CANADA'S COMMUNICATIONS SECURITY ESTABLISHMENT: FROM COLD WAR TO GLOBALISATION

Martin Rudner

OCCASIONAL PAPER
Nº 22 – 2000

CANADA'S COMMUNICATION SECURITY ESTABLISHMENT: FROM COLD WAR TO GLOBALISATION

Martin Rudner

OCCASIONAL PAPER
Nº 22 – 2000

The Norman Paterson School of International Affairs
Carleton University
1125 Colonel By Drive
Ottawa, Ontario
K1S 5B6
Telephone: 613-520-6655
Fax: 613-520-2889
www.carleton.ca/npsia

This series is published by the Centre for Security and Defence Studies at the School and supported by a grant from the Security Defence Forum of the Department of National Defence.

TABLE OF CONTENTS

ABSTRACT

The Communications Security Establishment (CSE) is Canada's largest, best funded and most highly secretive intelligence agency, and is the main provider of foreign intelligence to the Canadian government. CSE collects, analyses and reports on signals intelligence (SIGINT) derived from interceptions of foreign electronic communications, radio, radar, telemetry, and other electromagnetic emissions. In fulfilment of its foreign intelligence function, CSE collaborates closely in a special SIGINT sharing arrangement with the United States, United Kingdom, Australia and New Zealand known as UKUSA. CSE is also responsible for providing technical advice and guidance for protecting Canadian government communications and electronic data security.

The present study reviews the structure of authority and control over CSE within the Canadian intelligence community. It traces its origins back to the early post-war Communications Branch of the National Research Council, and examines its subsequent evolution during the Cold War. A survey of CSE operations during the Cold War covers local interceptions of adversarial diplomatic and clandestine communications, in-country intercepts from Canadian diplomatic posts abroad, and long-distance radio and satellite communications interceptions from listening posts in Canada. Particular attention is given to CSE's role in the UKUSA alliance and its *Echelon* sharing arrangement.

After the end of the Cold War, the Government of Canada issued, for the first time in 1991, a directive setting out its priority requirements for foreign intelligence collection. Signals intelligence has come to play a significant role in addressing these priority requirements, including foreign security threats, international terrorism, ethnic and religious conflict, proliferation of weapons of mass destruction, illegal migration, transnational organised crime, and economic intelligence. Today, economic intelligence presents a major conundrum for CSE and for its relationships with erstwhile partners in UKUSA and other nominally friendly countries.

Current trends in SIGINT imply two major challenges for CSE's future capability to perform its signals intelligence collection and processing

functions. The first of these challenges stems from ongoing trends in communications technology which tend to favour communications security over penetration, protection over interception. A second set of challenges arises from prospective changes in the dynamics of UKUSA once competition outstrips co-operation in the emergent globalised agenda for economic intelligence collection. Canada depends on CSE to develop its capabilities and international linkages in a way that safeguards its future capacity to respond to Canadian foreign intelligence requirements in an increasingly predatory international environment.

ABBREVIATIONS

BRUSA	British-US Agreement
CANUSA	Canada-US Communications Intelligence Agreement
CBNRC	Communications Branch of the National Research Council
CFIOG	Canadian Forces Information Operations Group
CJIC	Canadian Joint Intelligence Commitment
COMINT	Communications and Intelligence
CRIM	Centre de recherche informatique de Montréal
CSE	Communications and Security Establishment
CSIS	Canadian Security and Intelligence Service
CSO	Commonwealth SIGINT Organisation
DND	Department of National Defence
DSD	Defence Signals Directorate
GC&CS	Government Code and Cipher School
GCHQ	Government Communications Headquarters
GCSB	Government Communications Security Bureau
HF	High Frequency
HF-DF	High Frequency Direction Finding
ILETS	International Law Enforcement Telecommunications Seminar
Intelsat	International Telecommunications Satellite Organisation
ITS	Information Technology Security
NSA	National Security Agency
PCO	Privy Council Office
SIGINT	Signals Intelligence
UKUSA	SIGNET sharing alliance of the United States, United Kingdom, Australia, New Zealand and Canada

CANADA'S COMMUNICATION SECURITY ESTABLISHMENT: FROM COLD WAR TO GLOBALISATION

Martin Rudner

INTRODUCTION

The Communications Security Establishment (CSE) is Canada's largest and costliest intelligence organisation and the main provider of foreign intelligence to the Canadian government.[1] It is, arguably, also the most secretive component of the Government of Canada. For decades the very existence of CSE was unconfirmed, it has no statutory mandate, and virtually all details of its resources, objectives and operations are still shrouded in official secrecy.[2] What is known is that CSE collects, analyses and reports on signals intelligence (referred to as SIGINT) derived from interceptions of foreign electronic communications, radio, radar, telemetry, and other electromagnetic emissions. In fulfilment of these foreign intelligence functions, CSE participates in international collaboration and exchanges as part of a special SIGINT sharing arrangement with the United States, United Kingdom, Australia and New Zealand. CSE is also responsible for providing technical advice and guidance for protecting Canadian government communications and electronic data security.

CSE is a civilian agency of Canada's Department of National Defence (DND). Ministerial responsibility for CSE is vested in the Minister of National Defence; however, in a unique bifurcation of executive authority, administrative and operational controls are divided between DND and the Privy Council Office (PCO), the federal government's central agency, headed by the Prime Minister. Administrative and financial matters are under the control of DND, through the Deputy Minister of National Defence, its most senior official, whereas policy and operational controls over CSE are exercised by the Deputy Secretary, Security and Intelligence in PCO. At the policy level, the direction and co-ordination of Canada's intelligence effort

involves a complex web of PCO secretariats and inter-departmental committees.[3]
At the operational level, the actual staffing of Canada's SIGINT interception land sites is undertaken not by CSE as such, but by specialised military detachments of the Canadian Forces Information Operations Group (CFIOG), working under the overall direction of CSE. CFIOG deploys about 1000 personnel, mainly military Communications Research Operators (known colloquially as "291ers"), at Canadian Forces Base Leitrim, who also service the remote stations at Alert, Gander and Masset. An exchange arrangement with the United States has some 25 291ers posted to US Navy stations in California, Hawaii and Texas, while a similar number of American personnel are attached to the Leitrim facility.[4]

During the Cold War the Canadian signals intelligence effort was directed primarily at the Soviet Union and its Warsaw Pact allies. That lent Canada's foreign intelligence requirements a certain stability and predictability.[5] Following the collapse of Communism in Europe and the end of the Cold War, however, CSE found itself impelled to alter the scope and direction of its activities in response to shifting perceptions of the threat environment confronting Canada. A more variegated and volatile security situation had a far-reaching impact on Canadian foreign intelligence requirements. Thus, in 1991, for the first time ever, the federal Cabinet issued a directive on foreign intelligence priorities.[6]

The study that follows traces the historical evolution of CSE in performing its signals intelligence functions from the Cold War to this more diverse and globalised security agenda. Given the sensitivity of SIGINT issues, this study relies on open sources.

THE BEGINNINGS OF CANADIAN SIGINT

Canada has never had a consolidated, dedicated foreign intelligence service, unlike most of its allies. Historically, Canadian requirements for foreign intelligence have been addressed through an array of functionally differentiated agencies, most of which were linked to international intelligence sharing arrangements. Canada's involvement in SIGINT began prior to the Second World War, when the Royal Canadian Navy put in place

a monitoring station on the West Coast to supply raw intercepts to the British Admiralty. During the war the army, navy and airfare set up their own respective signals intelligence units in collaboration with their British counterparts.[7] These separate SIGINT units were later combined into a so-called "Joint Discrimination Unit." Meanwhile a civilian entity, styled the "Examination Unit", had been established in 1941 to provide communications intelligence and cryptanalysis, primarily of diplomatic traffic, for the Department of External Affairs (as it was then). In April, 1946, Prime Minister MacKenzie King approved the creation of a peacetime communications intelligence organisation, and in September of that year the existing military and civilian units were merged to become the Communications Branch of the National Research Council (CBNRC).[8] In 1975 the functions of CBNRC were relocated in their entirety to DND, and reconstituted as the Communications Security Establishment.

No statutory framework for CSE (or its predecessor) was ever put in place. In fact, for virtually all this period the very existence of a Canadian signals intelligence capability was itself an official secret.

While the decision to create a peacetime Canadian SIGINT capability preceded the onset of the Cold War, the looming confrontation with an expansionist Soviet Union gave a powerful impetus to this incipient foreign intelligence initiative. As it happened, a coincidence of events around the pivotal years 1945-1949 underscored the strategic value of signals intelligence in the Cold War context. In 1945, a cipher clerk in the USSR embassy in Ottawa, Igor Gouzenko, defected, bringing with him documentary evidence of a Soviet espionage network.[9] Although there is nothing to indicate that the Gouzenko defection impacted directly on Canadian SIGINT operations, the accompanying cipher material itself underscored the potential role for signals intelligence in the defence of Canadian and allied security.[10] Meanwhile, in 1946, US code breakers succeeded in deciphering previously intercepted Soviet KGB signals. This operation, code named *Venona*, paved the way for future SIGINT attacks on Soviet diplomatic, military, and intelligence communications.[11] In so far as just knowing the capabilities of communications intelligence can suffice to give warning of target vulnerability, these SIGINT organisations, technologies and operations were generally treated as matters of utmost secrecy.

