SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1992-93

Canada

Security Intelligence Review Committee
122 Bank Street, Jackson Building
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

Tel: (613) 990-8441
Fax: (613) 990-5230
Collect calls are accepted, and the switchboard is open
from 7:30 a.m. to 6 p.m. Eastern Standard Time.

Cat. No. JS71-1/1993
ISBN 0-662-60053-3

The Honourable Doug Lewis, P.C., M.P.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Lewis:

As required by *section 53* of the *Canadian Security Intelligence Service Act*, we transmit to you the Annual Report of the Security Intelligence Review Committee for the fiscal year 1992-93, for your submission to Parliament.

Yours sincerely,

Jacques Courtois, P.C., Q.C.
Chairman

Edwin A. Goodman, P.C., O.C., Q.C.

Michel Robert, P.C., Q.C.

Rosemary Brown, P.C.

George W. Vari, P.C., O.C., C.L.H.

ETERNAL VIGILANCE IS THE PRICE OF LIBERTY

J.P. Curran
[1750-1827]

Contents

Security Intelligence Review Committee

The Security Intelligence Review Committee at a Glance

The Security Intelligence Review Committee (called ``SIRC'' or ``the Committee'' in this report) acts as the eyes and ears of the public and Parliament on the Canadian Security Intelligence Service.

The Canadian Security Intelligence Service (CSIS) is a federal government agency, created in 1984 by the *Canadian Security Intelligence Service Act* (the *CSIS Act*). CSIS investigates terrorists, agents of hostile intelligence services, and others whose activities may be a, ``threat to the security of Canada.'' CSIS must protect its sources and methods. Inevitably, therefore, much of its work remains secret. This makes it difficult for Members of Parliament and the Canadian public to ensure that CSIS operations are effective and that, at the same time, CSIS respects the rights and freedoms of Canadians. To pre-empt these potential problems, the same law that created CSIS created SIRC.

The Committee is independent of the Government in its operations, but responsible to the Parliament of Canada. The *Canadian Security Intelligence Service Act* provides that its members are appointed by the Governor-General-in-Council, after consultation with the leaders of all parties having more than twelve members in the House of Commons. Individuals may be appointed to the Committee only if they are already Privy Councillors or are appointed to the Privy Council for that purpose by order of the Governor-General-in-Council.

To the extent that national security permits, the Committee reports to Parliament through its Annual Report. This is available to the public. It constitutes an evaluation of CSIS operations that would otherwise not be allowed to come under public scrutiny because of national security considerations.

The Committee also has the power to investigate complaints relating to CSIS. First, it can investigate complaints by a person about, ``any act or thing'' done by CSIS. It is not necessary that the person complaining be personally affected by what CSIS did.

Second, the Committee can review certain denials or revocations of security clearances affecting federal government employees, or job applicants, or persons who seek to sell goods or services to the federal government under contract.

Third, in a related vein, it can also review adverse security findings that would affect a person's right to immigrate to Canada or obtain Canadian citizenship. If the Committee finds a complaint justified, it recommends a remedy.

1. Introduction

The SIRC Mandate

In our Annual Report for 1991-1992, we said that if SIRC and CSIS management had fulfilled their respective roles in a reasonably competent manner over the previous eight years, then the Service should by now be operating in a legal, ethical, and appropriate manner. We added that, in general, we had found that to be the case.

This Annual Report reflects the fact that CSIS is now a very different organisation than it was four or five years ago. It is also operating in a radically changed environment now that the cold war no longer dominates international relationships.

Once again, we have some criticisms to make about the appropriateness of some of the activities of CSIS during the 1992-93 period but, on the whole, this report paints a picture of an agency that is working within the law and operating effectively.

However, the main concern of some interested observers of CSIS now seems to be not simply whether what is being done is being done well, but whether it needs to be done at all. The decade of the Nineties is turning out to have a dominant theme in both private and public affairs: frugality.

Parliament gave the Review Committee a very broad mandate that has always included two fundamental aspects of the activities of CSIS: its effectiveness in protecting the nation's security against foreign or domestic threats; and, while fulfilling this important role, its sensitivity to the civil liberties of Canadians. In the past, we have tried to act in accordance with the then public and parliamentary concerns, and have focused almost exclusively on civil liberties.

We have no intention of diminishing the extent of our concern for the protection of civil rights, but we have now started to focus somewhat more on whether some of the traditional activities of CSIS still meet the test of being necessary to the protection of Canada's security. Judging from our reading of editorial comment and our contacts with Parliamentarians, this increased attention to the *what* rather than the *how* of the activities of CSIS reflects a general feeling that the end of the Cold War should lead to a restructuring — and probably a reduction — in the CSIS organisation and budget.

We, however, must recognise that the security of our country is paramount, and we are convinced that Canada will continue to need to devote a considerable amount of its scarce public resources to counter-terrorism for the foreseeable future.

This year's Annual Report includes our comments on the Director's Task Force Report, which, as we mentioned last year, focuses on what CSIS should be doing in the Post-Cold-War world. Our observations on the conclusions of the Task Force are made in the light of discussions at a

seminar we held in September 1992. We asked experts in the field to give us their views on the future of CSIS, and we invited the Director, Ray Protti, to take part in the exchange of ideas.

Our views on the Director's Task Force Report can be found in Chapter 2. We still have some questions about the apparent new emphasis on the protection of science and technology, but we applaud the steady diminution in the interest of CSIS in the old Warsaw Pact countries, and its consequent steady movement of resources from counter-intelligence operations to counter-terrorism.

Since the fall of the Berlin Wall, many of the certainties and assumptions of the last forty years have become irrelevant. Espionage activity continues, as this report points out in Chapter 2, but much of it appears to be directed with little enthusiasm, and may well be due more to bureaucratic inertia than to conscious decision-making by the overworked and crisis-ridden governments of the former Warsaw Pact countries.

We believe that CSIS is re-orienting its activities in a sensible, prudent fashion, given current circumstances, and we expect that process to continue steadily over the next few years. The result will be a Service that acts effectively against the modern terrorist threat to vulnerable, highly interdependent, post-industrial societies such as our own, and which could cost the nation less.

2. The Changing Environment

(a) The Director's Task Force

Introduction

As we noted in our 1991-92 Annual Report, the Solicitor General asked the Director of CSIS to give him, ``an assessment of how the security environment might affect the Service's mandate over time."
[1] The Director created a Task Force to carry out the request and also to evaluate how CSIS should be structured to respond to the new security environment, and the resource implications arising from such restructuring.

The Forecast

The project began in February 1992 and ended in the Fall. One of the results was a five-year forecast in which CSIS summarized the implications of the new security environment for Canada. Our comments are made in the knowledge that the preparation of any threat forecast, especially one spanning several years, is an unenviable task and one fraught with peril.

In drafting the forecast, the Service drew upon its own internal analytical resources and also sought input from other agencies, both domestic and foreign.

An important factor, which we kept in mind as we reviewed the Task Force Report, was that the analysis and the resource proposals arising from that analysis did not represent current Canadian government policy, nor were they binding on CSIS.

The Task Force concluded that, since the establishment of CSIS in July 1984, the threat environment has changed considerably. It saw many implications for Canada and, consequently, for the mandate of CSIS. Overall, the report predicted that the security intelligence environment will be characterized by the global,

> ``...resurgence of nationalism, and a re-emphasis on nationally focused foreign, defence, economic and intelligence collection policies."

For the most part, we do not differ with many of the basic premises in the CSIS forecast. Chief among our agreements is that terrorism will remain pervasive and violent, and that the intelligence services of several countries will continue to be directed at Canada, in part to obtain defence technology at low cost.

[1] Security Intelligence Review Committee, *Annual Report 1991-92*, page 47.

Similarly, we do not dispute the fact that those countries which wish to acquire weapons are likely to continue to seek technology in this country. We agree, too, that some foreign governments will attempt to influence Canada's ethnic communities to support their own foreign policy interests. We also share the Task Force concerns about the activities of domestic extremists, and the opportunities for conflict that their activities can engender.

We believe that these areas represent potential real threats to Canada, and that the mandate of CSIS requires it to provide warning and advice to the Government concerning these threats. Our role, however, requires us to carefully review what CSIS does in these areas in order to ascertain whether the Service has conducted itself according to the Legislation, the Ministerial Directives and Policies in place, and whether its activities are appropriate and reasonable.

We looked at the implications raised by the Task Force Report for the key operational branches in CSIS.

Counter-Terrorism

In the counter-terrorism area, the Task Force discussed the ``Homelands'' issue wherein conflicts and tensions in other countries are brought to Canada and have the potential to provoke violence here. Major sources of concern in the Service's report are ``extremists'' based in a few of Canada's communities. The Task Force describes Canada as a ``safe haven'', and argues that there are persons and groups using Canada as a base for organizing terrorist activities abroad or for raising funds in this country to be used to support violence in other countries.

We agree that **any** such activity, whether organizing political violence or obtaining funds to purchase weapons, is unacceptable. However, it is also important to place the issue in context. Canada has experienced relatively little serious terrorist violence, and ``extremists'' are certainly not representative of the ethnic communities in which they live.

As a matter of routine, we examine the activities of CSIS to determine whether the powers it uses are proportionate to the threats posed to Canada. In this Annual Report, for example, we report on how well CSIS is managing its investigations into groups and persons associated with the conflicts in Asia and the Middle-East. One important aspect is how the Service conducts its community interview programs. We discuss this issue in Chapter 3.

Threats to Canada's security cannot be seen as arising solely from overseas conflicts. There is also the potential for terrorism on the domestic front. Racist extremists or radical groups which are prepared to use violence in support of a political objective have the potential to represent serious threats to Canadians. We examine what role the Service should play in regard to these areas, given the significant responsibilities of law enforcement agencies.

The line between criminal intelligence and security intelligence can sometimes be very fine indeed. We examine these issues in our Domestic Investigations section of Chapter 3 of this report.

Counter-Intelligence

The Task Force Report states that countries seeking economic advantage will continue to direct economic, scientific and technological intelligence collection efforts here and, in fact, may increase these efforts. We see the economic intelligence related arguments as important to continued CSIS efforts against traditional adversaries, and to the perception in the Counter-Intelligence Branch of its future role.

This issue has important implications for the use of powers by the Service. Traditionally, investigations pertaining to technology involved, directly or indirectly, military applications. We examine the role of CSIS in the economic and technological intelligence spheres later in this chapter.

We also examine the views of CSIS on some traditional counter-intelligence adversaries in our, ``Review of Traditional CI Threats in Light of Historic Political Changes," in Chapter 2.

Summary

The fundamental message from the Director's Task Force is that the security intelligence environment is, ``...diverse, volatile and complex." With the demise of the Soviet empire, the expectations of nationalist movements have been heightened around the world, and the reverberations may yet be felt in Canada. Established states have also been affected and they may place more emphasis on, ``nationally focused foreign, defence, economic and intelligence collection policies."

The explicit message of the Task Force is that, aside from a restructuring in counter-intelligence towards the economic, and proliferation of weapons of mass destruction, sectors, CSIS should conduct business as usual. The report states that public safety could be compromised if major resource cuts took place.

Many Canadians believe that there should be a ``peace dividend" arising from the demise of the East Bloc. The Service has reduced its resource levels; these downward pressures on expenditure and the emphasis upon frugality will probably continue. Our focus will be on observing the adjustments of the Service as it seeks to economize without damaging its operational effectiveness.

We view with concern any suggestion that the Service should undertake certain new programs rather than continue to concentrate its efforts where its task is clear, and where it performs well. Our section below on, " Protecting Science, Technology, and Economic Interests" deals with one facet of the question. We believe that any added emphasis on ``public safety" may further blur the line of demarcation between criminal intelligence and security intelligence operations. The Committee will be monitoring this matter closely.

The Director's Task Force Report is also interesting for what it does not say. The report does not call for restructuring in most areas to facilitate operations, nor for a reduction in the administrative structure. On the other hand, the report does make the case that the Service should examine the effectiveness of a broad range of activities. Whereas the report does not define the kinds of skills and capabilities new employees should have to master the challenges in the next five years and beyond, another study group within CSIS is presently looking at this area.

