relationships serve to facilitate a bilateral exchange of intelligence information regarding specific security threats among the countries concerned, and these days tend to focus on international terrorism, transnational crime, drug trafficking, money laundering,

financial fraud, people smuggling and the proliferation of weapons of mass destruction. The attacks of 11 September led to a deepening of international cooperation in the intelligence domain, with dozens of countries proceeding to share information and collaborate in operations against suspected terrorists, cells and networks (Woodward, 2001). This intelligence coalition was just as important to the war against global terrorism as the diplomatic and military coalitions.

In Canada's case, much of its intelligence liaison is taken up with immigration matters and visa security screening (SIRC 2001). Of the many bilateral arrangements currently in place, some 44 are considered to be "dormant", i.e. inactive. In establishing liaison relationships the record of the country and agency concerned are assessed and the ensuing arrangements must be compatible with Canadian foreign policy. CSIS recently curtailed the level of exchange activity with two foreign counterparts, in one case due to human rights concerns and in the other due to doubts about that agency's reliability and stability (SIRC 2001).

Canada's dependence on alliance partners and liaison for a very large portion of its foreign intelligence renders these international connections somewhat sensitive and complex. As part of the UKUSA intelligence sharing arrangement, there are allied liaison representatives at the Intelligence Assessment Committee in PCO, exchanging assessment material and sharing insights. Similar procedures are in place in Washington, London, Canberra and Wellington, although the British Joint Intelligence Committee sometimes excludes allied liaison officers from discussions on certain sensitive issues, in particular issues relating to European affairs (Urban, 1996; Rudner, 2002). In the Canadian context, alliance partners not only provide a substantial share of the foreign intelligence input, but furthermore help shape the assessment that inform Canadian foreign and security policy perspectives. About a quarter of Canada's intelligence assessment product derives input from alliance partners, though allied participation tends to be somewhat asymmetric in practice. Typically, the US responds with comment on Canadian assessment material but does not ask for input into their own; the UK gives feedback to Canada and occasionally requests Canadian comment on their own production; Australia rarely requests comment but sometimes provides feedback on Canadian material; New Zealand infrequently shares either assessments or feedback with Canada.

The establishment of constructive liaison relationships has helped to curtail foreign intelligence activities in Canada on the part some countries (SIRC, 2001). Yet, liaison with the intelligence services of even friendly countries is always an ambiguous affair. There is a strong propensity among intelligence services to monitor neutral and even friendly countries, which can render international cooperation somewhat awkward (Aldrich, 2001). As it is said: "There are no friendly secret services, only the secret services of friendly states."

International arrangements for plurilateral cooperation and liaison among intelligence services tend to be highly secretive. The Kilowatt group was formed in the 1970s by Belgium, Canada, France, Germany, Ireland, Israel, Italy, Luxembourg, Netherlands, Norway, Switzerland, Sweden, and UK, to deal with Arab terrorism, alongside the Magnetron group to counter other (non-Arab) terrorist phenomena. These highly secretive groups are backed by integrated data banks on terrorist organizations, operatives, methods and links which facilitate intelligence sharing and liaison among participating countries, and enhance their counter-terrorism capabilities (Friedman & Miller, 1983).

In addition to international liaison, Canada has also provided training programs for intelligence officers from other countries, helping to support, for example, the civilianization and professionalization of intelligence services in Latin American and former Communist countries.

INTELLIGENCE REVIEW AND OVERSIGHT

Canada's intelligence services are subject to two modes of oversight, parliamentary and institutional, or what may be termed "executive accountability" as distinct from "public accountability" (Whitaker, 1991). In principle, Parliamentary oversight is intended to facilitate public accountability for intelligence activities by providing a modicum of policy transparency and financial and operational scrutiny by the House of Commons and Senate of Canada, consistent with the legitimate requirements for operational secrecy or national security. The mechanisms for executive accountability are designed to provide oversight through intra-governmental institutions that evaluate and review the activities of the intelligence services to ensure compliance with policy, performance and statutory requirements. Unlike the United States, there is no legislative scrutiny of the Security and Intelligence Community as a whole in Canada, only of the individual intelligence services, *i.e.* CSE and CSIS.