By then, the senior echelons of the Canadian foreign policy and defence establishment would have become aware of the wartime contributions of *Ultra* and *Magic*, the British and American SIGINT breakthroughs against German and Japanese diplomatic and military communications, respectively.[12] They certainly knew of the ongoing British and American initiatives to develop new modalities for post-war co-operation in communications intelligence. Early on, in October 1945, the British SIGINT organisation, then styled as the Government Code and Cipher School (GC&CS), predecessor of what became in 1946 the Government Communications Headquarters (GCHQ), approached the Canadian authorities to solicit their participation in a combined Anglo-American communications intelligence initiative that would involve a complete sharing of intercepts. Aware that they could not achieve global SIGINT coverage by themselves, the British sought to divide the world into tripartite spheres of co-operation, but asked that Canada permit Britain to represent its interests in negotiations with the United States. It is noteworthy that, at the time, GC&CS conceived of the tripartite agreement as involving just military and clandestine radio traffic but not diplomatic interceptions. The Canadian Joint Intelligence Committee (CJIC) agreed to co-operate and mandated Britain to negotiate with the Americans on Canada's behalf.[13] In March 1946, an British-US Agreement (BRUSA) was concluded on communications intelligence sharing, which also embraced Canada.[14]

Prior to the 1960s, most international (and long-distance domestic) telecommunications traffic everywhere in the world was carried by high frequency (HF) radio networks. This HF infrastructure served for telephones and telegraph, and diplomatic and military messaging. Since HF radio signals achieve their long range by bouncing between the ionosphere and the earth's surface, they are vulnerable to interception as well as reception. HF radio signals can be readily intercepted with specialised antennae which can simultaneously monitor as many frequencies from as many bearings as may be desired, requiring only a suitable parcel of land in, ideally, a 'quiet' radio environment. Canada's geographic location provided particularly advantageous situations for intercepting HF communications across the northern regions of the USSR and East Asia and the adjacent waters of the Atlantic, Pacific and Arctic oceans.

After the Second World War, Canada, like Britain and the United States, shut down most of the SIGINT listening posts that had been set up in wartime. While the Leitrim site near Ottawa was kept operational, most other Canadian interception facilities and Royal Canadian Navy radio intercept and high-frequency direction-finding (HF-DF) stations were closed or returned to the Department of Transport.

Prompted by the BRUSA agreement, from 1946 a network of interception facilities was set up across Canada to cover gaps in the tripartite arrangement with Britain and the United States. Existing facilities at Leitrim, Coverdale (New Brunswick), and Prince Rupert (British Columbia) were expanded, and new intercept sites were established at Whitehorse in the Yukon, Churchill in northern Manitoba, and Lander, near Victoria (British Columbia). The Whitehorse facility, activated in 1948, intercepted Soviet and other Asian radio traffic; Churchill, opened the same year, copied Soviet radio traffic across the Arctic; and Ladner provided coverage of the Soviet Far East.[15] By the 1950s CBNRC was monitoring Soviet air force and air defence communications across the northern USSR from ten small radio intercept stations operated by the Royal Canadian Navy (Aklavik, Churchill, Coverdale, Frobisher Bay, Gander, Masset), Army Corps of Signals (Alert, Ladner, Leitrim) and Royal Canadian Air Force (Whitehorse).[16] In addition, a small network of HF-DF stations was created out of reactivated wartime posts and new naval installations at Aklavik (Northwest Territories), Masset (British Columbia) and Coverdale. These HF-DF stations were fully integrated into the Atlantic and Pacific HF-DF networks of the US Naval Security Group, while communications intelligence was channelled through CBNRC.

Building upon the tripartite arrangement under the 1946 BRUSA Agreement, a Canada-US Communications Intelligence Agreement (CANUSA) was concluded in May 1948, which, *inter alia*, established parameters for bilateral exchanges of communications intelligence albeit on a rather more limited basis than did the BRUSA arrangement. Be that as it may, this Agreement provided the impetus for Canada to further extend its involvement in alliance SIGINT activities. By the late 1940s, Canada had emerged as a modest but important source of strategically valuable signals intelligence on the Soviet Union and East Asia.

Canada's collaboration with allied SIGINT efforts, which was subsequently expanded into the wider ranging UKUSA alliance (see below), was valued not so much for this country's inherent capabilities in SIGINT or its contributions to intelligence production generally, as for its geographic advantage in providing communications intelligence coverage of the Soviet Union, especially its Arctic and Far Eastern regions. Indeed, Canada's SIGINT allies would have cause to lament Canada's meagre capacity to offer exchanges of intelligence product.[17] Nevertheless, Canadian geography made up for the otherwise lamentable "terms of trade." By November 1957, CBNRC had given up its attempts at machine cryptanalysis, reducing Canada's role to that of a mere supplier of raw intercepts to its more highly capable, better equipped SIGINT allies.

CANADA'S SIGINT COLLECTION EFFORT

Up to the present, most of the foreign intelligence provided to the Canadian government by virtue of Canada's own intelligence collection capabilities derives from signals intelligence provided by CSE. Canadian SIGINT operations collect 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.

Canada also has access to SIGINT collected by its allies in the UKUSA signals intelligence alliance (see below). This unique alliance links Canada's CSE to the United States, through its National Security Agency (NSA); the United Kingdom, through GCHQ; Australia, through its Defence Signals Directorate (DSD); and New Zealand, through the Government Communications Security Bureau (GCSB). The UKUSA alliance provides CSE with a shared global capacity to collect and deliver real-time SIGINT intercepts on targeted objectives to selected clients within the Government of Canada.

The clandestine and broadly intrusive function of SIGINT has had important implications for political control and accountability, oversight and legal

compliance relating to the privacy of Canadians. Ultimate political control over intelligence in the Canadian parliamentary system is vested in the Prime Minister. As head of government, the Prime Minister bears overall responsibility for Canada's national security and the safeguarding of the country's territorial integrity.

Parliament has traditionally played a very limited role in regard to foreign intelligence generally since most detailed information on budgets, operations and the performance of the organisations concerned, including CSE, must necessarily remain classified. However, along with all other Canadian government departments and agencies, CSE and other components of the intelligence community are subject to scrutiny and review by the Auditor-General of Canada, the Canadian Human Rights Commission, the Privacy Commissioner, and the Information Commissioner, as well as the courts. In 1996, the government took a step towards creating a more public accountability framework for CSE by appointing a CSE Commissioner with a mandate to review and report upon its activities in order to determine their compliance with the law. Assurances have been given repeatedly in ministerial pronouncements and in reports of review agencies like the Privacy Commissioner and CSE 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. Nevertheless, there is some deliberate ambiguity as to the extent to which interceptions of foreign targets may incidentally capture communications to or from Canadians.

The methods utilised to intercept targeted local communications are obviously highly sensitive. There are several ways in which local in-country interception operations could have been mounted. It is noteworthy that CSE shared some of the technologies of its UKUSA partner organisations that enabled them to surreptitiously intercept telephonic or digital communications, sift them for messages to or from targeted individuals or organisations, and decrypt the enciphered content.

Cryptanalysis represented a vital part of Canada's early SIGINT collection effort. At the outset, CBNRC provided the mathematical and cryptological skills to decipher intercepted Soviet bloc communications. However, by the late 1950s, this cryptanalytical effort had to be mostly abandoned.[18]

Historians claim that no Soviet diplomatic communications were ever decrypted after *Venona* because KGB penetrations of NSA and GCHQ thwarted subsequent code breaking efforts.[19]

Over the next two decades Canadian signals intelligence was but minimally involved in serious cryptanalysis. What was done was mostly undertaken manually, as few computer resources were deployed in Canada's SIGINT effort. It was only in the early 1980s that one of CSE's IBM 370 mainframes was made available for cryptanalysis, even though NSA was reportedly doubtful whether this computer could generate results. Nevertheless, CSE was now able to break into certain cipher keys that yielded up intelligence to Canadian requirements. Yet, by the time this system achieved a minimal capacity for code breaking, around spring 1981, CSE cryptanalysts were already acknowledging that more powerful computational technologies would be required for operational effectiveness.[20]

COLD WAR SIGINT OPERATIONS

Canadian signals intelligence operations during and after the Cold War may be considered in terms of four types of interception, in accordance with the location and technologies deployed. Local in-country interception operations were mounted within Canada, targeting communications to or from this country. External interception operations targeted communications in foreign countries from Canadian diplomatic posts. Long-range operations targeted communications and electromagnetic emissions abroad from interception facilities in Canada. Later, specialised facilities were installed to also monitor satellite communications links. The primary targets for each of these types of interception during the Cold War were the diplomatic, military and espionage communications of Soviet Bloc countries. Other countries communications were also sometimes targeted.