On balance, we consider that the Director's Task Force Report provides a competent analysis of the rapidly changing security and intelligence world in which Canada finds itself today.

(b) A Review of Traditional CI Threats in Light of Historic Political Changes

Long-Standing Threats to Canada

In 1990, we conducted a study entitled, ``East Bloc Investigations." We sought to determine whether the response of CSIS to the changing threat from that part of the world was appropriate. We found that CSIS had worked with decreased resources, had re-organised and reduced the section concerned and had, therefore, reduced investigations against the foreign intelligence services involved;[2] on the whole, however, the fabric and organisation of the CSIS Counter-Intelligence Branch had remained fundamentally unchanged.

In the Spring of 1993, when we began a similar review of CSIS operations, we found the CSIS Counter-Intelligence Branch adjusting to the volatile situation. It had, in the previous eighteen months, conceived two, new proposed organisation charts; the first, still-born due to the dramatically changing international threat and the resultant changes in priorities, the second, still surviving.

[2] The Service no longer specifically investigates most of these intelligence services.

We also reviewed the frankness of CSIS in passing information on these targets to its clients. Our concern was that only partial information might be passed, in order to protect intelligence and intelligence sources.

In fact, we did not find any discrepancies between what CSIS was telling its clients and what it knew and believed. We had some reservations, however, about their analyses. For example, it is perfectly fair to tell a client that, because of reductions in funding, there has been a decline in intelligence gathering activities; we question, however, whether these reductions are merely short term responses to economic problems.

General Observations

To some extent, the investigations against all target countries reviewed were affected by similar external forces:

- some members of the public, both in Canada and in allied nations, believe that the target countries are still using their intelligence capabilities against the interests of the West. Thus, CSIS continues to receive a heavy flow of unsolicited reports from Canadians concerning the suspicious activities of individuals or groups;

- CSIS continues to receive a significant number of requests from allied intelligence agencies. Many of these are routine checks on individuals;

- the volume of defectors and refugees has increased in the last few years, bringing additional information about intelligence activities in Canada. While, in fact, there may be less foreign intelligence activity in Canada today, we know more about it; and

- the Government, and particularly External Affairs, wants information about activities in some nations. Control over nuclear warheads, for example, is one important issue.

In our opinion, continuing intelligence activities by these nations, in the long-term view, make very little sense. All are in dire economic straits. All are seeking, to some degree, to become full members of the international community, and all want good relations with Canada.

CSIS managers believe that foreign intelligence activities are undergoing a fundamental shift in emphasis. They are moving from a focus on military capabilities and technologies towards economic competition and commercial technologies. CSIS officers believe that this shift in focus will change the nature of intelligence operations in the future.

Review of Foreign Intelligence Services

CSIS has been receiving defector information which, although dated in some cases, has allowed the Service to confirm an intelligence presence in Canada.

The level of activity of most foreign intelligence services in Canada remains low. The Service remarked, however, that all is not rosy because there are some areas of increased activity.

It is worth noting that not all former East Bloc states have formally disavowed the use of intelligence gathering activities abroad. For example, in July 1992, the Russian parliament signed the ``Law on Foreign Intelligence.'' This law confirms that Russia will collect intelligence outside of Russia, possibly, ``...using clandestine methods and means of intelligence activity.''

There are still foreign intelligence officers posted in Canada; the Service is looking at means of dealing with this problem.

We also reviewed available statistics on the extent of CSIS investigative activities. Data for 1992-93 is sketchy but, from the data available to us, we estimate that, in the case of one of the targets, CSIS has reduced activities by about 40-50%. We were informed that CSIS has also made significant cuts in investigations against other target countries.

Case Reviews

As part of the review, we also looked at randomly chosen investigations of individuals. Most CSIS investigations, we learned, involve foreign nationals.

We found that all the investigations we examined were justifiable under the *Act*. Reasons for investigation included: defector reports, records of prior intelligence activities in Canada, and reports from allies. In one case, a targeting authorization cited documents from the early 1980s; this has since been up-dated.

Conclusions

At this point, the status of foreign intelligence services is unclear. All are in transition.

In our review, we determined that there were no inconsistencies between what CSIS said and what it knew. CSIS was honest about the facts, although we did not agree with all of their assessments.

In our random audit of cases, we determined that all investigations were ``strictly necessary." In some cases, we found evidence of actual intelligence activity.

In the case of one target country, the nature of the threat, at the moment, appears limited. There is little evidence of actual intelligence activity. The nation in question, however, continues to send intelligence officers to Canada. We recommend that CSIS make further efforts, through External Affairs, to have these officers removed.

Although the situation is still fluid, we are of the opinion that the Service has responded appropriately to the changing international situation. The circumstances in each of the targeted countries may change dramatically in the next few years, and their intelligence activities will probably reflect those changes. CSIS will need to follow developments closely.

(c) Protecting Science, Technology, and Economic Interests

The prospect of a redirection of effort by CSIS towards the economic security area gives rise to a certain scepticism. As the Cold War threat vanishes and we look for resources to become available, another threat appears.

The general thrust of economic security activity is protection against the clandestine collection of important economic information, and the theft of proprietary information regarding either economic or technology assets.

Economic espionage is not new. Businesses and governments have long stolen economic or technical secrets. CSIS, and its predecessor agency, have always paid attention to theft of economic secrets in the context of their investigation of foreign intelligence officers, or theft of defence secrets. With Requirements — Technology Transfer (RTT), CSIS is focusing more sharply on non-traditional economic espionage.

Requirements — Technology Transfer was formed within CSIS in June 1991, to bring under one roof all organisational units involved in investigating illicit technology transfer. RTT does not focus solely on economic espionage; more than half of its effort is directed against weapons proliferation activities.

RTT is small, but can draw upon other branches within CSIS. In terms of its economic security role, it has two goals: to limit unauthorized transfer of technology by foreign interests, and to determine, ``...the sources, nature and extent..." of threats to Canadian security posed by the, ``...clandestine transfer of technology by foreign interests."

According to the National RTT Co-ordinator, RTT was formed partially as a response to the concerns of SIRC,[3] partially as a result of the realization that, with the end of the Cold War, ``...it was a new ball game..." in the economic espionage area, and partially due to a perception that economic espionage was increasing in response to intensifying trade competition.

RTT has an analysis component and an operational component. The analysis component is responsible for generating internal and external reports on technology transfer issues.[4] The operational component, ``...co-ordinates investigations, and liaises with the regions, HQ Branches, and the export control enforcement community." In addition, the operational component manages RTT's Liaison Awareness Program with the public and private sector. This program is RTT's major vehicle in identifying and assessing the technology transfer relating to economic security.

A premise of RTT is that both proliferation and economic espionage involve activities in areas where CSIS has had few contacts. To be effective in both areas, CSIS has now to develop a presence in the business and research communities. The Liaison Awareness Program is perceived as a basis for developing this link.

The Awareness Program is, ``...a Service-wide initiative aimed at sensitizing both the private and public sectors of the potential threats to their specific interests posed by the illegal or illicit transfer of technology." CSIS makes departments and companies aware of their vulnerability, and questions managers about their knowledge of any ``potential threats."

Who benefits? Smaller and middle-size firms often cannot afford specialized security advisors. CSIS may partially fill that gap. Larger firms, with security staffs, are often geared to inter-company espionage, rather than concerted efforts by state intelligence services.

---

[3] In 1989, the SIRC study, ``Protecting Scientific and Technological Assets: The Canadian Effort" recommended that:

* CSIS have a central co-ordinating body to direct investigations relating to technology loss and to examine different investigative and information gathering avenues;
* CSIS seek from government a mandate to assign a higher priority for investigation of threats to scientific and technological assets and, if necessary, seek additional resources;
* the government strengthen intelligence analysis, research and policy development; and
* that the government improve mechanisms for the co-ordination of, and for communication between, ``S&T participants" (External Affairs, National Defence, Customs and Excise, etc.).

[4] Prior to RTT, CSIS in general separated operational branches from intelligence analysis. Analysts were placed in Requirements - Analysis and Production.

For example, one company instructed employees travelling abroad to keep confidential papers in hotel safes. CSIS officers pointed out that such a procedure, perhaps adequate against competitors, is tantamount to handing the documents over to an interested foreign intelligence service.

The Liaison Awareness Program and RTT investigations relating to economic security are carried out under an ``issue-based'' Targeting Authorization and Review Committee (TARC) authority. The stated purpose of the authorization is to identify foreign government controlled individuals, groups, organisations or corporations:

> acquiring, or transferring illicitly or improperly from or through Canada or Canadian concerns abroad, those technologies of value to Canada's economic security; or
>
> providing support or assistance in the acquisition or transfer of such technology by illicit or improper means.

The economic security TARC authority sets parameters as to what may be investigated. The incidents must involve a foreign interest, an activity of a clandestine or deceptive nature, the potential acquisition of technology, and be of a significant detriment to Canada's economic security. The RTT Co-ordinator assured us that no investigative activities were undertaken unless the criteria were met.

The TARC authority directs that incidents are to be investigated in an incremental fashion to minimize the use of intrusive powers. The authority allows only the use of less intrusive investigative powers.

If officers believe that they need more intrusive powers to investigate, they must seek additional authority from TARC. Over 18 months, RTT has examined fewer than 100 incidents involving economic security, some dating back to 1981, and has yet to request any additional authority. In the same period, they have examined 250 incidents relating to weapons proliferation, and have requested a number of additional authorities.

RTT and the Liaison Awareness Program focus on eight identified key sectors. In our review, we examined the files of three sectors. We found that:

> there were current cases involving technology theft by foreign concerns;
>
> many of the incidents reviewed were untraceable, because they were too old, or because there was no evidence of any actual activity. For example, one incident involved an assertion by a manager that a competitor had his firm's confidential information;
>
> some incidents did not involve technology as much as business practices or information gathering; and
>
> some incidents were not clearly linked to activities by foreign governments.

The RTT Co-ordinator indicated that RTT is still in a formative stage, and that it is trying to build trust so that businessmen and researchers will come forward with current problems. He also stressed the distinction between investigation and collection of information.

From RTT administrative and liaison files, we also determined that:

> while RTT talks with such departments as Industry, Science and Technology, it has not conducted overall co-ordination of its efforts with them; and,
>
> based on a limited survey, the Liaison Awareness Program appears to be very well accepted by businessmen.

Conclusions

RTT is a new program, and the state of knowledge about economic espionage, especially in the post-Cold War environment, is limited. We have not examined RTT investigative activity directed against weapons proliferation.

In the past, governments have made use of economic espionage, and they are likely to do so in the future. At this point, however, no-one can measure the seriousness of the threat, nor whether it is increasing or decreasing.

We believe that RTT's activities, with respect to economic security, have had tangible benefits. Companies have become sensitized to security concerns, possibly averting losses of technology, and thus jobs. Valuable information has been collected about the techniques of economic espionage. Also, RTT efforts against economic espionage have complemented investigations against weapons proliferation.

RTT and the Liaison Awareness Program, however, appear to be focused on sectoral vulnerabilities, and not actual, ``threats to the security of Canada." Provision of awareness briefings seems to go beyond ``advice to government" as envisioned in the *Act*, although the program is arguably a means to an end. CSIS is also accumulating information that is not specifically linked to, ``threats to the security of Canada."

There are questions about the potential breadth of investigations. Although CSIS has focused its efforts on high tech firms, the information it gets and retains can touch on a host of business activities, such as financial practices. In addition, investigation of ``foreign interests'' can include investigation of the activities of foreign firms.

When we balanced the pros and cons, we did so mindful of the current environment of fiscal restraint.

We accept that the activities of foreign intelligence services in Canada must be investigated, whether they be acting against military or commercial targets. We are of the view that there is a role for CSIS in the areas of Canadian technology which bear directly upon national security. However, the protection of other technologies, which do not bear upon national security, should be the responsibility of the companies themselves.