Like all other departments and agencies of the Government of Canada, the Security and Intelligence Community is accountable to Parliament through their respective Ministers. Since details of intelligence budgets, targeting, international liaison and operations are kept secret from parliament, parliamentary oversight has been constrained by innate weaknesses in the legislative committee system coupled with the unwillingness of government or the intelligence services to respond to scrutiny (Farson, 2000). Neither have the Canadian Parliamentary committees demonstrated the breadth of purview, continuity, or access to sources comparable to their American Congressional counterparts or the British House of Commons Committee on Intelligence and Security.

The role of the Office of the Auditor-General of Canada (OAG) bridges, in some respects, parliamentary and institutional oversight. Whereas the OAG is an independent body reporting directly to Parliament, its mandate relates specifically to bureaucratic management performance and value for money, rather than broader public policy or operational concerns. In 1996, the OAG conducted a first-ever audit of Canada's foreign and security intelligence services (Auditor-General, 1996). That Report disclosed serious deficiencies in the oversight of the foreign intelligence function in particular, in as much as no external or internal review processes were in place to provide systematic assurances to ministers that control and accountability mechanisms are working effectively (until the appointment of a CSE Commissioner in 1996). There has not yet been a second OAG audit of the intelligence community.

Canada's intelligence services are also subject to review by the oversight institutions of government, most notably the Security Intelligence Review Committee (SIRC), the CSIS Inspector General, CSE Commissioner, the Privacy Commissioner, the Human Rights Commission, as well as to the provisions of the Access to Information Act (PCO, 2001). SIRC performs a threefold function: it is charged by the CSIS Act with providing Parliament and the public with an annual review of CSIS' performance of its duties and functions; it serves as a quasi-judicial tribunal with power to investigate complaints against CSIS; and may be tasked to advise on issues under the Human Rights or Citizenship and Immigration Acts. The challenges of reconciling these functions can sometimes be "intractable" (SIRC, 2000).

The Inspector General of CSIS reports to the Solicitor General and functions as an internal auditor to review the operations of the Service and to monitor compliance with ministerial directives and statute. According to the CSIS Act the Inspector General must submit to the Minister an annual Certificate assuring the Minister of this compliance. In the past, tensions between the Inspector General and CSIS Director loomed large and impeded the

performance of the internal review and monitoring functions (Farson, 2000). Indeed, between June 1998 and September 1999 the position of Inspector General was actually left vacant following the resignation of the incumbent. In contravention of the CSIS Act no Certificate was ever issued for 1998-99. The appointment of a replacement Inspector-General, who happened to be the former Executive Director of SIRC, Mr Maurice Archdeacon, was made in July, 1999, and a Certificate was eventually submitted in autumn, 2000.

In 1996, the government moved to create another institutional oversight mechanism by appointing a CSE Commissioner with a mandate to review and report upon CSE's activities with respect to compliance with the law. To date the CSE Commissioner has declined to appear before any Parliamentary Committee to be questioned about the annual reports, the role of that office, or CSE operations. Assurances have been given repeatedly in ministerial pronouncements and in reports of review agencies like the Privacy Commissioner to the effect that Canadian SIGINT operations respect the laws of privacy and do not intentionally target Canadians or monitor their domestic private communications or utilize alliance partnerships to circumvent the law (CSE Commissioner, 2001).

It is indeed inherently difficult to assess the operational performance of intelligence agencies. The Government' s own assessment of the performance and value of its intelligence effort is manifested in its resource allocations to CSE and CSIS, both in terms of budget and staffing. While the precise budgetary appropriations to the two intelligence collection agencies remain classified, it is apparent that both CSE and CSIS underwent sharp cutbacks in expenditures and personnel during the early post-war period. For 2000/01, the disclosed budgets of CSE and CSIS were approximately $106 million and $194 million respectively, expenditure levels that suggest that intelligence fared better than most other federal departments and services in withstanding declining resource commitments. In the immediate aftermath of the terrorist attack on the United States the Government provided an interim increase of almost $47 million to CSE and CSIS to enhance their technical capabilities collect foreign intelligence. $37 million of this was to go to CSE for research and development and to upgrade its technology infrastructure. At the time of writing a debate has commenced within government circles and beyond as to whether Canada should establish a dedicated foreign espionage agency, with CSIS claiming that it already has a mandate and a capability -- given resources -- to operate abroad in the domain of security intelligence. Whatever the outcome of this debate, it seems likely that Canada will be vastly expanding its budgetary commitments for intelligence capacity building for the foreseeable future.