Local SIGINT operations mounted within Canada during the Cold War targeted mainly the Soviet Bloc diplomatic and consular missions, trade and commercial offices, and organisations and individuals suspected of involvement in espionage or subversion.[21] Canadians were also intercepting the radio transmissions from Soviet research stations in the Arctic, allowing intelligence analysts to monitor their scientific experiments.[22] No official

confirmation of these sensitive operations was ever forthcoming. A 1956 operation (*Dew Worm*) to secrete listening devices in the Soviet embassy in Ottawa was a failure, as was another attempt to penetrate the Polish consulate in Montreal (Operation *Satyr*).[23] The Soviets returned the compliment by way of surreptitiously installing radio-intercept posts in their KGB residencies in Ottawa and Montreal to monitor Canadian communications. Moreover, the KGB radio-intercept post in New York succeeded in intercepting communications traffic between the Canadian permanent mission to the United Nations and Department of External Affairs.[24]

In parallel with these local and external operations Canadian signals intelligence also undertook long-distance SIGINT intercepts from interception stations in Canada. Long-distance HF radio intercepts enabled Canada and its allies to eavesdrop on internal Soviet (and other Warsaw Pact) military, naval, rocket force and air force communications networks across the Arctic. These Soviet Bloc armed forces HF radio networks were generally less well protected than political-level and diplomatic communications, and could be intercepted and processed with contemporary technologies. SIGINT interceptions of HF communications played a key role in the strategically vital polar theatre by way of providing 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.

By the mid-1970s, however, the USSR seemed better able to effectively protect its high-level communications against interception.[25] By then Canadian SIGINT operations were also targeting other perceived threats to Canada's national security and territorial integrity. Among the countries now targeted were those whose foreign policy behaviour was considered inimical to Canada and its allies, 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. With the election of a separatist government in the Province of Quebec, CSE allegedly began monitoring communications traffic between the governments of Quebec and France, according to disclosures by a disaffected former employee.[26] Such operations were ostensibly mounted by CSE itself, some say with support from SIGINT allies in Norway and the United States.

Canadian and allied SIGINT interceptions of in-country Soviet communications helped to fill the information void in these otherwise closed, secretive, unfriendly regimes. Information needed simply to manage bilateral relations, or to assess international behaviour and risks, which in other societies would have been open source, could only be acquired in the context of Soviet secretiveness by intelligence means. SIGINT interceptions of local communications was one of the most effective, least risky, means of penetrating the iron curtain of secrecy. Soviet countermeasures were deployed in the 1970s to frustrate SIGINT operations run from the US Embassy. It was suspected that the electromagnetic radiation may have caused the American ambassador to become ill with leukaemia, but this fear was later allayed.[27] There is no indication that any Canadians were affected by countermeasures against the listening post in the Canadian Embassy.

During the 1970s CSE, acting at behest of NSA, began mounting external interception operations from Canadian diplomatic posts abroad in an operation code named *Pilgrim*. 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. External communications interceptions provided, at the time, a unique aperture into in-country telecommunications. State-of-the art communications monitoring and processing equipment was supplied by NSA, which also trained Canadian personnel and guided the targeting.

This equipment, and the personnel, were surreptitiously located in certain Canadian embassies and consulates. 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.[28] A subsequent operation, *Sphinx*, was run in the late 1980s. The first permanent intercept site was reportedly established in 1983 at the Canadian High Commission in New Delhi, as operation *Daisy*.[29] Among the other capital cities where Canada is said to have run external SIGINT collection operations from diplomatic or consular posts were Abidjan (*Jasmine*), Beijing (*Badger*), Bucharest *(Hollyhock*), Rabat (*Iris*), Kingston, Jamaica (*Egret*), Mexico City (*Cornflower*), Rome, San Jose (Costa Rica), Warsaw and possibly Tokyo. All the intelligence collected by Canadian embassy-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 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.

On one occasion at least an external interception operation was reportedly mounted in an allied country at the invitation of that government. Thus, on the eve of the British general election of 1983, GCHQ was alleged to have conveyed a personal request from Prime Minister Margaret Thatcher for Canadian SIGINT assistance in monitoring communications of two of her cabinet ministers ostensibly "to find out not what they were saying, but what they were thinking."[30] CSE involvement was sought due to the extraordinary political sensitivity of the operation, which made it inappropriate for GCHQ itself to undertake. An interception facility was set up at the Canadian High Commission in London and the "take" was delivered to GCHQ. That such an ultra-sensitive operation was entrusted to CSE was testimony to the tight association and close confidences shared by the British and Canadian SIGINT organisations, which can sometimes transcend the confines of national sensibilities.

In 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.[31]

Although the NSA partially funded the modernisation of Canadian communications interception facilities in the 1960s, the number of stations was reduced to just six by the early 1970s. Frobisher Bay, Whitehorse, Churchill, Coverdale and Ladner were all closed down. A new station was activated in Inuvik (to replace Aklavik, closed in 1961), and a naval HF-DF station was opened in Bermuda in 1963. Following the transfer of SIGINT responsibilities to CSE in 1975, a complex of specialised SIGINT antennae and processing stations was constructed at Leitrim, Alert, Gander, Whitehorse (now closed) and Masset, staffed with military personnel from what is today the Canadian Forces Information Operations Group.[32] By the

late 1990s the interception stations at Alert, Gander and Masset were fully automated and would henceforward be remotely controlled from the central CSE collection facility at Leitrim.

CANADA AND THE UKUSA AGREEMENT

Canadian involvement in an international SIGINT alliance structure commenced in stages between 1946 and 1948 with separate arrangements with Great Britain and the United States, and culminated in an expanded five-power globally-capable architecture for the sharing of technological capabilities and intelligence product. After Canada was included in the 1946 BRUSA Agreement, albeit as an affiliate of the Britain, GCHQ sought to achieve further synergy and intelligence connectivity by mobilising the SIGINT efforts of the self-governing Dominions (as they were then), under its own leadership, of course. During the winter of 1946-47 the British convened a conference of the Dominions' signals intelligence services with the aim of creating a Commonwealth SIGINT organisation headed by GCHQ and having a global interception capability. Although this objective was too ambitious for the time, the conference did succeed in nurturing the development of close, even intimate working relationships among the SIGINT organisations of the UK, Australia and Canada, in particular.

This British attempt to mobilise dominion support for an 'Old' Commonwealth SIGINT network coincided with an acute crisis in Anglo-American intelligence co-operation, prompted by the post-war Labour Government's controversial sale of jet engines (and, as alleged at the time, jet aircraft) to the Soviet Union. Furious at what they saw to be a betrayal of Western interests, the Americans reacted by placing intelligence co-operation "under review" and stopping any further disclosures of intelligence "sources," "methods of acquisition," and "information pertaining to cryptography and cryptographic devices" - all the essentials of communications intelligence sharing.[33] The resulting freeze no doubt reinforced Britain's desire to create an alternative, Dominions-based arrangement for SIGINT co-operation. Around the same time, in early 1948, the United States moved swiftly, to avoid being outflanked, to negotiate separate bilateral communications intelligence co-operation agreements with Canada and Australia. Thus, Canada found itself entangled by circumstances in competing SIGINT

alliances with contending allies: the British-inspired Commonwealth SIGINT Organisation (CSO) Agreement of 1947 and the Canadian-US Communications Intelligence Agreement (CANUSA) of 1948. In any event, faced with a deteriorating Cold War situation in Europe, the British and Americans resolved their differences by April 1948, paving the way to the signing in June of the UK-USA Security Agreement (UKUSA) on communications intelligence co-operation, the UKUSA alliance.

Informed sources maintain that UKUSA is not a single treaty document 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.[34] Details of these agreements remain highly classified. This framework agreement created a tight, resilient collaborative arrangement between the First Party, the American NSA, and the Second Parties, the SIGINT agencies of Great Britain, Canada, Australia and New Zealand, for co-operation in the sharing of SIGINT technologies, in targeting and operational matters, and in exchanges of foreign intelligence collection.[35] It became an underlying principle of UKUSA that the partner countries did not target one another or their respective nationals.[36] As an expression of the intimacy of their co-operation, CSE (and its Australian and New Zealand counterparts) exchange liaison officers with the otherwise highly secretive SIGINT organisations of the United States (NSA) and Great Britain (GCHQ). This pattern of liaison exemplifies the hub-and-spokes configuration of the UKUSA relationship. Be that as it may, it is clear that most of Canada's foreign intelligence collection activities have taken place within the collaborative SIGINT framework of UKUSA.

The UKUSA connection has had implications for Canada's intelligence role in other international security contexts. Thus, as a partner in UKUSA, Canada was likewise involved in a so-called CANUKUS intelligence grouping within NATO. This tripartite Canada-UK-US intelligence grouping was said to have contributed the bulk of the input into the annual NATO Military Committee assessments of Soviet military power.[37] Other than German intelligence, which provided particular knowledge of Eastern Germany, CANUKUS furnished a preponderant share of NATO's intelligence requirements. Most of this joint intelligence input was derived from SIGINT, including CSE product.