3. Case Studies

(a) Al Turabi — Attack at the Ottawa Airport

On May 25, 1992 Dr. Hassan Abdallah Al-Turabi was assaulted at Ottawa International Airport, allegedly by a Sudanese refugee who is a martial arts expert. Al-Turabi, Chairman of the National Islamic Front in the Sudan, suffered serious injuries to the head and was hospitalized for several weeks. The media alleged that CSIS failed to provide security despite requests from the Sudanese Embassy, and that CSIS failed to communicate clearly or misinformed the RCMP.[5]

In carrying out our review, we were conscious of the mandate of CSIS in such situations. CSIS does not protect VIPs. This is a law enforcement role. Rather, the role of CSIS is to provide advice to Government about threats to VIPs during their stay in Canada.

Consequently, we reviewed whether CSIS advised the Government and law enforcement agencies in an effective manner in relation to the incident. Specifically we asked, did CSIS provide timely and complete information on Al-Turabi and possible threats to him while he was in Canada?

Our examination focused on Al-Turabi's visit to Canada, the events that led to the assault, and the activities of CSIS in relation to his personal security in Toronto and Ottawa.

The Arrival in Canada

Dr. Hassan Abdallah Al-Turabi is the religious leader of Sudan and is thus considered by many to be the de facto head of state in that country. Many observers of the African scene describe Al-Turabi as the main architect of the successful June 1989 coup in Sudan.

Dr. Al-Turabi arrived in Canada from the United States on May 24, 1992 for a three-day visit. His itinerary included meetings with External Affairs officials, Members of Parliament, the editorial boards of two Toronto newspapers, and major business interests in Toronto. He travelled on a Visitor's Visa.

Because he did not possess an Official's Visa, CSIS was not informed of his visit in advance. Furthermore, the committee which assesses the degree of protection needed for a particular visit, and on which CSIS sits as a member, was not convened.

Among other functions, this committee evaluates the need for a CSIS Threat Assessment.

[5] ``Bungled security alert blamed for attack at Ottawa airport," *The Ottawa Citizen*, Saturday June 27, 1992, B5.

On the day before Al-Turabi's arrival, the Toronto office of CSIS learned that the visit was to take place. The Service was also told that Al-Turabi could be a target of Sudanese dissidents. Consequently, for the next two days, CSIS sought to verify and expand on the preliminary information it had received.

Because CSIS HQ was unaware of Al-Turabi's impending visit, no assessment of threats to his safety had been prepared in advance. Information from other government agencies was not immediately available. When CSIS had compiled a more complete picture of the situation, it informed law enforcement officials of Al-Turabi's expected arrival.

When Al-Turabi arrived, a group of angry demonstrators forced him to seek refuge in his hotel at the airport. Police were present at the scene. Meanwhile, CSIS investigators continued to collect information which was then passed to federal agencies.

Events in Ottawa

CSIS learned that Al-Turabi was coming to Ottawa and immediately informed the local law enforcement officials.

Prior to his arrival in Ottawa, CSIS issued a Threat Assessment which concluded that the Service was, ``...currently unaware of any specific terrorist threats to Mr. Al-Turabi during his visit to Canada.'' The basis for this conclusion was the history of peaceful protests by the Sudanese community in Canada.

Al-Turabi arrived at Ottawa International Airport and went directly to his first appointment without incident.

Later that day, just prior to his departure, Al-Turabi, along with the other two members of his party, was attacked in the Ottawa International Airport. Two off-duty RCMP officers intervened and an alleged assailant was arrested. Al-Turabi was admitted to hospital, where he spent four weeks due to a medical complication.

CSIS found no evidence, after the assault, that the alleged assailant was part of an organized terrorist plot. CSIS had, in fact, notified law enforcement officials some four hours before the attack about Al-Turabi's departure plans.

Conclusions

The question we posed in this review was whether CSIS effectively fulfilled its role to advise the Government and the relevant law enforcement agencies; a role described by the McDonald Commission as:

> ``to provide those with executive responsibilities — police forces or government departments — with advance intelligence about threats to security, rather than to enforce security measures by executive actions of its own.''[6]

After learning of Al-Turabi's impending visit, CSIS spent the following days collecting information. CSIS Regions and police forces co-ordinated their efforts and regularly exchanged the information they possessed about threats to Al-Turabi. Notwithstanding the non-official status of Al-Turabi's visit, a Threat Assessment was produced and the Service gave it to federal agencies and the police.

While we understand that there were deficiencies elsewhere in the handling of this case, which have been subsequently corrected, we saw no information to corroborate the allegations, against CSIS, of mismanagement of the visit or the absence of, or inaccurate, communications to federal agencies, including the RCMP. On the contrary, our conclusion is that CSIS was effective in this case, consistent with its mandate to advise the Government and law enforcement agencies on the terrorist threat.

(b) Intelligence — Source Confidentiality

On June 17, 1992, the CBC reported that, ``...the names of secret government sources are routinely given to politicians.'' The report added that, under a 1986 Ministerial Direction, ``...successive Solicitors General have routinely approved operations involving sensitive sources and the Solicitor General is now told the identity of those sources.''

In our review, we searched for instances in which the Minister had, in fact, been given the identities of human sources. A review of files determined that, since 1984, there had been fewer than a dozen cases where the Minister had been provided with the identities of human sources. We examined each case. Only one case involved a Canadian citizen or landed immigrant. Most involved the resettlement of defectors, and all information given to the Minister was required to meet specific administrative needs, such as requirements under the *Immigration Act*.

In the single case involving a Canadian citizen, the Service was required to advise the Minister because of a potential impact on Canada's international relations.

[6] McDonald Commission, Second Report, Volume 1, *Freedom and Security Under the Law*, p. 421.

(c) Domestic Investigations

In fiscal year 1992-93, we reviewed the domestic investigations carried out by CSIS. Committee staff gathered and analyzed information on Service activities which took place during an 18 month period. Our research effort sought to determine whether the Service's information collection activities were within the law, Ministerial Direction, and CSIS policy. We also wanted to know whether the activities investigated by the Service represented threats to national security.

The objective of the CSIS investigations was to collect information with the potential to serve as an ``early warning'' alert regarding political violence.

For some early investigations, the Targeting Approval and Review Committee (TARC) restricted the investigative techniques to the collection of open information and liaison with other government departments. Other investigations involved the use of open sources and interviews of individuals, but did not permit the use of more intrusive measures.

TARC authorized all regions to collect information on issues with the potential to provoke violence. Incidents had already taken place. The Service was especially alert to report any activities that showed the links between extremists and the potential for political violence.

We noted that, in a small number of recent cases, the information the Service collected during investigations of certain individuals did not seem related to national security. Whereas we believe some investigations included law enforcement issues, lawful advocacy and dissent, we saw no evidence of activities under *section 2(c)* of the *CSIS Act*, ``threats to the security of Canada.'' The Service informed us, however, that these persons went beyond advocacy and dissent when they issued threats.

In other investigations, the approval of CSIS took place under *sections 12, 2(a)* and *(c)* of the *CSIS Act*. We found that the link with *section 2(a)* of the *Act* was less clear than the link with *2(c)*. The Service subsequently removed all references to *section 2(a)* in the amended targeting certificate.

During the early period of an investigation, the Service collected information on individuals which pertained more to criminal activities than to activities of a national security interest. Later in the investigation, CSIS focused its efforts more narrowly and demonstrated that the activities of this smaller number of persons did pose a threat to national security. The investigative powers in use then became more intrusive.

In one affidavit to the Court, CSIS did not mention that persons outside the scope of the investigation concerned could possibly have their communications intercepted. If provided with this information, the Court might have considered whether to impose more conditions on the interception process.

We concluded that, although another operation was lawful and took place under strict conditions, the Solicitor General should have been informed about this activity due to its sensitivity. When we looked at the information collected from the operation, we concluded that there was only a weak link to national security.

We also found that the Service briefly continued an operation after the requisite authority had expired. CSIS HQ conducted an investigation into the matter. After reviewing the circumstances of the case, we believe that no unlawful act took place. We understand that the Service has now instituted new procedures to avoid a repetition of the problem.

During the review of CSIS files, we discovered that certain operations approved in one year were authorized under two threat categories of the *CSIS Act*, one of which was incorrectly cited. We immediately alerted the Service to the error. CSIS returned the documents to the Court to point out the problem. The amendments were approved by a judge.

In one instance, CSIS stopped investigating a target after one year, but we were concerned about a message which suggested that the Service would continue to gather information on that person. We were subsequently advised that the Region did not make any inquiries about the person in question and, indeed, we did not see any. We will continue to monitor this case.

Conclusions

We observed that a few of the early investigations in 1991 involved the collection of some information which seemed, at best, on the periphery of the Service's mandate. As the investigation continued, the Service assessed that the potential for violence was increasing and it believed it could provide an overall analysis of the situation to federal government departments.

Much of the information in these investigations was collected by other agencies, and we wondered whether the Service was indeed contributing advice to Government that was not available elsewhere. That said, we understand that the Service had difficulty in identifying the appropriate targets early on, and so we do not take issue with the initially rather wide scope of the investigation.

We are concerned, however, about the manner in which CSIS implemented some of its recent investigations. We think that, initially, the Service sometimes cast its net too widely and included both those who warranted watching as well as persons not likely to engage in violence. Service staff pointed out that they consulted with the Solicitor General and, following that, they investigated only where there were reasonable grounds to suspect a threat.

In one case, we doubt seriously that the actions investigated were a national security matter. We agree that the activities were illegal, but they seemed to be entirely a law enforcement issue.

We understand the Director has suspended the investigation; we will review the Service's analysis of what it collected at the end of the targeting period, should the investigation resume.

(d) Middle-East Movements

Purpose of the Review

In 1992-93, we reviewed CSIS' investigations of a number of organisations which are linked to an area of the world known for its conflicts: the Middle-East. The organisations represent two culturally distinct ethnic groups. There are, however, factors which are common to them: they are sponsored or directed by a Middle-East group or government involved in that region's conflicts; they, or associated groups, are known for having used terrorism in the past; and they are suspected of having the potential to use violence in Canada.

Our review assessed whether the Counter-Terrorism Branch of CSIS, which was responsible for the investigations, presented a fair and balanced case to the Targeting and Approval and Review Committee (TARC). We also examined the use of the different investigative techniques authorized by that Committee. We were especially attentive to the exchanges of information with foreign security intelligence agencies.

Threats to National Security

We first assessed whether the Service had reasonable grounds to suspect threats to national security from the targets. We concluded that CSIS did have reasonable grounds to investigate most of the organisations, largely due to the actions of the parent organisations overseas.

We doubt, however, that one organisation targeted represented a threat to national security. Our view, based on the information we saw, is that the continuing investigation does not appear to take some recent developments into account. This investigation has been on-going for several years. A body of information exists to show that the group is one of the legitimate voices of a specific ethnic group. The intelligence produced by the Service does not prove otherwise.

In general, we believe that, in the instances we reviewed, the Counter-Terrorism Branch presented a fair and balanced case against most of the organisations and individuals. The submissions to TARC accurately reflected the information and intelligence collected by the investigators.

In one case, however, we believe that the Branch did not provide information in its possession to TARC; information which could have cast doubt, at the very least, on the level of the threat posed by the organisation. In another request for targeting, we saw no information to justify the continuation of the investigation against a person associated with one of the groups under CSIS scrutiny.

A small number of individuals under investigation were evidently operating on behalf of a foreign government. Their activities seemed to fall into the category of *section 2(b)* of the threats to Canada, in addition to *2(c)*, as targeted. The government in question has links to terrorism overseas, but the information collected by the Service appears to mainly be of a *2(b)* nature. We recommended that CSIS review the *CSIS Act* section under which these individuals are targeted.

Exchanges of Information with Foreign Agencies

When we looked at the information CSIS passed to foreign agencies, we were agreeably impressed with the caution exercised by the Service. Overall, we compliment the Service for its restrictions on exchanges with some foreign agencies known for their questionable human rights records.