THE CHALLENGES AHEAD

The attacks of 11 September catapulted the intelligence community to the forefront of Canada's war against global terrorism. After decades of decline, the intelligence community is suddenly being given high level policy attention, substantial additional resources - budgetary and personnel - and extended operational authority. In response to the global threat environment, the main intelligence services are undergoing a far-reaching role expansion, while other government departments like Citizenship and Immigration Canada and the Canada Customs and Revenue Agency are significantly expanding their respective intelligence capabilities. As this transformation unfolds, Canada's intelligence community is likely to encounter four elemental challenges to its future capacity to respond to national security requirements: (a) the weak capacity for coordination of Canada's decentralized and diverse Security and Intelligence

Community; (b) the need to reconfigure its strategic approach to intelligence collection as between HUMINT and SIGINT methods; (c) the accommodation of intelligence collection exigencies with the principles of law enforcement, privacy rights and civil liberties; and (d) concerns about international intelligence cooperation and coalition building with new and hitherto unlikely partners. Each of these challenges invokes policy choices that will impact upon the evolving role and effectiveness of Canada's intelligence community.

Up until now, intelligence coordination among the various agencies and departments involved has been the responsibility of the Privy Council Office and was rendered simple, in effect, by the stable, almost predictable adversarial dynamics of Cold War intelligence. The emergence of new and more blatant security threats has resulted in a pluralization of intelligence efforts, which today encompass a wide array of agencies and departments, including such newcomers as the Office of Critical Infrastructure Protection and Emergency Preparedness, Canada Customs and Revenue Agency, Financial Transactions and Reports Analysis Centre along with line departments like Citizenship and Immigration. The existing coordinating arrangement, which works primarily through periodic consultative meetings, is scarcely equipped to ensure policy coherence and overarching operational control over the Security and Intelligence Community as a whole.

Resulting deficiencies in the coordination and exchanges of intelligence information between CSIS, Citizenship and Immigration Canada and the RCMP, for example, have reportedly impeded the identification of suspect refugee claimants and immigrants (Humpheries, 2001). A tighter fusion of the intelligence capabilities of all components of Canada's Security and Intelligence Community is a prerequisite for operational effectiveness. It remains to be seen whether the high-level policy coordination that the new Cabinet Committee on Security is intended to promote at the ministerial level will percolate downward into improved functional coordination at the operational level.

Along with horizontal, inter-departmental coordination the Intelligence Community is faced with a challenge of vertical, client-oriented coordination. Both CSIS and CSE have worked on tailoring their intelligence products to meet the precise requirements of users (so-called "customer relations"). Line departments and agencies expect and demand real-time, customized information resources, so that the value added of intelligence must derive from its timeliness, reliability and relevance. The effectiveness of intelligence is predicated on close interaction between its producers and consumers (Treverton, 2001).

. The development of highly sophisticated technical means of collection was, arguably, the most significant legacy of the Cold War for intelligence. For Canada this legacy reflected itself in the preponderance of resources devoted to technical means of intelligence collection and early warning, notably SIGINT and electronic surveillance. Yet, advances in publicly obtainable communications technology and information security in the late 1990s were threatening to erode the capabilities hitherto available to SIGINT. These technological developments tended to favour communications security over interception, protection over penetration, and encryption over cryptanalysis (Singh, 1999; Bamford, 2001). The ability of CSE and its partner organizations to monitor communications traffic will become all the more problematic as telecommunications systems shift over to high-capacity optical fibre networks which cannot be readily intercepted by current SIGINT technology.