SATELLITE COMMUNICATIONS AND ECHELON

The inauguration of the space age in communications after the 1960s was to greatly expand global telecommunications traffic whilst engendering an enhanced role for UKUSA in signals intelligence (SIGINT). The development of space based technologies has served both to facilitate global telecommunications and, conversely, to intercept these communications from space itself and on land. Space-based SIGINT satellites and their processing facilities are exceptionally costly; the latest renditions cost to the order of US$1 billion apiece. Since 1968 at least three classes of SIGINT satellites (*Canyon*; *Rhyolite/Aquacade*/*Magnum/Orion*; *Jumpseat/Trumpet*) as well as several classes of dedicated COMINT satellites (*Chalet/Vortex/Mercury*) have been launched by the United States, the only country to have deployed space technologies for the interception of communications. While particulars about American SIGINT satellites launched after 1990 remain classified, the apparent expansion of the relevant ground centres associated with these satellites seems to indicate that space-based collection systems have grown in significance. Canada did not possess SIGINT satellite technologies of its own; however, 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.

Since the 1970s a rapidly increasing share of international telecommunications traffic has been relayed by Intelsat (International Telecommunications Satellite Organisation) satellites and other regional communications satellites. At first just two specialised ground interception stations, one British and the other American, were sufficient to achieve UKUSA monitoring of all Intelsat traffic across the world. However, subsequent refinements to Intelsat satellite design impelled the UKUSA alliance to build a chain of six intercept stations over the years in order to maintain global coverage, and to link these in a functional network. The launching of Soviet and other regional communications satellites spurred the building of other suitably situated SIGINT interception facilities to augment this UKUSA network. One of these operated under CSE aegis at Leitrim, Ontario, ostensibly targeted on Latin American satellite communications.

American SIGINT satellites yielded a prodigious flow of intercepted telecommunications traffic requiring powerful computers to process, search, filter, and identify material of intelligence interest. CSE involvement in the UKUSA network of ground-based installations for satellite SIGINT collection demanded a substantial upgrading of its technological base. The first satellite interception dish was installed at Leitrim in late 1984; another medium-size dish was erected in 1986. Staffing likewise had to be augmented and trained to analyse and disseminate the ensuing intelligence product.

To deal with this surge in SIGINT collection after 1984 CSE undertook a revitalisation 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. 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. By the late 1990s there were four satellite dishes operating at Leitrim.

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*.[38] Highly secret still, *Echelon* had its origins in the computerised processing and networking technologies which evolved since the 1970s and were greatly enhanced in the 1990s. Compared to earlier SIGINT systems deployed during the Cold War, which were designed primarily to intercept diplomatic, espionage and military communications, *Echelon* had a broad banded capacity to monitor virtually all types of electronic communications among public and private sector organisations and individuals in almost every country.

The *Echelon* system links together an array of large-scale computer processing capabilities so as to enable the various UKUSA intercept stations to function as parts of an integrated, virtually seamless SIGINT network. These interception and processing technologies are able to sort through vast flows of telecommunications traffic to identify specifically targeted messaging. At the operational heart of this integrated SIGINT processing and

networking system is the so-called *Echelon* "Dictionary" computer. These Dictionary computers, which can store a comprehensive database on designated targets, including names, topics of interest, addresses, telephone numbers and other criteria for target identification, are emplaced only in certain *Echelon*-linked SIGINT interception facilities, though not in Canada. Given the tight networking achieved under *Echelon*, every participating interception facility's Dictionary computer contains not only its parent organisation's designated keywords but also a list for each of the other partner SIGINT agencies.

While CSE may not have its own *Echelon* production capability, this networking arrangement enables Canada to post its search lists with the *Echelon* Dictionaries at other partner' facilities. Intercepted communications would be processed through these inter-connected Dictionaries, with targeted intercepts being forwarded automatically to the listing organisation. The reciprocity arrangement under UKUSA gives partner SIGINT organisations virtually automatic access to Canadian interception modalities - local in country, external, HF long distance, or satellite downlinked - without Canada necessarily being aware of their targets, while in return CSE gets to share and participate in the global capabilities of the *Echelon* system.

SIGINT TECHNOLOGY ACCESS AND SHARING

Echelon was designed to be a shared, collaborative SIGINT collection network. The technologies behind *Echelon* and other high capacity SIGINT modalities were for the most part American in origin. The technologies developed for signals intelligence purposes were so specialised and of such advanced complexity that only experienced US defence contractors and niche suppliers could design and manufacture this purpose-built equipment for NSA, and then only with government technical and financial backing.[39] Some of this equipment was made available to other partner SIGINT organisations. Among the American technologies reportedly procured by CSE were Cray supercomputers, *Echelon* systems and their miniaturised versions (*Oratory*) for outstations, miniaturised interception and processing equipment for embassy-based interceptions, high-capacity/high-speed information retrieval technologies, and high-speed traffic/topic analysis search engines, *inter alia*.

CSE and other SIGINT partner organisations also relied on NSA training facilities for their cryptanalytical and other technical specialists.

This networking system demonstrated its robustness, and the burden-sharing capabilities of the UKUSA arrangement, when the NSA main computer system crashed calamitously for four days in January 2000. What was described as a "system overload" shut down the computers used to process collected SIGINT intelligence from the 24th to the 28th of January, causing an unprecedented breakdown in the processing and analysis of raw intercepts.[40] Nevertheless, SIGINT interceptions continued uninterrupted, and the processing of incoming intelligence was shunted to other components of the *Echelon* system for the duration of the NSA outage. CSE was likely to have been involved, underscoring the high degree of systems integration among UKUSA partners and the particular value of this capability to the senior partner, the United States.

Whereas *Echelon* was conceived as a shared network, there are suggestions that its actual workings are asymmetric. According to New Zealander Nick Hagerty's disclosures about GCSB involvement in *Echelon*, each participating SIGINT organisation can only access that system for its own stipulated targets, and does not necessarily share any of the intelligence generated for other partners.[41] Participating organisations may request intelligence product from other partners *Echelon* Dictionaries, but actual access is effectively controlled by that country. If that is the case, Canada might not be able to receive output of the whole *Echelon* network even though a considerable portion of CSE's own intelligence collection probably goes to serve other UKUSA partners requirements. It seems likely that only the NSA colossus, by virtue of its size and leadership role within *Echelon* can access the full global potential of the system. For lesser players like CSE these controls on *Echelon* access render the reciprocal sharing of signals intelligence under UKUSA in effect asymmetrical.

This asymmetry is also manifest in the targeting of SIGINT satellites. All the SIGINT satellites available to UKUSA are proprietary US craft embodying American technologies, though the uplinking and downlinking networks can also involve other partners facilities. Under the *Echelon* system these US satellites could be tasked in effect through the Dictionary mechanism. Notwithstanding the sharing principle underlying UKUSA, the orbital

positioning and targeting of these satellites remain exclusively under the control of the United States. While the US has sometimes been willing to reposition satellites so as to hover and zero in on targets requested by UKUSA allies, such requests were not without their difficulties and the response was entirely at American discretion.[42]

It should be noted, parenthetically, that the NSA also transferred certain of its SIGINT technologies to the American private sector. Once these technologies had become operationally obsolescent, there were spun off to commercially successful civilian applications. However, the tables were turning by the late 1990s, when it became apparent that private sector-inspired developments in certain areas of information and communications technology, like for example encryption, were beginning to run ahead of governmental SIGINT capabilities. Indeed, NSA has come under increasingly sharp criticism from congressional intelligence committees for not keeping pace with advances in communications technology.[43]

CSE sought to promote the local development of SIGINT technologies in niches where Canada enjoyed some particular competitive advantage and where Canadian solutions might also possibly spin off to commercial applications. Over the years Canada's high-tech industry achieved demonstrated strengths in information and communications technology. Since an integrated market for Canadian and American defence industries already existed, it was considered possible that a Canadian SIGINT technology could be readily marketable to NSA and other partner organisations.

Two particularly relevant areas of niche technology where Canada seemed to enjoy competitive advantages were continuous speech recognition, software that translates verbal into digital text, and speaker/voice recognition, software than can identify individual talkers. In 1990 CSE awarded the first of a series of contracts to the Centre de recherche informatique de Montréal (CRIM) to design and build word-spotting technology for COMINT applications that could function reliably even in poor conditions.[44] After encountering insurmountable difficulties, CRIM proposed instead in 1993 to concentrate on developing a voice/topic identification module in collaboration with some American defence contractors. Further contracts were let, but progress towards an operational topic spotter system was still only in the experimental phase seven years later. Also in 1993, CSE commissioned CRIM to produce

a workable speaker identification system. There are indications that this was achieved, and in 1995 NSA reportedly procured a Voice Activity Detector and Analyser which may have incorporated Canadian technology.[45]

CANADA'S POST-COLD WAR SIGINT AGENDA

These advances in SIGINT technology and capabilities coincided with the ending of the Cold War and the adoption of new, more globalised priorities for Canada's foreign intelligence. In 1991, for the first time, the Government of Canada adopted a directive setting out its priority requirements for foreign intelligence collection. 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 organised crime, economic (counter-)espionage, and trade intelligence.[46] These emergent objectives were given operational expression in SIGINT targeting, utilising the enhanced technological capabilities that were now available.