However, we were initially concerned with one incident where CSIS communicated information to an allied agency about the activities of a Canadian citizen. Whereas the information sent overseas was not complete as to context, the additional documentation we saw demonstrated that there were grounds for the assumptions made by CSIS.

Advice to Government

Another dimension on which we assessed the Service's investigations was whether the Government of Canada was provided with timely and complete advice. CSIS produced valuable intelligence on the most extremist organisation we reviewed. The CSIS Reports and the Threat Assessments issued on that group provided the reader with a clear understanding of the situation. As for the other organisations, we saw relatively little intelligence communicated to the Government. In one case, we believe that the Service should have provided intelligence to its clients to differentiate the activities of one group, involved in legitimate activities, from the other group which is known for its propensity to use violence.

Further, we recommend that CSIS issue a report to its clients which clearly distinguishes between the activities of the two groups.

(e) The Asian Homeland Conflict

The Committee reviewed the activities of CSIS in relation to the implications for Canada of a conflict in an Asian country. The study covered the period from January 1990 to December 1992, a time which marked heightened concern over the activities of groups and individuals in Canada in support of the ethnically based insurgency against the government of that country.

Background

This homeland conflict is based on long-standing differences between the country's ethnic majority and an ethnic minority fighting for secession. The ensuing military operations, the terrorist attacks, the reported atrocities committed by both sides, and the displacement of members of the minority group from the majority controlled territory, has resulted in the exodus of a large number of refugees and migrants to western countries. The acts of violence carried out by extremists within the minority group have become progressively more serious in nature, including attacks against government forces and civilians, and assassinations of key political and military leaders. A significant number of individuals from this minority group currently reside in Canada. While not necessarily agreeing with the violent methods used by the extremists, a large proportion of community members in Canada support the goals of the extremists and consider them to have the greatest chance of realizing their political aspirations.

There is a network of support organisations in all countries hosting a large community of this ethnic group. In Canada, the support base is linked to the active participants in the conflict in the homeland. It doubles as an ethnic cultural and refugee support group. As well, there are a number of cultural organisations in Canada which, while not directly controlled by parties actually engaged in the conflict, participate in activities such as fund-raising. The proceeds go, in part, to support military operations and, in part, to provide humanitarian assistance to community members who have remained in their homeland.

CSIS, in accordance with its mandate, has investigated the situation to determine the extent to which these activities may constitute a threat to the security of Canada. A key goal of the enquiry was, of course, to ascertain whether terrorist activities, hitherto confined to the homeland and contiguous regions, could spread to Canada.

Review and Findings

In our review, we attempted to determine whether:

> the Service's investigations of the activities in support of the violence associated with this ethnic conflict were in compliance with legislation, Ministerial Direction, and CSIS policy and procedures;

the activities of the groups and individuals investigated by the Service represented threats to the security of Canada;

the collection of information by CSIS was strictly necessary and whether the investigative techniques were in proportion to the threats posed by the targets; and

the Service provided timely and complete information on the level of the threat to the Government of Canada.

We found that, during the period under review, the Service was investigating a number of individuals who were either supporting the violence in their homeland through fund raising or through other activities.

Targeting Decisions

We examined the Service's targeting authorizations and supporting information in respect of a representative cross section of the targeted individuals. We found that in each case the Service had sufficient grounds to conduct the investigation and to use the investigative methods authorized. We followed the course of the investigations in the files and were satisfied that the activities of the targeted individuals represented a threat to the security of Canada as defined in the *CSIS Act*. We saw nothing in the documents we examined to indicate that any targeting decision or any aspect of the investigations failed to comply with the relevant legislation.

Disclosure of Information on Canadian Citizens

We noted one example where the Service appeared to act without full and prudent regard for a Ministerial Directive. Part of the intent of that directive was to ensure that particular caution was exercised when providing information to countries that do not share Canada's respect for democratic or human values, especially where the information concerned Canadian citizens or permanent residents.

In this case, the Service communicated to a foreign agency the details of an individual's plans to travel to another country and, possibly, to meet with members of a group associated with terrorist activity.

The latter information was based solely on the uncorroborated beliefs of an informant, and was disclosed even though the Service was aware of reports of human rights abuses by security forces in that country. The individual's full identity was not known to the Service, neither was his citizenship status or any information on his previous involvement with terrorist activity, beyond his believed fund-raising on behalf of the extremist group engaged in the conflict.

We consider that the consequences for the individual and his family, had they been identified when they arrived in the foreign country, could have been extremely serious and that a potential tragedy was avoided more by good luck than good judgement. Fortunately, in this case, they were not identified and returned to Canada safely.

Investigative Methods

We saw that, in the vast majority of cases, the Service conducted its investigations in a restrained manner, considering and rejecting the more intrusive methods of investigation when the level of threat did not clearly justify them. As in other so-called ``homelands conflicts'' coming to the attention of the Service, there was an initial, necessary learning process so that investigators could understand the nature of the implications for Canada, and the level of threat that might be faced. A part of this learning process often includes a community interview program.

In this review, we saw reports of such an interview program being conducted in various cities in Canada. We found that it was a duly authorized investigative activity that complied with the law. We saw no reports of any complaints made by the community. In only one case did we notice what appeared to be an inappropriate use of the program by an investigator. This involved a CSIS officer's statements to an individual about a relative; it elicited great personal distress.

As we have noted in our previous Annual Report, a community interview program is designed to evaluate the presence and magnitude of a suspected threat to the security of Canada; individuals being questioned are not being investigated. Since neither the individual in this case nor his relative were targets, we consider that the investigator distorted the purpose of the program in pursuing this line of questioning.

Advice to Government

We examined a number of intelligence reports, which were issued by CSIS in the period under review, on this particular conflict and its implications for Canada. We found the reports to be an accurate representation of the information held by CSIS at the time of publication, and they provided a useful, if somewhat general, picture of the situation for use by other government departments and agencies.

The Service also provided information about specific individuals and activities to several Canadian government departments and agencies having lead responsibilities in areas of immigration, external relations, and law enforcement. We found that the dissemination of this information was appropriate and consistent with the Service's mandate.

Conclusions

The investigation by CSIS of activities associated with the threats arising from ``homelands conflicts'' is a difficult and complicated undertaking. When virtually an entire ethnic community in Canada appears to be solidly behind a resistance movement in its former homeland, and is also desperately concerned over the plight of relatives and friends there, the task becomes even more demanding.

The danger is that the investigative net can be spread too widely in these situations and can involve the use of intrusive techniques against people and organisations that cannot be justified by the threat they represent.

In this case, we found that the Service has successfully walked the fine line that the situation demands. Its investigations have clearly been concentrated on the principal individuals supporting the violence in the homeland and, in the period we reviewed, it has held back from the use of investigative techniques that were not proportionate to the threat.

It is fortunate for Canada that the participants in the conflict have so far chosen not to export their violent activities beyond their homeland and contiguous regions. Nevertheless, as the recent assassinations attributed to extremist members of the minority ethnic group have shown, terrorism continues to be a factor, and there is certainly the capability, and the potential, for the use of such tactics anywhere in the world, including Canada. Any activities in Canada which support the violence in their homeland must, therefore, continue to be monitored most carefully.

(f) Iranian Woman Deported

In early April 1993, the *Vancouver Sun* reported that the leader of the Mujahedin-E-Khalq (MEK)[7] in Canada had been deported to Britain.[8] After a Federal Court of Canada decision, an Adjudicator ordered her deportation pursuant to a National Security Certificate, stating that she was an inadmissible person in Canada pursuant to *paragraph 19(1)(g)* of the *Immigration Act*. We reviewed whether CSIS provided a fair, balanced and complete picture of the information and intelligence it found in its investigations. We have no mandate to review the Court's decision to deport this person.

The Service believed that the individual should be deported for two reasons: as leader, she was responsible for all of MEK's activities in Canada; and she participated in planning the attack

[7] The Mujahedin-E-Khalq (MEK) is an Islamic socialist organization which represents the main (Iranian) military opposition to the Islamic Republic of Iran. Part of the National Council of Resistance, MEK Headquarters are currently in Iraq.

[8] *Vancouver Sun*, 8 April 1993.

carried out by the MEK against the Iranian Embassy in Ottawa on April 5, 1992.[9] We reviewed the Service's investigation and found that the advice submitted accurately described the threat to the security of Canada.

We believe that CSIS performed its legal responsibilities appropriately.

(g) North African Immigrant

In the fall of 1992, the Ottawa media broadcast a story about a North African immigrant who allegedly entered Canada on a fraudulently obtained American passport in 1982, and was granted landed immigrant status. The story referred to ``intelligence documents'' from a foreign agency which claimed the immigrant was a former diplomat and an intelligence agent. A recently published book claimed, furthermore, that the subject was one of the suspects in the 1988 bombing of the Pan American flight which crashed at Lockerbie, Scotland.

We reviewed the CSIS documentation and observed that most of the information relevant to this case was derived from domestic and foreign agencies. The case has been investigated by several security and law enforcement agencies in the West. Most of the immigrant's offences, both alleged and actual, reportedly took place prior to the creation of CSIS.

We examined the most serious allegations, which linked the landed immigrant to the Pan American bombing. The information from the criminal and security investigations which we reviewed did not support allegations that the subject was involved in the Pan American crash.

(h) Sheik Rahman's Alleged Visit to Ottawa

In April 1993, an Ottawa newspaper[10] claimed that Sheik Omar Abdel Rahman entered Canada illegally in the Fall of 1992. He was portrayed in the media as the ``spiritual leader'' of the extremists who were involved in the bombing of the World Trade Centre in New York on February 26, 1993. The newspaper alleged that the Service did not do its job when it let the Sheik come to Ottawa. We took note of the newspaper's allegations and used the opportunity to review the role of CSIS in prohibiting terrorists from entering Canada.

---

[9] SIRC Annual Report, 1991-92, pages 15-18.

[10] *Le Droit*, 15 April 1993.

Immigration and Customs officers are the first line of defence against undesirable foreign nationals trying to enter Canada. CSIS has no powers of arrest and it cannot physically stop persons from entering the country. The role of CSIS is to provide warnings to Immigration and Customs officials. One of the tools the Service uses to perform this function is the Enforcement Information Index.

This Index is an automated data base which contains the names of persons who are inadmissible to Canada for various reasons. It is administered by Immigration Canada. The Service may add names to the list when it suspects a foreign national of being associated with a terrorist group. The Index includes biographical data, and the reasons why he or she is to be kept out of the country.

In the specific case of Sheik Omar Abdel Rahman, the Service provided advice to Immigration Canada almost two years before his alleged visit to Ottawa. We, therefore, feel that CSIS performed its duties appropriately.

(i) The Quebec Delegation in Paris

Last year, we reported that we had conducted a preliminary review of allegations that CSIS had spied on La Délégation générale du Québec à Paris.[11] At that time, our review showed no evidence of any such operation. Since then, we have completed our investigation. We wrote to the Solicitor General to inform him of our conclusion that there is no substance to the allegations of CSIS intelligence activities against the Quebec Government delegation in Paris.

[11] SIRC Annual Report 1991-92, page 36.

4. Other CSIS Operations

(a) Arrangements with other Departments and Governments

Foreign Arrangements

In fiscal year 1992-93, CSIS received approval from the Solicitor General for eight new or expanded foreign arrangements. We note with great interest that almost all of the new arrangements involve varying degrees of co-operation with some foreign agencies in what was previously described as the East Bloc. CSIS is moving cautiously in this area and we see the arrangements as representative of both the political maturity of CSIS and an acknowledgement that a number of formerly autocratic regimes have undergone major political reforms.

The year also saw the termination of two arrangements with foreign security agencies which have been, or are in the process of being, dismantled.

In our 1991-92 annual report, we mentioned that the Minister approved an arrangement, subject to the foreign agency meeting certain conditions. Late in 1992-93, this foreign agency accepted the Solicitor General's conditions and CSIS proceeded to implement this arrangement. We will monitor the information exchanged under this new agreement.