In order for SIGINT to preserve its future effectiveness, massive investment in costly and innovative technologies for interception and cryptanalysis and, indeed, analytical capacity

building will be called for. Canada will have little option other than to look to the UKUSA alliance for the SIGINT technologies necessary for its future foreign intelligence requirements. Indeed, Canada's dependence on its American intelligence connection will likely grow even more acute apropos some of the more sophisticated technical means, such as satellite-based imagery (IMINT).

Were Canada to proceed to create for itself a foreign espionage capability, it will have to develop a vigorous and competent HUMINT potential. The HUMINT challenge will be to recruit and train operatives with the required linguistic and cultural proficiency as well the tradecraft to run agents in such sensitive and hazardous operations. In the war on terrorism intelligence efforts will have to be targeted against relatively small and amorphous cells, elusive networks, obscure organizations and suspect governments over prolonged periods of time (Treverton, 2001). Recent experience discloses that terrorist methods of communication may no longer be vulnerable to SIGINT interception. Intelligence collection will therefore have to concentrate on offensive covert methods for penetrating suspect target groups. Given the high value of the intelligence to be derived, the historical primacy of SIGINT will likely make way to a more balanced fusion with this HUMINT effort to identify, penetrate, monitor and counter the elusive terrorist threat.

A related challenge pertains to the human resource requirements for HUMINT as well as the intelligence analysis and assessment functions. Some coordination with higher educational institutions may be called for in order to ensure that these human resource needs for international and interdisciplinary area studies knowledge and language proficiencies are met.

The intensified involvement of intelligence services in counter-terrorism and with transnational crime risks blurring the boundaries with law enforcement and human rights (Treverton, 2001). The enactment of new and powerful counter-terrorism legislation in Bill C-36 has prompted concerns as to how to sustain an acceptable balance between the requirements of national security and public safety, on the one hand, and privacy rights and civil liberties, on the other. It is pertinent to acknowledge in this regard that Canadian jurisprudence is more protective of privacy rights than many other legal systems, including that of the United States (Palango, 1998). To be sure, the CSE Commissioner has provided a reassurance as regards SIGINT, at least, that Canada does not use its international alliances to circumvent the laws of Canada, or provide allies with communications they could not otherwise legally collect for themselves (CSE Commissioner, 2001). Yet, any transgression of legal prerequisites can jeopardize the gathering of admissible evidence for bringing alleged terrorists or other criminals to justice, thus compromising the role of intelligence in public policy.

Intense public and, indeed, parliamentary concern over the adoption of more formidable anti-terrorist legislation could challenge Canada's Parliament to perform a more vigorous oversight function regarding intelligence matters. The establishment of a House of Commons or joint Parliamentary Standing Committee on Security and Intelligence could undertake a more comprehensive oversight role apropos the Security and Intelligence Community in its entirety than is feasible by the more narrow and limited departmental-focus of existing committees. Indeed, this was recommended by the 1998 report of the Special Senate Committee on Security and Intelligence (Senate, 1998), but was never acted upon. In present circumstances the formation of a more robust mechanism for Parliamentary oversight could help to assuage public concern by providing greater transparency and reassurance about compliance with law and policy, whilst also serving to demystify the intelligence services by facilitating broader public understanding of their role and purpose.

International cooperation in intelligence collection and early warning has always played a pivotal part in Canada's foreign and security intelligence efforts. Certainly the UKUSA alliance has been a most valuable asset. Until recently, there was some concern in Canadian intelligence circles that European security and defence integration might conceivably some day induce Britain to join in a Euro-centric architecture for intelligence cooperation that would decouple the historical trans-Atlantic partnership (Rudner, 2002). A British defection would be fateful for UKUSA, but would furthermore leave Canada singularly dependent on the US for much of the SIGINT that informs its foreign intelligence capability. Historically, the United States had certain reservations about sharing sensitive intelligence products even with its most intimate alliance partners, including Canada (Aid & Wiebes, 2001). It is by no means certain, in these circumstances, that Americans would wish to continue sharing intelligence resources and product so liberally on a purely bilateral basis with a junior partner like Canada.