Although CSE does not disclose its operational targets, the various annual reports of government agencies, occasional media reportage and other disclosures give indication of the persistent security challenges and new priorities shaping Canada's foreign intelligence agenda.

While the expanded foreign intelligence requirements identified certain new objectives, this in no way implied a relegation of traditional Canadian security concerns. Indeed, Canadian intelligence assessments perceive an ongoing espionage threat from Russia and other former Cold War adversaries.[47] They also assess security risks arising from newly assertive powers like China or India with hegemonic ambitions in regions of strategic significance to Canada; countries trying to evade internationally mandated sanctions or Canadian embargoes; warring states attempting to interfere with peacekeeping or preventive diplomacy initiatives; rogue states like Iran, Iraq or Libya seeking to exploit a presence in Canada for nefarious purposes; or even nominally friendly countries whose perspectives on certain key issues relating to national security may conflict with those of Canada. Thus, clandestine French activities in support of Quebec separatism were closely monitored and countered by Canadian intelligence services.[48] The security

concerns of Canadian intelligence extended as well to the inappropriate activities of foreign governments trying to exercise improper influence on Canadian decision-making or public opinion, as when China attempted surreptitiously to buy control of local Chinese-language print and broadcast media outlets in order to manipulate sentiment in the aftermath of the 1989 Tiananmen Square massacre.[49] CSE plays a part in helping to defend Canadian sovereignty and strategic interests by collecting operational intelligence on international security threats for Canadian government departments; providing counterintelligence support by monitoring clandestine activities; and protecting Canada's communications systems against foreign intrusion.

International terrorism figures prominently among the security concerns for Canadian foreign and security intelligence.[50] 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.[51] Among the international terrorist organisations or fronts active in Canada are Hezbollah and other Shiite Islamic terrorist organisations from the Middle East, the Palestinian Hamas, the Provisional Irish Republican Army (PIRA), the Liberation Tigers of Tamil Eelam from Sri Lanka, the Kurdistan Workers Party (PKK) from Turkey, and every significant Sikh terrorist group from India. These organisations established Canadian sanctuaries in order to raise and transfer funds, procure weaponry and material, set up operational bases, and to cover infiltration across the border to the United States or overseas.

Operational responsibility for security intelligence against terrorist threats to public safety or national security is vested mainly in the Canadian Security Intelligence Service (CSIS), working together with other government departments (*e.g.* Citizenship and Immigration, Department of Justice), the Royal Canadian Mounted Police (RCMP) and local police services. It may be presumed that CSE monitors the international communications of suspected terrorist elements based in Canada as well as the activities of complicit foreign groups trying to operate through Canada to attack friendly countries. In a recent instance, SIGINT interceptions helped foil an alleged conspiracy by a Montreal-based cell of the Algerian 'Armed Islamic Group' (GIA) to commit a terrorist bombing attack in the US during the New Year's 2000 celebrations.[52]

Transnational crime was recognised at the Group of 7 (G-7) Summit in Halifax in 1995 as a national security threat to many facets of public order: political, economic, social and environmental.[53] Since then international criminality has emerged as a priority concern for foreign and security intelligence in Canada and other UKUSA countries.[54] Organised criminal enterprises originating in Eastern Europe, Asia, North and South America, and Africa span the world, moving money, people and goods across borders, including Canada's. Even more threatening than the traditional transnational crimes like trafficking in drugs and arms, money-laundering, and tax evasion, are the larger-scale, potentially more devastating instances of major international fraud, corruption and the manipulation of political and financial systems, which can destabilise democratic governments, subvert legitimate institutions, undermine social order, and distort economic activities. UKUSA operations against international crime extended to the creation of a dialogue forum involving the five partners with other European countries, the International Law Enforcement Telecommunications Seminar (ILETS), which aimed to co-ordinate design standards for telecommunications equipment and software so that they remain accessible to legal surveillance. Of course, this implied that global telecommunications would remain vulnerable to covert interception, which some in the European Union have come to regard as a significant threat to their commercial interests and privacy rights.[55]

Canada has not been immune to these types of transnational criminality. In 1995 CSIS indicated that Canada's intelligence community would take on a role in combating transnational crime, primarily through the provision of international criminal intelligence and strategic analyses to law enforcement agencies.[56] As part of this combined effort it may be expected that CSE would target the international communications of criminal personalities or organisations.

International commercial crime is especially vulnerable to SIGINT interceptions, given its inescapable dependence on electronic means of voice and data communications. SIGINT interceptions could offer a unique aperture into illicit transactions and criminal activities that threaten the integrity of Canadian financial and commercial institutions. As well, SIGINT could contribute timely information on the bona fides of certain large commercial entities operating out of turbulent regions of the world and seeking to do business in Canada.[57] The intelligence collected can serve to

aid law enforcement and the effectiveness of financial and commercial regulatory agencies. Furthermore, it could help inform Canadian foreign policy decision-making regarding the countries concerned.

Canadian foreign and security intelligence concerns are also directed at the connection between transnational criminality, on the one hand, and terrorist racketeering and criminal collaboration with insurgency movements elsewhere, on the other. In one of the more notorious instances, the Liberation Tigers of Tamil Eelam established an underground network among Tamil sympathisers across Canada and also became extensively involved in racketeering to generate financing for their insurgency war in Sri Lanka.[58] Their criminal activities are alleged to have included drug trafficking partnerships with Pakistani heroin producers, immigrant smuggling, commercial fraud, and extortion from Tamils residing in this country and elsewhere. SIGINT operations can provide law enforcement agencies and foreign policy-makers with timely intelligence about attempts by transnational criminal elements to undermine the integrity of other countries and influence our own in ways detrimental to the laws and interests of Canada.

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. Canadian nuclear capabilities are devoted exclusively to peaceful purposes. Its non-proliferation foreign policy is aimed at ensuring that Canada's nuclear exports are utilised 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, CSE operations aim at identifying attempts by countries of proliferation concern to acquire Canadian weapons-related technology and expertise. Intelligence produced by SIGINT helps keep the Government of Canada and its allies alert to proliferation threats.[59]

THE ECONOMIC INTELLIGENCE CONUNDRUM

Many countries, from major powers to other smaller trade-dependent nations, have made the collection of economic intelligence an increasingly significant function of their respective foreign intelligence services. Economic intelligence is expected to identify opportunities and warn of threats to

national economic and commercial interests. As early as 1970 the former Executive Director of the US Foreign Intelligence Advisory Board assigned economic intelligence a priority equivalent to diplomatic, military, technological intelligence.[60] Canada's post-Cold War intelligence directives identified economic espionage and competitiveness among its priorities for targeting.[61]

The implications of economic intelligence collection inject a competitive impulse, not to say conflicts of interest, into the otherwise co-operative ethos of UKUSA. To deal with this, a consensus seems to have emerged amongst the UKUSA partner organisations to the effect that commercial firms are not allowed to actually task SIGINT operations for their own commercial purposes. Doing so could have posed operational risks, and is in fact unnecessary. Rather, the practice seems to have been for each UKUSA country to mandate its own national intelligence assessment organisation and relevant government departments to task and receive economic intelligence from SIGINT sources. Decisions on whether to disseminate this economic intelligence to the private companies were typically taken by these other governmental instrumentalities and not by the SIGINT organisations themselves. For example, it is reported that 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 private firms.[62]

Until recently Canadian efforts in economic intelligence seem to have been primarily defensive in orientation.[63] According to intelligence sources, Canada's chief concern in this domain 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."[63] CSIS carried the main responsibility for countering economic espionage in the context of its security intelligence mandate, however SIGINT doubtless made a contribution. One indication of growing CSE involvement in this domain was its 1995 effort to recruit additional staff with qualifications in economics, commerce and international business, in order to build up its own analytical capacity in economic intelligence.[64]

CSE operations in economic intelligence have gone rather beyond the strictly defensive to also help promote Canadian economic competitiveness and commercial objectives in world markets. Accounts published by reliable journalists 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.[65] 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.

CSE efforts in economic intelligence do not appear to have provided Canadian commercial firms with access to SIGINT products, at least not directly. The Canadian government has no identifiably dedicated unit either in the Privy Council Office, which co-ordinates Canada's intelligence effort, or in the intelligence agencies, or in the Department of Foreign Affairs and International Trade or Industry Canada, which could handle the interface between commercially-relevant intelligence and the private sector. Indeed, the peculiar structure of Canadian industry would greatly complicate any provision of government-sourced commercial intelligence to the private sector. 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 politically determined markets, but there is no evidence that the Canadian government supplies these firms with commercial intelligence in support of their marketing ventures. Of course, government officials may sometimes provide advice and counsel by way of helping to promote Canadian trade, without necessarily revealing their sources in economic intelligence. Canada's crown corporations present a somewhat different challenge for economic intelligence; these enterprises, established by the federal and provincial governments, control important sectors of the export economy, including grain exports, energy exports, and export insurance and finance, where

commercial intelligence can yield competitive advantages in government-to-government negotiations. However, it is questionable whether any intelligence so garnered was actually shared with crown corporations like the Canadian Wheat Board or Atomic Energy Canada Limited, or whether government negotiators themselves used this information to shape their bargaining positions on such public sector transactions as wheat sales to China or Candu sales to South Korea.