Domestic Arrangements

During 1991-92, the Service concluded one Memorandum of Understanding (MOU), an agreement between Transport Canada and the Service. The agreement formalizes procedures for co-operation and exchanges of information between CSIS, the Department of Transport regional security officers, and security officers at 11 major airports in Canada. Negotiations on this agreement began in April 1986, but were held up by legal and administrative concerns, and by other organisational priorities within CSIS.

(b) Exchanges of Information with Foreign and Domestic Agencies

Domestic Exchanges of Information

Under *section 38(a)(iii)* of the *CSIS Act*, the Committee is to review arrangements for exchanges of information and co-operation under *section 13* and *section 17* of the *Act*. In particular, the Committee is to, ``...monitor the provision of information and intelligence pursuant to those arrangements."

Each year, the Committee audits domestic exchanges of information under *section 17* of the *Act*. As yet, there are no agreements under *section 13*(security assessments). We audit the actual

exchanges taking place over the last year, and conduct reviews at CSIS regional offices.

Domestic exchanges cover the provision and receipt of information from federal departments and agencies, provincial departments and agencies, the RCMP, and other police forces. All exchanges are documented and tagged for retrieval using the Service's computerized data base.

We began this year's audit by examining how well domestic arrangements, and the system for logging exchanges, were working. According to participants, and from what we saw, there are no problems. Appropriate information is flowing smoothly between CSIS, police forces and governments. With a few possible exceptions due to ``human error,'' the CSIS logging system is comprehensive and accurate.

We examined whether CSIS is acquiring sensitive information, such as medical or welfare information. We found no case where such information was obtained. We scrutinized closely any information obtained from departments or agencies having sensitive information.

We reviewed the acquisition of information from federal departments. The Service must follow a prescribed formula to obtain information that was not collected for security intelligence purposes. With the exception of information volunteered by a federal department official in one case, we found no cases where information had been inappropriately obtained.

In the course of our review, we examined about 1,100 exchanges and found little of concern. In making some exchanges, the Service may not be complying with the letter of a *section 17* arrangement. Also, in some cases, CSIS may periodically be given information about protests that are unlikely to involve violence. In addition, in some cases, CSIS obtains and retains general information that seems not to concern ``threats to the security of Canada.''

As a special aside, we also looked at dissemination of information under *section 19* of the *Act*. The Service, in providing information under *section 17*, must also meet the tests of *section 19*. We examined an area of possible concern: the dissemination of information by CSIS during awareness briefings to private firms, concerning technology transfer. We did find a few statements touching on operational information, but determined that the information was public knowledge. Because of the weight given to Service assessments, we suggested that officers clarify the public origins of any information they might give.

Under *section 19 (2)(d)* of the *CSIS Act*, the Service can release information to Ministers of the Crown or ``persons in the public service of Canada,'' with the approval of the Minister if the public interest clearly outweighs considerations for invasion of privacy. According to new policy in the CSIS Operational Manual, the Minister, or the Service as his agent, can also make ``special

disclosures" to Members of Parliament, provincial or municipal officials, or the private sector, ``...where the Service believes that the national interest warrants the disclosure of security information or intelligence outside the Government of Canada."

The Solicitor General, in the public interest, may from time to time have to release, or have the Service release, security intelligence information through ``special disclosures." We recommended that ``special disclosures" be such as to meet the same tests as *19(2)(d)* of the *CSIS Act*, including notification of the Committee.

Foreign Exchanges of Information

During 1992-93, the Committee reviewed samples of correspondence which CSIS released to foreign agencies. We undertook the study to ensure that there was no excessive or unnecessary use of powers by the Service. The review was conducted pursuant to *section 38(a)(iii)* of the CSIS *Act* whereby we are to review arrangements entered into by the Service and monitor the provision of information and intelligence pursuant to those arrangements.

In addition to examining the documentation at CSIS Headquarters, SIRC also conducted reviews at two Security Liaison Officer (SLO) posts to ensure that the material sampled at HQ was representative of the information provided by the Service under foreign arrangements during 1992-93. We also looked at a new policy which governs the foreign exchanges of the Service.

At CSIS HQ and at the posts, we were particularly interested in the controls in place for the provision of information, and whether CSIS placed restrictions on the release of certain types of information to foreign agencies. We examined all exchanges with the posts and we selected nearly 200 cases for intensive review.

This audit differed from previous ones in that we used the new computer-based tracking system, a welcome new development, to account for what they send overseas. We used it to ensure that the documents that we selected for intensive examination were representative of the material CSIS disseminates to foreign agencies. We think the new sampling system works well.

In fiscal year 1992-93, CSIS produced several new policy instruments for foreign liaison. The most important one was the policy for disclosing operational information and intelligence. For the first time, CSIS placed in policy what was previously communicated in bits and pieces to employees through an assortment of documents, as well as via the oral tradition in the Service. Consequently, we think the new document is significant in that the basic principles for information exchanges are clearly set out. These principles include concern for the safety of individuals and the concept of providing only what is necessary.

One key policy area, in which SIRC has been interested for several years, relates to information on Canadians. The Service has specified for the first time in the Operational Manual that CSIS staff should pay particular attention to the potential uses to which foreign agencies will put information on Canadians. We note, however, that a Ministerial Direction urges caution in sharing information with foreign agencies on Canadians and Landed Immigrants. The new CSIS policy does not include the latter category.

While the new disclosure chapter addresses many policy gaps we have pointed to in the past, several issues remain. A vehicle for communicating warnings to staff about the release of information to certain foreign agencies has yet to be developed. We also await the new chapters in the Administration and the Operational Manuals which will replace the foreign liaison manuals. These are urgent requirements.

After we reviewed the files at CSIS Headquarters and at the two Posts, and after having interviewed CSIS employees and others, we concluded that the current foreign liaison system is working well. Communications between the operational branches in Ottawa and the SLOs seem to have substantially improved after the uncertainty generated by the demise of the Foreign Liaison Branch in 1989-90.

We are concerned about security screening requests and other operational exchanges sent to states with poor human rights records. Adding to that concern, was the fact that the intelligence organisation, in at least one state, may not adequately safeguard the small amount of screening information that CSIS does send it.

We understand, however, that the Service does not provide much or, in some cases, any sensitive information to a number of states with which it has foreign arrangements, including the intelligence organisation noted above.

CSIS requires that foreign agencies provide an explanation each time they ask the Service for security traces. Requests from one foreign agency often lacked this important information. This is contrary to policy and, because CSIS may not correctly guess the reason for a foreign agency's request, increases the possibility that information may be inappropriately disseminated.

We believe the Service did a commendable job in not providing information to a foreign agency when it asked for traces on two legitimate institutions in Canada. In another investigation of one individual, however, CSIS provided information to a foreign agency which the Service obtained from a source who unknowingly breached the confidentiality requirements of a private Canadian company under federal regulation.

In conclusion, the SIRC review revealed that the information exchanges we examined conformed to the foreign arrangements in place. The control provisions at the posts and at CSIS HQ were similarly satisfactory. Aside from the exceptions described above, we found that the information exchanges were consistent with the requirements set out in statute and policy.

(c) Warrant Statistics

Under the *CSIS Act*, the Federal Court may approve the use of certain intrusive powers, such as telephone intercepts. The Director seeks these powers through warrants.

Prior to the *CSIS Act*, the Government published statistics on the use of warrants pursuant to the *Official Secrets Act*. We have now taken over the task. The Committee obtains the statistics for publication from CSIS. The CSIS data is as follows:

Table 1. New and Renewed Warrants

	1990-91	1991-92	1992-93
New Warrants Granted	27	39	32
Warrants Renewed	51	73	115
Total	78	112	147

``Renewed Warrants" includes warrants renewed on termination and warrants returned to the courts for amendment. Warrants can be for one year, or for a shorter period. Despite the increase in warrants (35), the number of targets, as of March 31st, has decreased over the previous year.

We attribute the increase in warrants to changing legal requirements. From our own data, we can state that the statistics do not indicate any increase in CSIS investigative activities.

The Committee also compiles its own statistics based on a review of actual warrants. According to our data, the number of Canadians or Landed Immigrants named in warrants remains in the same order of magnitude as last year; hundreds, not thousands. There has been a significant decrease in activity in the CI area.

Our compilation and analysis of warrant statistics has proved challenging. Data can change from year to year for reasons not relating to activity, including changing legal requirements and amended procedures. This makes comparisons difficult.

(d) Counter-Terrorism (CT) Branch

The Counter-Terrorism Program

The fundamental role of the Branch is to provide advance warning concerning potential threats to the security of Canada, not merely to react after the fact. The two constituencies for the early warning advice, in the Service's eyes, are the Government of Canada and the general public.

As CSIS noted in its public report, ``An effective Counter-Terrorism program aimed at public safety will remain the Service's first priority."[12] This priority means the Service must remain alert to a series of threats which include terrorism arising from political or social ideologies, ethnic nationalism, religious extremism, and other terrorists with or without state sponsors. This is a formidable task, and the consequences of failure are significant.

The Director's Task Force proposals hardly affect the Counter-Terrorism Branch. Neither the structure nor the programs were seen to require significant changes. Senior management in the Branch moves its personnel as required, in order to respond to developing new threats or changes to old ones.

In 1992-93, we reviewed various facets of the CT Branch's operations. We have described them in Chapter 3, in the sections dealing with: The Asian Homeland Conflict, Domestic Investigations, Middle-East Movements, Al Turabi — Attack at the Ottawa Airport, and Iranian Woman Deported.

Threat Assessments

CSIS alerts other departments and agencies in the federal government to actual and potential threats through the threat assessments it produces. During the 1992-93 fiscal year, the Threat Assessment Unit produced a total of 1029 threat assessments; a 20% increase over the previous year.

Research Studies

This marks the fourth year that we have raised the issue of the resources devoted to the research function in the Counter-Terrorism Branch. Simply put, we observed that the unit has generally done good work in providing assistance to the operational intelligence function and could do more, if its staff were not also engaged in briefings. In this section, we describe a document we reviewed in 1992-93, which was produced by the Unit.

[12] Canadian Security Intelligence Service, *CSIS Public Report 1992*, Ottawa, 1993.

At the Director's request, the Branch produced a functional analysis of the Service's community interview programs. In these programs, CSIS investigators interview leaders and individuals within a specific ethnic community. The purpose is to gather information about the reaction within the community to certain events, such as conflicts in the homeland.

The paper evaluated the programs that the Service conducted between 1990 and 1992. We examined the report and, in our opinion, the analyses and the guidelines for these programs are both logical and practical. With one exception, we think that adherence to these rules would have prevented the problems we noted in our review last year of the community interview program arising from the Gulf War. Our principal concern is that the guidelines fail to give guidance on what is appropriate, and what is not appropriate, information to collect.

We have learned that the Service is incorporating the community interview program into a new section in its Operational Manual.

(e) Counter-Intelligence (CI) Branch

1992-93 has been a year of soul-searching and redirection for the Counter-Intelligence Branch of CSIS. The old system, based on national desks, has been partially replaced with one built on ``Collection Analysis Programs'' focusing on issues. The first four priorities are investigations involving:

> Proliferation of Destabilizing Technologies/Technology Transfer;
>
> Security and Integrity of Government Property, Personnel, and Assets;
>
> Foreign Interference/Influence; and
>
> Espionage General, including undeclared Intelligence Service presence in Canada.

The Branch is living through a period of immense change and transition. It is coping with down-sizing, and employees, therefore, are feeling somewhat unsettled.

Change is pervasive and affects all aspects of the Branch's operations. More emphasis is being placed on ``consumer'' requirements and meeting the information needs of federal departments and agencies. New investigative approaches are being used, including greater use of community interviews. The emphasis is shifting from the collection of information about traditional targets to new areas of security intelligence interest which are evolving as the world situation changes.