The war on terrorism has impelled Canada and its allies towards extending the boundaries of international intelligence cooperation to countries with whom such dealings would hitherto have been unthinkable. An urgent requirement for HUMINT sources on Islamic terrorism has created an environment conducive to exchanges of intelligence with governments in the Middle East and Central Asia, many of which are authoritarian or otherwise suspect (Ajami, 2001; Ungoed-Thomas, 2001). Exchanges of intelligence are reportedly taking place even with rogue countries like Iran, Libya, Sudan and Syria, whose security services may have penetrated these networks and have information to trade (Rissen &Weiner, 2001; Rifkind, 2001). In return, countries like Canada may be asked to share sensitive information regarding exiles and opposition groups, or strategic intelligence about third countries (Woodward, 2001). The imperative for intelligence cooperation can sometimes make strange bedfellows; however, in present circumstances, the trading of intelligence with politically disparate, fundamentally adversarial regimes could have profound implications for foreign policy, civil society and human rights in the Western democracies, as well as for regional security and democratic development in the Middle East itself.

The responses to all these challenges on the part of Canada's Security and Intelligence Community will affect its future capabilities and effectiveness. There is some concern in international intelligence circles, which also may be shared by Canadians, that diverting intelligence assets towards purposes for which they was not intrinsically designed, such as law enforcement, can confound and weaken these efforts (Treverton, 2001). Even if Canada chooses to bolster up its capacity to collect foreign intelligence significantly, whether by creating a dedicated espionage agency or by building on CSIS capabilities, this country will probably still have to depend on international cooperation and liaison to access vital intelligence resources. The ultimate challenge for Canada's Security and Intelligence Community will be to develop and sustain both the capacity - through its own capabilities and international cooperation - and the prowess to deal robustly with daunting future security taskings likely to be punctuated by elusive, multifaceted, globalized threats.

REFERENCES

Aid, Matthew & Cees Wiebes. 2001. "Conclusions," Special Issue on Secrets of Signals Intelligence During the Cold War and Beyond, *Intelligene and National Security* 16 (Spring): 313-332.
Ajami, Fouad. 2001."The Sentry's Solitude," *Foreign Affairs* 80:6, 2-16.
Aldrich, Richard. 2001: *The Hidden Hand. Britain, America and Cold War Secret Intelligence* London: John Murray.
Andrew, Christopher. 1994. "The Making of the Anglo-American SIGINT Alliance," in Hayden Peake & Samuel Halperin, eds., *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer*. Washington, DC: NIBC Press.
Arnold, Gary. 1992. "Officials Deny Report of Canada-France Spy Feud," *Ottawa Citizen,* 22 May.
Aryasinha, Ravindra.2001. "Terrorism, the LTTE and the Conflict in Sri Lanka," *Journal of Conflict Seucurity & Development* 1:2, 25-50.
Bamford, James. *2001. Body of Secrets. Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century.* New York: Doubleday.
Bell, Stewart. 2000. Hezbollah Terrorists Favour Stolen Ontario SUVs," *National Post,* 17 October.
Bell, Stewart. 2001a. "Canada Grows as a Target for Terrorists," *National Post,* 18 July.
Bell, Stewart. 2001b. "No Way to Fight Terrorism," *National Post,* 18 July.
Bell, Stewart. 2001c. "Cyber-attacks Threat Canada: CSIS," *National Post,* 18 July.
Bell, Stewart. 2001d. "RCMP Probing 'Jihad' Web Sites, *National Post,* 18 August: A1.
Blatchford, Christie. 2001. "Canada and Terrorism: Programmed to Receive," *National Post*, 24 November, A18-19.
Black, Eldon. 1996. *Direct Intervention. Canada-France Relations 1967-1974,* Ottawa: Carleton University Press)
Campbell, Duncan. 1999. *Interception Capabilities 2000*, the Report to the Director-General for Research of the European Parliament. Brussels: European Parliament, Scientific and Technical Options Assessment program office.
Campbell, Duncan. 2001. "Fight Over Euro-Intelligence Plan," *The Guardian* [UK], 3 July.
Canada, Office of the Auditor-General. *1996. The Canadian Intelligence Community. Control and Assessment,* Ottawa.
Canadian Forces. 1992: *Peacekeeping Operations, 1992,* Ottawa:Canadian Forces Publication 301(3).
Canadian Security Intelligence Service (CSIS). *1995 Public Report and Outlook,* Ottawa.
CSIS. 1997. *1997 Public Report*, Parts 1, 3 URL: www.csis-scrs.gc.ca/eng/publicrp/pub1997e.html
CSIS. 1999. "Trends in Terrorism, Perspectives," *CSIS Report 2000/01,*Ottawa*,* 18 December.
CSIS. 2001. *Public Report 2000,* Ottawa.
Cleroux, Richard. 1991. *Official Secrets,* Toronto: McLelland & Stewart.
Communications Security Establishment (CSE) Commissioner. 2001. *Annual Report 2000-2001* Ottawa: Public Works and Government Services Canada.
Department of National Defence, Directorate of Defence Analysis. 2000. *Strategic Capability Planning for the Canadian Forces,* Ottawa: Department of National Defence.
Farson, Stuart. 2000. "Parliament and its Servants: Their Role in Scrutinizing Canadian Intelligence," *Intelligence and National Security* 15 (Summer): 225-258.