CSE is also responsible for Canadian information technology security (ITS). Canada has state-of-the-art industrial capabilities in various sectors of information technology, and Canadian companies have been targeted by foreign governments for economic or industrial espionage.[66] Some of the foreign governments engaging in technological espionage are recent adversaries while others are erstwhile friends and allies. Moreover, certain of these information technologies can have dual-use, and may be vulnerable to redeployment by weapons proliferators or even terrorists. As the lead federal agency for ITS, CSE provided technical information, tools and expert services to government departments and private industry in areas of Network Security, Internet Security, Cryptography and Public Key Infrastructure. CSE industrial programs are also collaborating with Canadian industry to develop advanced ITS products and services.[67]

It is inherently difficult to assess the operational performance of intelligence agencies. According to the 1996 Auditor-General's report, CSE has made a significant effort to cost its operations and products and identify gaps in its collection of signals intelligence in relation to national priorities and the specific requirements of client departments.[68] The Government's own assessment of the performance and value of signals intelligence is indicated in its resource commitments to CSE, both funding and staffing. In the early post-Cold War period, government budgetary appropriations for CSE were estimated at C$113 million for fiscal year 1995-96, a reduction of about 10% in real terms from 1990-91 (*i.e.* Cold War) levels. This compared favourably with the sharp cutbacks that took place in federal spending generally, including (indeed especially) national defence. While a declining trend continued for virtually all government departments and agencies, the nominal CSE budget for 1999/2000 of C$109 million suggests that Signals Intelligence continued to fare better than most other government services.[69] Staffing has remained stable at approximately 900 (exclusive of Canadian

Forces Information Operations Group personnel), with the proportion of analysts probably expanding. DND defence planning guidelines project a 6% increase in CSE's budget over the next five years.

FUTURE CHALLENGES

Signals intelligence collection provides Canada's policy-makers and security establishment with a capacity to cope with risk and threats to Canadian interests in an otherwise uncertain and volatile global security environment. Canada has a comparatively small population, yet it is a member of the G-7 and is extensively engaged in international relations in security, trade and finance, social affairs, environment, development, peacekeeping, and global governance. These international activities entail a requirement for foreign intelligence in support of policy-making and the conduct of bilateral and multilateral relations. CSE has been able to provide this intelligence in part by dint of its own SIGINT capabilities, but more significantly through the extended capabilities available to Canada under the UKUSA arrangement.

Current trends in SIGINT imply two major challenges for CSE's future capability to perform its signals intelligence collection and processing functions. The first of these challenges stems from ongoing trends in communications technology which tend to favour communications security over penetration, protection over interception. A second set of challenges arises from prospective changes in the dynamics of UKUSA once competition outstrips co-operation in the emergent globalised agenda for intelligence collection, in particular economic intelligence. It is ironic that these challenges derive from existing arrangements that have served CSE well, but are now developing in directions that can jeopardise the future capacity of CSE to respond to Canada's foreign intelligence requirements.

The technological lead in computers and information technology once enjoyed by SIGINT organisations has now been very largely dissipated.[70] Widely available technologies today offer others, including potential adversaries, the same technical advantages to protect their communications as SIGINT hitherto had to monitor this traffic. As a result, access to global communications networks is likely to become increasingly problematic for signals intelligence. This will become even more challenging as international

telecommunications shifts over to high capacity optical fibre networks which reportedly cannot be intercepted by current SIGINT technologies.[71] Intrusive access would be necessary for interceptions. Clandestine operations of this type would be risky, and could become politically unacceptable.[72]

SIGINT advantages in cryptanalysis are likewise dissipating in face of rapid advances in civil and commercial cryptography along with the development of more effective cryptographic security systems.[73] Indeed encryption is becoming widespread very rapidly as electronic commerce expands, an increasingly problematic trend for communications intelligence collection, in particular. It is clear that CSE and its SIGINT partner organisations were unsuccessful in their bid to constrain private sector cryptography by arguing for 'public key escrow' and similar systems ostensibly to support law enforcement (as distinct from signals intelligence) requirements. Innovative and costlier technologies will have to be deployed in future in order to stretch cryptanalytical capabilities sufficiently to extract the intelligence required.

The transition from the Cold War to a new, more globalised SIGINT agenda poses certain other challenges for the future of UKUSA operational solidarity and intelligence sharing. It has been a principle of UKUSA co-operation that its SIGINT activities do not target one another or their respective nationals (including corporations). Whenever SIGINT intercepts incidentally implicate nationals of the partner countries, steps are taken to protect the anonymity of the individual(s), or enterprise(s) in the handling and sharing of the intelligence. This principled understanding was necessary in order to ensure compliance with national law and self-interest in the partner countries while facilitating inter-group collaboration and sharing of signals intelligence collection; it also served to mitigate conflicts of interest.

Once the Cold War was over, however, the adoption of a more broadly globalised agenda for foreign intelligence collection by each of the UKUSA partner countries, including Canada, had far reaching implications for the shared SIGINT enterprise. Unlike the focused SIGINT effort of the recent past, the more broadly targeted post-Cold War intelligence directives adopted by the UKUSA governments were not entirely congruent one with the other. Differences and asymmetries in priorities created a potential for conflicts of interest over SIGINT targeting and intelligence collection. Although UKUSA partners remain committed to the principle of refraining from targeting each

other or their respective nationals, nevertheless a former US National Security Council official Howard Teicher made a point of commenting:

> I would never say never in this business because, at the end of the day, national interests are national interests ... sometimes our interests diverge. So never say never - especially in this business.[74]

Arguably, the risks of conflicts of interest within UKUSA are greatest in the increasingly important SIGINT domain of economic intelligence. It is here that the UKUSA ethos of co-operation may be most vulnerable to protectionist impulses and dysfunctional competition. In as much as UKUSA countries are major trading partners between and among themselves, they are often engaged in trade negotiations or dispute settlement procedures at the bilateral, regional (*e.g.* APEC, NAFTA) and multilateral (*e.g.* World Trade Organisation) levels. Since these economies are also competitors in many world markets, they are frequently keen commercial rivals. In the circumstances, SIGINT economic intelligence operations that *never* targeted other partners' commercial interests or negotiating stances would probably be deemed irrelevant by domestic policy makers, and yet any effort to systematically target allies' proprietary commercial, technological or policy secrets would compromise UKUSA collaboration and render the *Echelon* alliance highly problematic. Nonetheless, press accounts describe the activities of friendly and even allied countries in eavesdropping on one another in order to gain negotiating advantages at bilateral and multilateral meetings on international trade.[75]

Hence the paradox of co-operation/competition that confronts SIGINT in the domain of economic intelligence. Economic intelligence collection which is timely and informative for competitive advantage can be *passi passu* inherently undermining and destructive of operational co-operation and technology sharing. Yet any turn of events that would tend to constrain collaboration in UKUSA would substantially weaken CSE's capacity to achieve near global access to SIGINT facilities to meet Canada's foreign intelligence requirements. Foreign intelligence is an essentially competitive enterprise in which countries seek their own advantage, and in which all gains are differential, asymmetric gains.

Another area of potential conflict of interest among UKUSA partners concerns the use of SIGINT interceptions for law enforcement purposes.[76] In targeting transnational crime, SIGINT operations must take account of the mandatory legal and technical prerequisites governing interceptions for law enforcement purposes, as distinct from interceptions of communications intelligence. Not only must this distinction be recognised and observed, it must be observed operationally and reciprocally across the multiple legal jurisdictions of UKUSA so as not to compromise the bona fides of law enforcement. Any blurring of this distinction would risk dangerous illegalities and human rights transgressions and the gathering of inadmissible evidence. 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.[77]

It is questionable whether Canadian law or Charter of Rights and Freedoms can be applicable to SIGINT operations that task CSE facilities to target alleged transnational criminality at the behest of UKUSA partners. The legal issues implicit in SIGINT-derived evidence have never been tested before Canada's courts. Whenever questions have been raised, mere reference to Canada's 'international' obligations has sufficed to defer detailed inquiries. Up until now Canadians have been generally (albeit tacitly) willing to countenance SIGINT interceptions for 'security' purposes, however broadly defined. Were there to be perceived violations of law and human rights, however, these are unlikely to be politically unacceptable to government and public. Yet for Canada (or another partner country) to impose national legal or human rights standards unilaterally onto SIGINT interceptions might well jeopardise future UKUSA collaboration against transnational crime and other sensitive targets.