Last year, we mentioned the establishment of a new body, Requirements-Technology Transfer. This group co-ordinates investigations concerning the proliferation of destabilizing technologies, and the theft of scientific and technological secrets. The group is small. Emphasis to date has been on ``proliferation'' investigations and on providing awareness briefings to governments, educational bodies, and high technology firms. Further discussion on investigations involving the economic security issue can be found in Chapter 2.

(f) Analysis and Production Branch (RAP)

In our annual report last year, we reported on the structural changes to the Analysis and Production Branch. We noted the establishment of a new functional unit to provide strategic and issues-oriented analyses concerning: technology transfer, economic espionage, and several other issues which CSIS deemed to have the potential to constitute threats to the national security of this country.

In large measure, the Branch structure has not changed since last year, although those RAP analysts who were responsible for Science and Technology were placed in the Technology Transfer Branch. Several years ago, we questioned the wisdom of having RAP analysts separated from their colleagues in Production. The Service ultimately removed the analysts from the operational branches to create a more effective and responsive production branch. We will be interested to learn if this recent secondment of the analysts to the operational branch is permanent, and whether the effectiveness of the Branch is diminished as a result.

We also noted that the Branch had increased its capability to assess economic security issues and had formed a new unit to collaborate on a closer basis with those federal government departments which receive the CSIS analyses.

With regard to RAP's liaison with its clients, we were advised that an ``environmental scan'' was conducted by CSIS to survey the issues of concern to the other departments and agencies with which the Branch does business. The scan, or review, dealt with geopolitical issues such as the break-up of the former East Bloc, conflicts around the globe, and economic and domestic issues.

Commentary

In the year under review, the Analysis and Production Branch published ten issues of Commentary. This publication addresses broad concepts and strategic situations. The work is of a high quality, and we would like to congratulate the Service on its achievement in this area. The studies are not classified and cover the following topics:

1. Religion and the Dilemmas of Power in Iran
2. Militant Activism and the Issue of Animal Rights
3. Egypt and Iran: Regional Rivals and Diplomatic Odds

4. Cuba: Real Problems and Uncertain Prospects
5. Succeeding the KGB: Russian Internal Security in Transition
6. A Change of Government in Israel: New Promise for the Peace Process?
7. Democracy, Neo-authoritarianism and International Security
8. Central Asians: Recruits for Revolutionary Islam
9. The Commonwealth of Independent States: Still Crawling
10. The Tortuous Road to Peace in the Balkans.

(g) Files

File Management

In fiscal year 1992-93, CSIS reviewed a grand total of 122,771 files, destroyed 112,448 of them and sent 6,873 of historical value to the National Archives. The rest have been reclassified into other file categories. Access to most of these files is restricted, and their review by analysts or investigators requires senior management approval.

As we reported in our last Annual Report, we again observed that CSIS drastically reduced the number of remaining counter-subversion files — this year by almost 80%. We also noted a considerable decrease in the number of files on individuals from the former East Bloc.

We noted a substantial drop in the number of file inquiries from outside agencies. These agencies ask for information about persons who have been resident in Canada at one time or another. The requests are separate from the security screening activities of the Service.

On the other side of the ledger, we noted increases in the number of immigration and refugee screening files. The number of files to screen applicants for government positions also increased.

Several new categories of files represent the changed emphasis of the Service's activities. These include the transfer of technology, proliferation concerns, and information exchanges with the public and private sectors.

Comparable to the previous year, CSIS opened approximately 85,000 files in 1992-93. As before, the vast majority were administrative and screening files such as: immigration, citizenship, government security checks, and checks for foreign agencies.

Files Inherited from the RCMP Security Service

We have continued to monitor the status of the 510,000 files which CSIS inherited from the RCMP in 1984. During fiscal year 1992-93, the Service reviewed 64,069 files and retained 6,616

of them. The remainder were sent to National Archives or were destroyed. The Service estimates that 104,000 of the files from the RCMP remain to be reviewed.

In summary, the disposition of these files was as follows:

Total Reviewed	64,069
Destroyed	52,068
Retained	6,616
National Archives	5,385

File Policies and Procedures

In 1988, the Solicitor General instructed CSIS to develop and implement a framework of policies and procedures to govern the management of file holdings. In previous years, the Service partially complied with the ministerial direction by producing operational policies to govern the collection of information and the retention of that information in files.

In the Fall of 1992, the Service published a policy which created a framework to manage all information holdings. The new directive consolidates the requirements of several federal Acts, including the *Access to Information Act, Privacy Act, National Archives Act,* and the Government Security Policy.

(h) Internal Security

The Committee has always had a concern about the ability of CSIS, as an Intelligence Service, to protect itself from breaches of security. In last year's report, we indicated that, ``...there have been some weaknesses in the past, perhaps, in handling internal security matters." adding that, ``The Service has addressed these weaknesses." Subsequent examinations have revealed that we may have underestimated the weaknesses, and overestimated the measures taken to correct them. The Committee has expressed its concerns to the Director and we will continue to monitor this area.

(i) Foreign Intelligence

Under *section 16* of the *Act*, the Service may assist in the collection of information concerning the defence of Canada and the conduct of the international affairs of Canada. This information is termed, ``Foreign Intelligence." Collection must be effected in Canada, and cannot be directed

against a Canadian citizen, landed immigrant or federally or provincially incorporated corporation.

Under the *Act*, the role of SIRC is limited. We examine any requests for assistance from the Minister of Defence or the Minister for External Affairs. Further, we examine any security intelligence ``spin off'' and we examine any retention by CSIS of information about Canadians.

As part of our mandate, we also review the flow of any ``Foreign Intelligence'' into CSIS from the Communications Security Establishment (CSE). We ensure that any information retained by CSIS is genuine security-intelligence ``spin-off'' required for legitimate investigations, and that it fully meets the standards set by *section 12* of the *Act*.

(j) Statistics on Operational Activities

Under the *CSIS Act*, the Committee is to, ``...compile and analyze'' statistics, ``...on the operational activities of the Service.''

Our review covers a number of areas. We examine person years, strength statistics, and financial data. We compile statistics on the use of warrants and other investigative techniques. Also, we examine a number of other statistics, such as security screening data, targeting authorizations, Ministerial Directions, and files.

We compare data by region, target groupings, and other categories. If the data raises questions, we pursue them with CSIS. Sometimes the questions concern the effort being expended against particular targets.

In 1989, the Solicitor General introduced ``National Requirements.'' These are basically the goals of CSIS investigations. In early 1993, we learned that CSIS would begin allocating person-years to each of the five ``National Requirements.'' One of the requirements, for example, is to report on ``foreign interference.''

Under the old system, person year statistics were generally classified in such a way that they could be identified with actual targets. The new classification categories will obscure this connection and make our analyses more difficult. This problem will be further compounded as the new classifications are applied to other statistics compiled by the Service. We will continue to analyze their statistics, along with other information we gather, in order to produce meaningful data for our use.

5. Complaints

Introduction

During the 1992-93 fiscal year, we received 29 new complaints. Most were made under *section 41* of the *CSIS Act*; they were complaints about, ``any act or thing done by the Service."

Table 2. Complaints, April 1, 1992 to March 31, 1993

	New Complaints	Carried Over from 1991-92	Closed in 1992-93	Carried Over to 1993-94
Security Clearance	2	0	0	2
Citizenship	0	0	0	0
Immigration	0	1	0	1
Human Rights	0	0	0	0
Section 41	27*	3	25	5
Total	29	4	25	8

* Of the 27 complaints, 9 were outside the Committee's jurisdiction.

Of the remaining 18 (27 minus 9), four individuals believed that they were the subject of undue surveillance by the Service. Five individuals complained about the length of time it took to receive their security clearance for immigration purposes. They were advised to contact CSIS, and were satisfied with the Director's response. Two were general complaints against the Service regarding operational activities and we were able to satisfy these complaints. Four withdrew their complaints without providing explanations. The remaining three were fully investigated by the Committee.

Mandate

Section 41 of the *CSIS Act* directs the Committee to investigate complaints made by ``any person'' with respect to ``any act or thing done by the Service.'' Before the Committee investigates, however, two conditions must be met:

- the complainant must have first complained to the Director and have not received a response within a period of time that the Committee considers reasonable, or the complainant must be dissatisfied with the Director's response; and

- the Committee must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

Furthermore, under *subsection 41(2)*, the Committee cannot investigate a complaint that can be channelled through another grievance procedure under the *CSIS Act* or the *Public Service Staff Relations Act.*

This year, many *section 41* complaints involved persons who believed that they were being subject to undue surveillance by CSIS. We chose to comply with the policy of the Service, neither to confirm nor deny that a person is a target. However, we thoroughly investigated the allegations to ensure that:

- the Service had not used and is not using its powers unreasonably or unnecessarily; and

- the Service is performing its duties and functions effectively, efficiently and legally.

Complaints about Security Clearances

Under *section 42* of the *Act*, a complaint can be made to the Committee by:

- a person refused federal employment because a security clearance has been denied;

- a federal employee who is dismissed, demoted or transferred, or denied a promotion or transfer for the same reason; and

- anyone refused a contract to supply goods and services to the government for the same reason.

We received two complaints about security clearances during 1992-93. The first complaint involved an individual, formerly employed with the Department of National Defence, who complained about the Department's downgrading of a security clearance. Due to the downgrade

from a level III to a level I clearance, the individual was forced to resign from the Defence Department and is appealing this decision with SIRC.

Another complaint involved an employee of the Service whose security clearance was revoked, leading to dismissal. This individual is appealing the Service's decision.

Citizenship, Immigration, and Human Rights Complaints

We received one complaint in 1992-93 concerning a person designated as inadmissible under the *Immigration Act*. No complaints were received about refusals of citizenship, and the Canadian Human Rights Commission has not referred any cases to us in the last several years.

6. Security Screening

Introduction

The Service's legal framework for the Security Screening program is provided in the *CSIS Act*, the *Immigration Act*, the *Citizenship Act*, Ministerial Directions pertaining to the provision of security assessments, and the Government Security Policy.

New Development

As the majority of screening cases the Service handles have a set format and a standard method of processing, it was clear that the security screening program could benefit from automation. Significant progress has been made by the Service in developing the electronic processing of security screening requests as a base for its program internally, and in interfacing with its clients. Significant cost savings will be realized by dealing with requests for levels I and II clearances in a paperless fashion.

An integral part of implementing this automated security screening system with departments is ``profiling." This involves tailoring the automated indices check to flag particular departmental concerns, based on a threat and risk assessment.

The system is working effectively, and now provides a search capacity which enables users to rapidly locate and track the details of any particular case.

Government Security Screening

The Service's average processing times, as of March 31, 1993, were 15 days for Level I (Confidential), 19 days for Level II (Secret) and 90 days for Level III (Top Secret).

Recent changes in the world political situation have been enormous; consequently, the Service has been pursuing with the Treasury Board Policy Centre a major review of Treasury Board Government Security Policies (Physical, Electronic Data Processing [EDP], and Personnel) created in the mid 1980s, during the Cold War. This review is vital in order to reflect the changing challenges faced by the Government in protecting its intelligence assets.

In the view of the Service, the proposed changes to the Personnel Screening Standards in the Government Security Policy (GSP) will have only a slight effect on the risk to government assets, but the accompanying savings in person-years and dollars will be significant.

Immigration and Citizenship Screening

During fiscal year 1992-93, the Service processed approximately 72,000 Immigration and Citizenship requests.

The Service was able to maintain, on average, a 90 calendar day turnaround time for processing immigration applications. However, as in previous years, a small percentage of the total number of cases received were complex and required extended processing times.

A comprehensive assessment of a program to streamline immigration procedures outside Canada — profiling — is in process and should be completed by the end of the Fall of 1993.

Refugee Determination Backlog

The Refugee Determination Backlog was officially terminated at the end of March 1993.

Immigration has advised the Service that any cases forwarded for processing after March 31, 1993 will be submitted under the Refugee Ongoing Program. There are approximately 1,500 applications yet to process but Immigration could not, at this point, inform the Service how many would be sent to them for processing.