Friedman, Richard & David Miller. 1983. *The Intelligence War. Penetrating the World of Today's Advanced Technology Conflict,* London: Salamander Books.
Frost, Michael & Michel Graton. 1994. *Spyworld. Inside the Canadian and American Intelligence Establishments,* Toronto: Doubleday.
Hager, Nick. 1996. *Secret Power: New Zealand's Role in the International Spy Network,* Nelson, NZ: Craig Potton Publishing.
Herman, Michael. 2001. *Intelligence Services in the Information Age*, London: Frank Cass & Co.
Humpheries, Adrian. 2001. "Caplan Made Promises She Could Not Keep," *National Post*, 3 November.
"How Militants Hijacked the NGO Party," *Financial Times* (London), 12 July.
International Peace Academy. 1984. *Peacekeeper's Handbook,* New York: Pergamon Press
Johnston, Paul. 1997. "No Cloak and Dagger Required: Intelligence Support to UN Peacekeeping," *Intelligence and National Security* 12 (October): 102-112.
Livesey, Bruce. 1998. "Trolling for Secrets - Economic Espionage is the New Niche for Government Spies," *Financial Post* (28 February)
Matas, Robert. 2001. "How Al-Qaeda Hatched Plot to Bomb Heart of Montreal," *Globe and Mail,* 30 November, A1.
National Post. 2001. "Defunding Terrorism," 8 September: A15.
NATO, Peacekeeping, and the UN, Berlin Information Center for Transatlantic Security, Germany, 1994,
Nomikos, John. 2000. *Intelligence Requirements for Peacekeeping Operations*, Research Institute on European and American Studies Working Paper, Athens, Greece
Palango, Paul. 1998. *The Last Guardians,* Toronto: McLelland & Stewart.
Porteous, Samuel. 1995. *Economic/Commercial Interests and Intelligence Services*, CSIS Commentary #59, Ottawa: Canadian Security Intelligence Service.
Porteous, Samuel. 1996. *The Threat from Transnational Crime: An Intelligence Perspective*, CSIS Commentary #70, Ottawa: Canadian Security Intelligence Service.
Privy Council Office. 2001. *The Canadian Security and Intelligence Community. Helping Keep Canada and Canadians Safe and Secure,* Ottawa.
Pugliese, David & Jim Bronskill. 2001. "Mounties Create Unit to Control Public Protest," *National Pos,* 18 August: A2.
Richelson Jeffrey, & Desmond Ball. 1985. *The Ties that Bind: Intelligence Cooperation Between the UKUSA Countries,* London: Allen & Unwin.
Rifkind, Malcolm. 2001. "Why the US Must Rely on Arab Intelligence," *The Times* [London] (8 November).
Rissen, James & Tim Weiner. 2001. "3 New Allies Help CIA in its Fight Against Terror," *New York Times* (30 October).
Robinson, Bill, www: *The Communications Security Establishment: An Unofficial Look Inside Canada's Signals Intelligence Agency* (URL: http://watserv1.uwaterloo.ca/~brobinso/cse.html.
Rudner, Martin. 2001. "Canada's Communications Security Establishment from Cold War to Globalization," *Intelligence and National Security* 16 (Spring): 97-128.
Rudner, Martin. 2002. "Britain Betwixt and Between: UK SIGINT Alliance Strategy Balancing Trans-Atlantic and European Connections," *Intelligence and National Security* [forthcoming]
Sachs, Susan.2001. "Merger Spread al-Qaeda Tentacles," *New York Times* (21 November)