The more Canada's foreign intelligence requirements become globalised in future, the greater will be CSE's reliance on UKUSA sharing arrangements and the more its operational activities will become exposed to the underlying risks. The prospect of any lessening of these co-operative SIGINT capabilities, whether due to technological trends, differential interests of partners, or legal dilemmas, could severely circumscribe Canada's capacity for foreign intelligence collection. Canada depends on CSE to manage its own resources and international linkages in a way that safeguards its future

capacity to respond to Canadian foreign intelligence requirements in an increasingly predatory international environment.

ABOUT THE AUTHOR

Martin Rudner is Director of the Centre for Security and Defence Studies at The Norman Paterson School of International Affairs, Carleton University. He is also Professor at the School and teaches several courses, including on Intelligence and Security.

LIST OF OCCASIONAL PAPERS

1. Aliya and the Demographic Balance in Israel and the Occupied Territories (1992)
   James W. Moore

2. A New Germany in a New Europe (1992)
   John Halstead

3. Does the Blue Helmut Fit? The Canadian Forces and Peacekeeping (1993)
   Ian Malcolm

4. Yugoslavia - What Went Wrong? (1993)
   John M. Fraser

5. The Origins and Future Demise of the Democratic People's Republic of Korea (1994)
   Charles K. Armstrong

6. Contesting an Essential Concept: Dilemmas in Contemporary Security Discourse (1994)
   Simon Dalby

7. Ethnic Conflict and Third Party Intervention: Riskiness, Rationality and Commitment
   David Carment, Dane Rowlands and Patrick James

8. Conflict Prevention and Internal Conflict: Theory and Policy, A Workshop Summary (1995)

9. David Mitrany, the Functional Approach and International Conflict Management (1995)
   Lucian Ashworth and David Long

10. Dealing with Domestic Economic Instability: U.S. Foreign Policy and the Rally Effect, 1948-1994 (1996)
    Athanasios Hristoulas

11. Modelling Multilateral Intervention in Ethnic Conflict: A Game Theoretic Approach (1996)
    David Carment and Dane Rowlands

12. The Interstate Dimensions of Secession and Irredenta: A Crisis-Based Approach (1996)
    David Carment

13. The Functional Approach, Organization Theory and Conflict Resolution (1996)
Craig N. Murphy

14. Using a Culturally-Specific Process of Mediation and Dispute Resolution to Promote International Security (1997)
Roger Hill

15. Exploring Canada's Options on 'Global' Issues (1997)
Evan H. Potter and David Carment

16. Canadian Foreign Policy: From Internationalism to Isolationism? (1997)
Jean-François Rioux and Robin Hay.

17. Making the Impossible Possible: The PLA's Cross-Strait Operations in the 21st Century (1999)
Jianxiang Bi

18. Water Balances in the Eastern Mediterranean: A Workshop Summary (1999)
Ozay Mehmet.

19. Conditions of Influence: A Canadian Case Study in the Diplomacy of Intervention (1999)
John B. Hay

20. Information Warfare: Media-Military Relations In Canada (1999)
Michael Croft, Sharon Hobson, and Dean Oliver

21. Twisting Arms and Flexing Muscles: Perspectives on Military Force, Humanitarian Intervention and Peacebuilding - Report on a Workshop (2000)
Natalie Mychajlyszyn

22. Canada's Communications Security Establishment: From Cold War To Globalization. (2000)
Martin Rudner

Ordering Information:

- Please send a cheque or money order for $10.00 to (made out to **The Norman Paterson School of International Affairs**) to Elizabeth James, NPSIA, Carleton University, 1125 Colonel By Drive, Ottawa, ON, K1S 5B6.
- Please add $2.00 to the cost of each item when ordering by mail.
- If the item is picked up in person, the cost is as listed here.

NOTES

[1] Federal government expenditure on signals intelligence and information technology security involves the combined budgets of CSE itself and the Canadian Forces Information Operations Group, which provides operational personnel for its interception facilities, and which together exceed spending on the domestic security intelligence organization, the Canadian Security Intelligence Service.

[2] CSE (like its predecessor, the Communications Branch of the National Research Council) was established by Order-in-Council, that is by cabinet decree, rather than on the basis of formal enabling legislation. There is very little information in the public domain regarding CSE. Some carefully crafted official information is available in the *Report of the Auditor General of Canada, 1996, The Canadian Intelligence Community - Control and Accountability* (Ottawa: November, 1996) Chapter 27; in annual reports of the Office of CSE Commissioner; in infrequent officials' testimony before Parliamentary committees; and in snippets of other periodic reports (e.g. DND budgetary documents, The Privacy Commissioner's *1995-96 Annual Report*). The CSE's own website (URL: http://www.cse.dnd.gc.ca) concentrates on its public information technology security mission. There have been occasional newspaper articles on CSE activities and references to it in studies of other Canadian intelligence organizations or allied SIGINT organizations. An unofficial website prepared by Bill Robinson on *The Communications Security Establishment: An Unofficial Look Inside Canada's Signals Intelligence Agency* is accessible at the URL: http://watserv1.uwaterloo.ca/~brobinso/cse.html.

[3] For a synopsis of the structure of government control and accountability over the Canadian intelligence community, see the *Report of the Auditor General of Canada*, 1996, Chapter 27: *The Canadian Intelligence Community. Control and Assessment*, Paras. 27.66-27-94 (http://www.oag-bvg.gc.ca/domino/reports.nsf/html9627ce.html).

[4] Peter Hum, "I Spy", *Ottawa Citizen* (10 May 1997).

[5] Auditor-General, *The Canadian Intelligence Community*, para. 27.30.

[6] Auditor General, *The Canadian Intelligence Community*, para. 27.82.

[7] On the wartime history of Canadian signals intelligence see John Bryden, *Best Kept Secret: Canadian Secret Intelligence in the Second World War* (Toronto: Lester, 1993); Wesley Wark, "Cryptographic Innocence: The Origins of Signals Intelligence in Canada in the Second World War," *Journal of Contemporary History* (1987).

[8] Kevin O Neill, *History of CBNRC* (1987)[Classified]. Parts of this internal history have been released in abridged form under the Access to Information Act.

[9] Vladislav Zubok and Constantine Pleshakov, *Inside the Kremlin's Cold War. From*

Stalin to Khrushchev (Cambridge: Harvard University Press, 1996), p. 146.

[10] For an article placing Gouzenko's defection into the larger foreign policy context relating to Canadian involvement in the Cold War, see Robert Bothwell, "The Cold War and the Curate's Egg: When did Canada's Cold War Really Begin?" *International Journal*, Vol. 53, No. 3 (Summer, 1998).

[11] Nigel West, *Venona: The Greatest Secret of the Cold War* (Toronto: HarperCollins, 1999.

[12] While most CBNRC personnel were Canadian, for several years senior staff came from Britain's GCHQ, giving indication of the early and close working relationship established between the British SIGINT organization and its emergent Canadian counterpart.

[13] John Bryden, *Best Kept Secret*, pp. 280-1; Christopher Andrew, "The Making of the Anglo-American SIGINT Alliance," Win Hayden Peake and Samuel Halperin, eds., *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer*, Washington, DC: NIBC Press, 1994, p. 105.

[14] Stephen Dorril, *MI6. Inside the Covert World of Her Majesty's Secret Intelligence Service* (New York: Free Press, 2000), pp. 54-55. Australia likewise consented to being represented in the alliance by Great Britain.

[15] Bryden, *Best Kept Secret*, p. 291-2; Wark, "Cryptologic Innocence," p. 659. I am indebted to Matthew Aid for making available his impressive historical records on Canadian SIGINT.

[16] Robinson, *The Communications Security Establishment*, SIGINT sites; O'Neill, *History of CBNRC*, Chap. 2; Matthew Aid, communication to author.

[17] Bryden, *Best Kept Secret*, p. 296; Memorandum, Agee to Coordinator of Joint Operations, *Proposed US-Canadian Agreement*, June 7, 1948, RG-341, cited in communication from Matthew Aid.

[18] Bryden, *Best Kept Secret*, p. 326. For a summary of Canadian cryptanalysis in the service of signals intelligence, see Bill Robinson, "The Fall and Rise of Cryptanalysis in Canada," *Cryptologia* (January, 1992) and "Cryptanalysis at CSE," *The Communications Security Establishment*.

[19] Mark Urban, *UK Eyes Alpha* (London: Faber and Faber, 1996), p. 6

[20] Robinson, "Cryptanalysis at CSE" and "The Fall and Rise of Cryptanalysis in Canada."

[21] Richard Cleroux, *Official Secrets* (Toronto: McLelland and Stewart, 1991), p. 266.

[22] N. C. Gerson, "Collaboration in SIGINT: Canada-US," *NCVA Cryptolog* (Spring, 1999); Matthew Aid personal communication.

[23] Peter Wright, *Spycatcher*, New York: Viking, 1987.

[24] Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive. The KGB in Europe and the West* (London: Allen Lan, The Penguin Press, 1999), pp. 451, 448, 850, footnote 63.