7. Regional Audits

Scope

Regional audits take the form of a series of reviews which cover warrants, surveillance, targeting authorization, and other matters. The reviews give us a chance to examine how Ministerial Directions and CSIS policy actually affect the day-to-day work of investigators in the field. Each study includes quantitative data on the extent of a Service activity. We often compare the regional with the national data, and data from the current year with that from prior years.

The regional audits commence immediately after the end of the fiscal year and the information they produce is, therefore, the most current we have.[13]

The audits tend to be more holistic than specific. They go beyond examining individual cases or investigative tools. For example, we examine not just how warrants work but also the targeting authorizations upon which the warrants are based, the use of other investigative tools, and any decision-making involving the Minister.

Targeting

Essentially, the review of targeting covers the validity of targeting decisions. Some decisions are made directly by the Targeting and Approval Review Committee(TARC), chaired by the Director. Others, generally for less intrusive investigations, are made by Operational Directors General, with authority delegated by TARC.

All of the targeting decisions we examined were based on reasonable grounds to suspect a threat to the security of Canada. We were also satisfied that regional investigators strictly followed the parameters of targeting policy, and that the investigative means chosen were proportionate to the magnitude of the threat posed. However, we sometimes thought that the documents cited inappropriate parts of *section 2* of the *CSIS Act* (the definition of threats to the security of Canada), or used them imprecisely.

In one case, a technology transfer investigation, the Service cited *section 2(c)* of the *Act* (serious violence) as the basis for targeting. The request for targeting authorization and the instruction provided to investigators, however, did not contain any reference to activities falling under *2(c)*.

In another case, the Service made use of *2(c)* (serious violence) and *2(a)* (sabotage) to justify investigations involving protests and possible serious violence. The investigation was justified,

[13] The formal findings, however, are only published in the following year's annual report.

but the use of the term ``sabotage'' in this case stretched its meaning too far. The Service dropped the reference to *2(a)* in subsequent authorizations.

Warrants

Warrant affidavits can be extremely lengthy and include a great deal of minor detail. A retired judge addressed this problem in his report, which we describe in Chapter 8.

Each year, we review the facts contained in warrant affidavits. The Service, in preparing affidavits submitted to the Federal Judge, footnotes each significant fact, citing a specific document or report. We examine the documents and reports cited to ensure that they do indeed support the facts. Where necessary, we examine the accuracy of the documents or reports themselves. We also generally evaluate the affidavit to ensure that the facts provide a balanced view.

Our review identified minor discrepancies, but no major problems of fact or interpretation.

In one case, officers attempting to modify, on an urgent basis, a very lengthy affidavit may have inadvertently confused pertinent references.

We also found that many facts were not confirmed by the associated supporting documents; we did, however, locate the correct supporting documentation.

We examined information obtained from warrants and, in particular, the protection given to information which might come from communications between a solicitor and his/her client. We are satisfied that this is being handled well.

Surveillance

Of all the different activities in which the staff of CSIS are required to participate, surveillance, being the most difficult and sensitive, is the closest to being an art. Canada enjoys a high international reputation in this field of intelligence.

We have no discomfort with the level of authority used here by the Service but, as in previous years, we have noted the large amount of information gathered in the course of these surveillance operations. We will continue to watch this area.

Sensitive Operations

We review sensitive operations authorized by the Minister, and the use of certain sensitive investigative tools. Current Ministerial Direction, for example, requires that the Minister

personally authorize campus investigations and joint operations involving allied intelligence services.

In one investigation, we examined an operation touching on the possible theft of technology and intellectual property. We noted that no case had been made formally that there were, in fact, definite indications of actual or potential intelligence activities.

8. Review of General Matters

(a) Ministerial Direction and CSIS Instruction

Under *section 38(a)(ii)* of the *CSIS Act*, the Committee is to review Directions issued under *section 6(2)* of the *Act*. We examine all new Directions as soon as they are issued. Also, in the course of our review of actual cases, we examine the adequacy of the Ministerial Direction and the degree to which it is observed in practice. Instructions in the ``CSIS Operational Manual," often based on Ministerial Direction, are similarly reviewed.

This year, we received three new Directions. The first cancelled 12 archaic Directions deemed to be, ``...outdated, redundant, or without further practical effect." The second dealt with operational co-operation with allied intelligence services in Canada. The last specified consultation requirements in carrying out certain types of covert operations.

(b) Operational Manual

This year, we also received five significant amendments to the ``CSIS Operational Manual." One section concerned policy for the disclosure of information obtained in the course of investigations, and specifically authorized the disclosure of information by the Service as the agent of the Minister. Another concerned the processing of information obtained under warrants, including the protection of solicitor/client information. A new section on targeting changed the targeting categories used, provided for the handling of open information, and defined ``environmental scanning." Finally, there were new instructions concerning the handling of certain investigative resources.

This year, we also asked CSIS about progress in the revision of sections of the CSIS Operational Manual that pre-date the *CSIS Act*. The Service indicated that, this year, they produced a comprehensive policy on the disclosure of information under *section 19*, and that they are now nearing completion of a full set of instructions governing the use and processing of warrants.

Last year we noted a particular concern with provisions in a section predating the *CSIS Act* entitled, ``Demonstrations, Lawful Advocacy, Dissent or Protest." This section has now been deleted from the Operational Manual.

In general, new CSIS policies reflect a tendency towards the devolution of operational decision-making from the Minister back to the Service. Through our examination of actual cases in the future, we will assess the practical implications of this devolution.

(c) Disclosures in the Public Interest

The Minister, under *section 19* of the *Act*, can disclose information to other Ministers or to persons in the public service of Canada where the public interest outweighs the protection of

privacy. The Minister must, however, notify the Committee of any such disclosure.

In 1992-93, the Committee received no notifications under *section 19(2)(d)*.

(d) Employment Conditions

The Governor-General-in-Council, under *section 8(4)* of the *Act* may make regulations concerning employment conditions.

CSIS indicated that it received no such regulations in 1992-93.

(e) Subversion

Section 2 of the *CSIS Act* defines threats to the security of Canada, and *section 2(d)* has been termed the ``subversion'' provision. Current Ministerial Direction requires the Minister to approve any investigations under *section 2(d)*.

The Minister approved no *2(d)* investigations during fiscal year 1992-93.

(f) Report of the Director, and Certificate of the Inspector General

Under *section 38(a)(i)* of the *CSIS Act*, the Committee is to review the Annual Report of the Director to the Minister, and the Certificate of the Inspector General. The Inspector General provides a Certificate to the Solicitor General which assesses the Director's report, and comments on compliance. The Director typically submits his report in June or July, following completion of the fiscal year. The Inspector General's Certificate is submitted to the Minister in November or December.

The Director's Annual Report, in general, discusses the threat environment, the operations of various organisational units of the Service, and the use of various intrusive powers. It includes some of the statistics used by the Committee in analyzing CSIS operations.

The Inspector General, in her 1992 Certificate, said that, ``...while I am satisfied with the Annual Report in essence, there is room for significant improvement.'' In her compliance review, she examined a small number of cases of non-compliance. One involved possible unauthorized disclosure of CSIS information. She also noted that *section 20(2)* of the *CSIS Act* does not provide a threshold of unlawful conduct to be reported to the Minister, and that minor infractions, speeding for example, are not reported. She suggested that the Service develop a system to monitor such infractions.

(g) Reports of the Inspector General

Under *section 40(a)* of the *CSIS Act*, the Review Committee can ask the Inspector General to conduct a review of CSIS activities, and report her findings to the Committee. In 1992-93, the Committee made no such request.

However, we review all reports prepared by the Inspector General on her own initiative. During 1992-93, we received three such reports.

In the first, the Inspector General conducted a review of four warrant affidavits. The review covered content and process. The Inspector General was generally satisfied that the affidavits were accurate and balanced, although she found some errors. In one instance she noted a, ``...lack of balanced analysis and adequate substantiation." She remarked that, ``Our findings lead us to believe that CSIS affidavit quality controls are still not, in all cases, acting as the rigorous safeguards they were intended to be."

In the second, dated April 1993, the Inspector General provided the findings of a multi-year review of CSIS collection activities under *section 12*, involving the assistance of private individuals. She noted a discrepancy between the Ministerial Direction, ``Security Investigations on University Campuses" and CSIS policy concerning the collection of information on campus. She cited a lack of policy on the use of municipal and provincial officials to obtain information. She also commented on various investigative practices in light of recent court decisions interpreting *section 8* of the *Canadian Charter of Rights and Freedoms*.

In the third report, a case study, the Inspector General examined intensively an investigation that had lasted for a considerable time. She looked for any unnecessary or excessive use of powers, or any non-compliance with the law, Ministerial Direction, or CSIS operational policies. She concluded that the investigation was ``strictly necessary" and compliant. She questioned, however, the collection of certain information, ``...of unlikely relevance" and the duration of a related investigation, adding that they, ``...give rise to concerns about the affected individuals' privacy interests."

(h) Special Reports

Under *section 54* of the *CSIS Act*, we may make special reports to the Solicitor General on any matter relating to the performance and functions of the Service. In 1992-93, we submitted the following studies to the Minister under *section 54*:

> Domestic Terrorism Targets — A SIRC Review, July 92 (TOP SECRET) (90/91-13)
>
> Review of CSIS Investigation of ``The Illegal" November 92 (TOP SECRET) (90/91-10)

CSIS Activities in Regard to the Destruction of Air India Flight 182 on June 23, 1985 — A SIRC Review, November 92 (TOP SECRET) (91/92-14)

Regional Audit — Report on Targeting Authorizations (Chapter 1), November 92 (TOP SECRET) (90/91-11)

A list of all SIRC Reports and Studies since 1984 is attached as Appendix B of this report.

(i) An Internal Review of the Warrant Process

In April 1992, CSIS released a report on the warrant acquisition process for CSIS. The report was prepared by a retired judge who had experience in hearing *section 21, CSIS Act* warrant applications.

The judge found the warrant process to be cumbersome and bureaucratic. A warrant application went through 32 steps, involved a minimum of 34 people, and took between three and six months to complete.

The judge recommended that the warrant approval process be simplified and streamlined, and have a one month time limit. He suggested that the drafting of affidavits and warrants should become the responsibility of, and be prepared by, CSIS Legal Counsel.

We understand that, while some procedural details remain to be fine-tuned, the reform proposals have, by and large, been implemented, resulting in warrant acquisitions taking only one third of the time previously required.

We support the general thrust of the report. The warrant process had become cumbersome and inefficient, and bureaucratic paper trails had replaced individual responsibility.

CSIS has implemented most of the report's recommendations.

(j) SIRC Consultations and Inquiries

Formal Inquiries

In our review function, not counting inquiries arising out of complaints, we directed 153 formal inquiries to the Service in the 1992-93 fiscal year. The average time CSIS took to answer a formal question was a lengthy 73 days. We consider this to be unsatisfactory.

Briefings

We met with the Director on: November 18, 1992; March 4, 1993; and on April 14, 1993. We were briefed on regional operations: in Toronto on October 15, 1992; in Vancouver on March 10, 1993; and by the Ottawa Region on April 15, 1993.

Meetings

We met with the Deputy Solicitor General on February 10, 1993; with the newly-appointed Deputy Solicitor General on May 4, 1993; with the Inspector General on June 22, 1993; and with the Solicitor General on August 10, 1993.

(k) Unlawful Conduct

Under *section 20(2)* of the *Act*, the Director is to report to the Solicitor General any instance where, in his opinion, an employee of CSIS may have acted unlawfully in the performance of his or her duties and functions. The Solicitor General, in turn, reports such incidents to the Attorney General, and provides the Committee with a copy of, ``...anything given to the Attorney General."

In 1992-93, we received two such cases.

One person has complained to SIRC and the other may yet do so. We are, therefore, unable to comment further.

(l) The Annual CSIS Public Report — 1992

The CSIS report for 1992 gives a brief review of the global economic and political situation, highlighting the many areas of instability. It draws logical, if depressing, inferences with respect to the need for Canada to be alert to a variety of present and future threats to its peace and security.