Senate of Canada. 1998. Report of the Special Senate Committee on Security and Intelligence, William Kelley, Chairman, Ottawa: Senate of Canada.
Security Intelligence Review Committee (SIRC). 2000. *SIRC Report 1999-2000*. Ottawa: SIRC.
SIRC. 2001.SIRC *Report 2000-2001*. Ottawa: SIRC
Soloman, John. 2001. "Authorities Identify Six Terror Centers in US," *Jerusalem Post* (18 November)
Seper, Jerry. 2001. "FBI Alert Based on Coded Message," *Washington Times* (1 November).
Simmie, Scott. 2001. "Why Spy Agency Had a Key Role in Terror Alert?" *Toronto Star* (1 November).
Singh, Simon. 1999. *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography,* London: Anchor.
Smith, Hugh. 1994. "Intelligence and UN Peacekeeping," *Survival* 36 (Autumn): 174-190.
United Nations. 2000. *Report of the panel on UN Peace Operations*, A/55/305 - S/2000 801 (21 August)
Smyth, Julie. 2001. "All Foreign Students Face Tougher Scrutiny," *National Post* (22 September).
Treverton, Gregory. 2001. "Intelligence Crisis," *Government Executive Magazine* (1 November); URL: www.GovExec.com
Ungoed-Thomas, Jon. 2001. "Beating the Terrorists: Egypt Used Torture to Crack Network," *Sunday Times* (London), 25 November.
United Nations General Assembly. 2000. *Resource Requirements for the Implementation of the Report of the Panel on UN Peace Operations. Report of the Secretary-General.* A/55/507 (27 October)
Urban, Mark. 1996. *UK Eyes Alpha,* London: Faber & Faber.
van Buuren, Jelle. 2000. *Making Up the Rules: Interceptions versus Privacy,* Amsterdam: Buro Jansen & Jannsen Stichtung Eurowatch.
Wark, Wesley. 1997. "Cryptographic Innocence: The Origins of Signals Intelligence in Canada in the Second World War," *Journal of Contemporary History* 22: 639-665.
Whitaker, Reg. 1991. "The Politics of Security Intelligence Policy-making in Canada: 1970-84," *Intelligence and National* Security 6:4 (October): 649-668.
Woodward, Bob. 2001. "50 Countries Detain 360 Suspect at CIA's Behest," *Washington Post* (22 November), A01.

ENDNOTES

[1] Members of the Cabinet Committee on Security included John Manley (Foreign Affairs), chair; Elinor Caplan (Citizenship and Immigration), Herb Grey (Deputy Prime Minister), Paul Martin (Finance), Art Eggleton (National Defence), David Collenette (Transport), Martin Couchon (National Revenue), Lawrence MacAulay (Solicitor General), Anne McLellan (Justice), and Stéphane Dion (Intergovernmental Affairs).

[2] *Canadian Security and Intelligence Community*, pp. 6-9.

[3]The Soviets returned the compliment by way of surreptitiously installing interception facilities in KGB residencies in Ottawa and Montreal to monitor Canadian communications traffic. Moreover, a KGB post in New York was able to intercept communications between the Canadian permanent mission to the United Nations and Department of External Affairs.

[4] France launched its *Helios-1A*, a photo-imaging (IMINT) satellite, in 1995, however it was later disclosed that its carried piggyback an experimental *Ceris* (Characterisation de l Environment Radio-electrique par un Instrument Spatial Embarque) small interception package said to be capable of monitoring satellite communication relays.

[5]

[6] *Echelon* may have been a codeword for this interception program, so that it is possible that this codeword has been discarded and replaced with another, as often happens when classified intelligence operations have been compromised by publicity.