[25] Urban, *UK Eyes Alpha*, p. 6.

[26] Eldon Black, *Direct Intervention: Canada-France Relations 1967-1974* (Ottawa; Carleton University Press, 1996) refers to Canadian "security authorities" providing intelligence on French communications with "dubious contacts in Quebec" (pp. 50-1). For reports on CSE monitoring Quebec separatist communications with France, see Doug Gilmour, "WCC Members Likely Targets for Defence Monitors - Ex-Spy," *Edmonton Journal* (15 October 1982); Peter Moon, "Canadian Agency Safeguards its Role in World Spy Game," *Globe and Mail* (30 March 1987); Gerry Arnold, "Officials Deny Report of Canada-France Spy Feud," *Ottawa Citizen* (22 May 1992); Mike Frost & Michel Gratton, *Spyworld: Inside the Canadian and American Intelligence Establishments* (Toronto: Doubleday, 1994), cited in Robinson, "Eavesdropping on the Quebec separatist movement," *The Communications Security Establishment.*

[27] Andrew and Mitrokhin, *The Mitrokhin Archive,* p. 453.

[28] Frost and Gratton, *Spyworld*, pp. 19, 72, 76; Bruce Livesey, "Trolling for Secrets - Economic Espionage is the New Niche for Government Spies," *Financial Post* (28 February 1998).

[29] Frost and Gratton, *Spyworld,* pp. 183, 191.

[30] This episode was revealed by former CSE employee, Mike Frost, in a CBS "60 Minutes" program and reported in "Spy Agencies List in on Diana", *The Sunday Times* (27 February 2000).

[31] Canadians reportedly underbid the United States on this wheat deal after having intercepted a car phone conversation between the US Ambassador and Ottawa Embassy discussing the American negotiating position. *Cf.* "The Murky Side of Trade," Livesey, "Trolling for Secrets."

[32] Jeffrey Richelson and Desmond Ball, *The Ties that Bind: Intelligence Cooperation Between the UKUSA Countries* (London: Allen and Unwin, 1985), p. 144. All the outlying receiver stations are now remote controlled from Leitrim.

[33] Cited in Stephen Dorril, *MI6*, p.56.

[34] On the unusual character of the UKUSA arrangement see Jeffrey Richelson, *The US Intelligence* Community (New York: Ballinger, 1989), esp. chap. 12; Robinson, "The UKUSA Community," in *The Communications Security Establishment*; Richelson and Ball, *The Ties that Bind*, pp. 142-3 *et passim*; on the origins of UKUSA see Christopher Andrew, "The Making of the Anglo-American SIGINT Alliance," in Hayden Peake and Samuel Halperin, eds., *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer* (Washington, DC: NIBC Press, 1994).

[35] One of the rare explicit official references to the UKUSA agreements was made by the Deputy Clerk, Security and Intelligence, Privy Council Office, in testimony before the House of Commons Standing Committee on National Defence and Veterans Affairs, 2 May 1995.

[36] Margaret Bloodworth, Deputy Clerk, Security and Intelligence, Privy Council Office, evidence presented to the House of Commons Committee on National Defence, 2 May 1995.

[37] Urban, *UK Eyes Alpha*, pp.32-3.

[38] Very little has been revealed officially about *Echelon* by any of the UKUSA governments. Among the seemingly better informed sources are *Interception Capabilities 2000*, the Report to the Director-General for Research of the European Parliament prepared by Duncan Campbell (1999); and the disclosures about New Zealand's involvement in Nick Hager, *Secret Power: New Zealand's Role in the International Spy Network* (Nelson, NZ: Craig Potton Publishing, 1996), esp. chap. 2 and "Exposing the Global Surveillance System," *Covert Action Quarterly* (Winter, 1997).

[39] One of the rare descriptions of contemporary SIGINT equipment is provided in the Technical Annexe to *Interception Technologies 2000*.

[40] "NSA System Inoperative for Four Days", *Washington* Post (30 January 2000).

[41] Hager, "Exposing the Global Surveillance System."

[42] For an account of the British experience in persuading the US to reposition its SIGINT satellite to provide intelligence coverage at the time of the Falklands war see Urban, U*K Eyes Alpha*, p. 57.

[43] "NSA System Inoperative for Four Days".

[44] *Interception Technologies 2000*, Technical Annexe, paras. 33-36.

[45] *Interception Technologies 2000*, Technical Annexe, para. 36.

[46] *Auditor-General, The Canadian Intelligence Community*, para. 27-31.

[47] Canadian Security Intelligence Service, *1997 Public Report*, Parts 1, 3 URL: www.csis-scrs.gc.ca/eng/publicrp/pub1997e.html.

[48] *Cf.* Black, *Direct Intervention*, pp. 50-1.

[49] According to the media disclosure, telephone intercepts were part of this counterintelligence operation: "CSIS warned Ottawa of Beijing Media Plot," *Globe and Mail* (9 February 2000).

[50] CSIS *1997 Public Report*, Part 2.

[51] CSIS, *Trends in Terrorism*, Perspectives, Report 2000/01 (18 December 1999).

[52] Newspaper accounts describe the role of SIGINT interceptions in unravelling what appears to have been a complex Islamic terrorist conspiracy: "US Probe Ties Bomb Plot to Bin Laden Group," *Washington Post* (20 February 2000); see also "Calls Said to Link Woman to Man with Explosives," *New York Times* (13 January 2000), "Canada Adds Details on Algerians' Suspected Bomb Plot," *New York Times* (21 January 2000), "Algerian Charged in Bombing Plot Aids FBI Probe," *Washington Post* (21 January 2000).

[53] Samuel Porteous, *The Threat from Transnational Crime: An Intelligence Perspective*, CSIS Commentary #70, Ottawa: Canadian Security Intelligence Service, Winter, 1996.

[54] CSIS *1997 Public Report*, Part 3; Whose (*sic*) Being Spied On?" BBC (13 September 1999).

[55] "Comment les États-Unis espionnent l'Europe," *Le Monde* (23 février 2000).

[56] CSIS *1995 Public Report and Outlook* (Ottawa: Canadian Security Intelligence Service, 1995). The RCMP Economic Crimes Directorate is responsible for investigating commercial crime in Canada. Parliament is currently considering a Bill to set up a dedicated Financial Transactions and Reporting Analysis Centre to monitor international money movements.

[57] Porteous, *The Threat from Transnational Crime.*

[58] *Vide.* Porteous, *The Threat from Transnational Crime.*

[59] CSIS *1997 Public Report*, Part 3.

[60] *Interception Technologies 2000*, para. 97; Samuel Porteus, *Economic/Commercial Interests and Intelligence Services*, CSIS Commentary #59, Ottawa: Canadian Security Intelligence Service, July, 1995.

[61] *Vide.* Auditor-General, *The Canadian Intelligence Community*, para. 27.27.31; CSIS, *1997 Public Report*, Part 3.

[62] *Interception Technologies 2000*, para. 100.

[63] CSIS, *1997 Public Report*, Part 3.

[64] Porteus**,** *Economic/Commercial Interests and Intelligence Services.*

[65] Livesey, "Trolling for Secrets."

[66] CSIS *1997 Public* Report, Part 3.

[67] On the Canadian Information Technology Security program operated by CSE see the CSE website at URL: http://www.cse.dnd.gc.ca.

[68] Auditor-General, *The Canadian Intelligence Community*, Chapter 27: *The Canadian Intelligence Community. Control and Assessment*, paras. 107-109.

[69] Robinson, *The Communications Security Establishment.*

[70] According to LtGen. Michael V. Hayden, Director of NSA, the SIGINT agency is already lagging behind private sector technological developments in telecommunications (Address to Kennedy Political Union of American University, 17 February 2000). See also *Interception Capabilities 2000*, paras. 106-108.

[71] The possible existence of a new, top secret American technology to intercept fibre optic traffic is mentioned in Le Nouvel Observateur [Paris] (10-16 December 1998), pp. 10-22.

[72] NSA has sought to overcome this growing cryptanalytical constraint by collaborating with CIA in a joint initiative, the Special Collection Service, which undertakes clandestine intrusive operations to intercept traffic from otherwise secure targeted systems: "Une alliance secrete entre la NSA et la CIA," *Le Monde* (22 février 2000).

[73] Simon Singh, *The Code Book* (1999) examines the evolution of codes up to current experimentation with quantum cryptography, which is said to be absolutely unbreakable; see also *Interception Capabilities 2000*, paras. 109-110.

[74] Cited in *Interception Capabilities 2000*, para. 105.

[75] *Cf*. "The Murky Side of Trade Meetings"; Duncan Campbell and Paul Lasmar, "The New Cold War: How America Spies on Us for its Oldest Friend - The Dollar," *The Independent* (2 July 2000).

[76] *Cf. Interception Capabilities* 2000, "Policy Issues for the European Parliament," para. 4.

[77] *Cf.* Paul Palango, *The Last Guardians* (Toronto: McLelland and Stewart, 1998), pp.165-7.