9. Inside CSIS

(a) Human Resources

CSIS conducted two Intelligence Officer Entry Training classes during the 1992-93 fiscal year. There were 25 new recruits hired from outside the Service, comprised of 11 female and 14 male students, all of whom graduated.

In the first level Intelligence Officer category (I0-01), there were 47 per cent female employees, compared to 52 per cent last year. In the more senior IO-02 category, there were 51 per cent female employees, compared to 46 per cent last year. In the next senior level, women represent 17.3% of the officers.

We note that women in senior management increased from 9.8% in 1992 to 11.8% in 1993. In the same category, we noted that one member of a visible minority holds a senior management position.

All graduating students had met the Service's linguistics requirements prior to entering the Intelligence Officers Training Program.

(b) Public Relations

The Service employs a public liaison officer and a media liaison officer to deal with external enquiries. While *section 19* of the *CSIS Act* prevents these officers from confirming or denying specific CSIS operational activity, they are able to provide verbal and written unclassified background information regarding the role and functions of the Service, and the environment in which it operates.

The Director of CSIS has also made himself available to the news media. During the Spring of 1992, he met with the editorial boards of five major daily newspapers: The Halifax Chronicle-Herald (April 21); the Ottawa Citizen (May 11); the Edmonton Journal (May 20); the Calgary Herald (May 21); and, the Vancouver Sun (June 22). The Director also delivered a speech to the Royal Canadian Military Institute (RCMI) on October 8, 1992. In addition, the Minister tabled the second annual CSIS Public Report on April 1, 1993.

(c) Accommodations

Construction of the National Headquarters building is progressing as planned. Phase I has been delivered, under budget and on schedule. Phase II is moving forward quickly and will be delivered within budget, with an anticipated completion date of October 15, 1995.

(d) Finances

Each year, we examine CSIS finances, based on limited data on expenditures by category, and new spending items. We analyze year by year spending and query CSIS about significant changes.

The totals for the Main Estimates, and Supplementary Estimates are as follows:

Table 3. Total Estimates (in thousands)

1985-86	$115,908
1986-87	$132,844
1987-88	$136,861
1988-89	$157,852
1989-90	$165,417
1990-91	$205,325
1991-92	$211,229[14]
1992-93	$225,416[15]
1993-94	$228,665

The increases in 1992-93 and 1993-94 can be attributed to spending on the new CSIS Headquarters building. Operational spending is forecast to decline in 1993-94, and following years.

We are awaiting a review of CSIS spending by the Auditor General.

In April of this year, the Solicitor General announced an 11% cut in approved positions. The effect on CSIS employees was cushioned by high vacancy rates.

[14] 1991-92 Main Estimates reduced by $2,722,000 for Government Deficit Reduction Initiatives program.

[15] CSIS 1992-93 Total Estimates were supplemented by $8,528,000 to cover part of the construction costs of the National Headquarters and other projects.

10. Inside SIRC

(a) Accounting to Parliament

On November 18, 1992, the Solicitor General tabled the Committee's 1991-92 Annual Report. The tabling was followed by a news conference.

The Committee appeared before the House of Commons Sub-Committee on National Security on November 25, 1992 to answer questions on the Annual Report.

On December 23, 1992, the Hon. Jacques Courtois, P.C., Q.C., already a member, was appointed Chairman of SIRC, to replace the retiring Chairman, the Hon. John W.H. Bassett, P.C., C.C., O.Ont.

Two new Committee Members, the Hon. George Vari, P.C., O.C, C.L.H., and the Hon. Edwin A. Goodman, P.C., O.C., Q.C. appeared before the Sub-Committee on February 10, 1993 to answer questions about their appointments to SIRC, on November 30 and December 23, 1992, respectively.

On April 20, 1993, the Hon. Rosemary Brown, P.C., was appointed to replace a retiring Member, the Hon. Saul Cherniack, P.C., Q.C. On May 13, 1993, the Review Committee appeared before the Sub-Committee to answer questions about its 1992-93 Main Estimates.

(b) Staying in Touch

We met with two representatives from the B.C. Civil Liberties Association while visiting Vancouver on February 9, 1993.

(c) Spending

Our 1992-93 budget is set out below in Table 4. At $1,510,000, it represents a decrease of 3.7 per cent from the budgeted spending of $1,568,000 in 1992-93. Our 1993-94 estimate of $1,460,000 represents a decrease of 3.3 per cent from the 1992-93 budget.

During the 1991-92 fiscal year, we returned a total of $51,000 to the Government, reducing our planned 1992-93 budget by an additional 3.3 per cent.

Table 4. SIRC Budget 1992-93		
	1992-93	**1991-92**
Personnel	$828,000	$805,000
Goods and Services	$673,000	$754,000
Total Operating Expenditures	$,1,501,000	$1,559,000
Capital Expenditures	$9,000	$9,000
Total	**$1,510,000**	**$1,568,000**

Source: 1993-94 Estimates, Part III, Section II, figure 7

(d) Personnel

The Committee retains a small, permanent staff of fourteen: an Executive Director, a Senior Complaints Officer to handle complaints and ministerial reports; a Director of Research Counter-Terrorism, a Director of Research Counter-Intelligence, and four Research Officers; an Executive Assistant who co-ordinates activities on behalf of the Chairman, conducts all media liaison, co-ordinates the production of the Annual Report, and undertakes research projects; an Administrative Officer who is also the Committee Registrar for hearings; and, an Administrative Support Staff of four. There is a particular burden on the Committee's administrative support staff because the material handled by the Committee is sensitive and highly classified, and must be dealt with using special security procedures.

The Committee decides formally at its monthly meetings the research and other activities it wishes to pursue, and sets priorities for the staff. Day-to-day operations are delegated to the Executive Director, with direction where necessary from the Chairman in his role as the Chief Executive Officer of the organisation.

Appendices

A. Glossary

CEIC — Canadian Employment and Immigration Commission

CI — Counter-Intelligence

COMMITTEE — Security Intelligence Review Committee (SIRC)

CPIC — Canadian Police Information Centre

CSE — Communications Security Establishment

CSIS — Canadian Security Intelligence Service

CT — Counter-Terrorism

DIRECTOR — the Director of CSIS

DND — Department of National Defence

EDP — Electronic Data Processing

GSP — Government Security Policy

IO — Intelligence Officer

IPC — Intelligence Production Committee

MEK — Mujahedin-E-Khalq

MINISTER — the Solicitor General of Canada, unless otherwise stated

MOU — Memorandum of Understanding

RAP — Analysis and Production Branch

RCMI — Royal Canadian Military Institute

RCMP — Royal Canadian Mounted Police

R & D — Research and Development

RTT — Requirements Technology Transfer

SERVICE — Canadian Security Intelligence Service (CSIS)

SIRC — Security Intelligence Review Committee

SIU — Special Investigation Unit (DND)

SLO — Security Liaison Officer

TARC — Targeting Approval and Review Committee

B. SIRC Reports and Studies since 1984

(Section 54 reports — special reports the Committee makes to the Minister — are indicated with an *)

Eighteen Months After Separation: An Assessment of CSIS' Approach to Staffing Training and Related Issues, April 14, 1986 (139 pages/SECRET) * (86/87-01)

Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service, May 1986 (SECRET) ***** (86/87-02)

The Security and Intelligence Network in the Government of Canada: A Description, January 1987 (61 pages/SECRET) ***** (86/87-03)

Closing the Gap: Official Languages and Staff Relations in the CSIS, June 1987 (60 pages/UNCLASSIFIED) ***** (86/87-04)

Ottawa Airport Security Alert, March 1987 (SECRET) ***** (86/87-05)

Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions, May 1987 (SECRET) ***** (87/88-01)

Counter-Subversion: SIRC Staff Report, August 1987 (350 pages/SECRET) (87/88-02)

SIRC Report on Immigration Screening, January 1988 (32 pages/SECRET) ***** (87/88-03)

Report to the Solicitor General of Canada on CSIS' Use of Its Investigative Powers with Respect to the Labour Movement, March 1988 (18 pages/PUBLIC VERSION) *****(87/88-04)

The Intelligence Assessment Branch: A SIRC Review of the Production Process, September 1988 (80 pages/SECRET) ***** (88/89-01)

SIRC Review of the Counter-Terrorism Program in the CSIS, November 1988 (300 pages/TOP SECRET) ***** (88/89-02)

Supplement to SIRC Report on Immigration Screening (January 1988 1989), November 1989 (SECRET) ***** (89/90-01)

Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS, April 1989 (40 pages/SECRET) ***** (89/90-02)

SIRC Report on CSIS Activities Regarding the Canadian Peace Movement, June 1989 (540 pages/SECRET) ***** (89/90-03)

A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information, August 1989 (SECRET)
(89/90-04)

Report to the Solicitor General of Canada on Citizenship/Third Party Information, September 1989 (SECRET) ***** (89/90-05)

Amending the CSIS Act: Proposals for the Special Committee of the House of Commons, September 1989 (UNCLASSIFIED) (89/90-06)

SIRC Report on the Innu Interview and the Native Extremism Investigation, November 1989 (SECRET) ***** (89/90-07)

A Review of the Counter-Intelligence Program in the CSIS, November 1989 (700 pages/TOP SECRET) ***** (89/90-08)

Security Investigations on University Campuses, February 1991 (TOP SECRET) ***** (90/91-01)

Release of Information to Foreign Agencies, January 1991 (TOP SECRET) ***** (90/91-02)

Domestic Exchanges of Information, September 1990 (SECRET) *****
(90/91-03)

Regional Studies (six studies relating to one region), October 1990 (TOP SECRET) (90/91-04)

Investigations, Source Tasking and Information Reporting on 2(b) Targets, November 1990 (TOP SECRET) (90/91-05)

Section 2(d) Targets — A SIRC Study of the Counter-Subversion Branch Residue, September 1990 (SECRET) (90/91-06)

CSIS Activities Regarding Native Canadians — A SIRC Review, January 1991 (SECRET) *****
(90/91-07)

Report on Multiple Targeting, February 1991 (SECRET) (90/91-08)

Study of CSIS' Policy Branch, October 1990 (CONFIDENTIAL)
(90/91-09)

Review of the Investigation of Bull, Space Research Corporation and Iraq, May 1991 (SECRET)(91/92-01)

Report on Al Mashat's Immigration to Canada, May 1991
(SECRET) ***** (91/92-02)

CSIS and the Association for New Canadians, October 1991 (SECRET) (91/92-03)

Exchange of Information and Intelligence between CSIS & CSE, Section 40 Study, October 1991 (TOP SECRET) * (91/92-04)

Victor Ostrovsky, October 1991 (TOP SECRET) (91/92-05)

Report on Two Iraqis — Ministerial Certificate Case, November 1991 (SECRET) (91/92-06)

Threat Assessments, Section 40 Study, January 1992 (SECRET) *****(91/92-07)

East Bloc Investigations, August 1991 (TOP SECRET)
(91/92-08)

Review of CSIS Activities Regarding Sensitive Institutions, August 1991 (TOP SECRET)(91/92-10)

A SIRC Review of CSIS' SLO Posts (London & Paris), September 1992 (SECRET)(91/92-11)

The Attack on the Iranian Embassy in Ottawa, May 1992 (TOP SECRET) ***** (92/93-01)

Domestic Terrorism Targets — A SIRC Review, July 92 (TOP SECRET) ***** (90/91-13)

Review of CSIS Investigation of "The Illegal", November 92 (TOP SECRET)***** (90/91-10)

CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985 — A SIRC Review, November 92 (TOP SECRET)***** (91/92-14)

Regional Audit — Report on Targeting Authorizations (Chapter 1), November 92 (TOP SECRET)***** (90/91-11)

CSIS Activities during the Gulf War: Community Interviews, September 92 (SECRET) (90/91-12)

The Audit of Section 16 Investigations, September 92 (TOP SECRET) (91/92-18)

Regional Audit, January 93 (TOP SECRET)(90/91-11)

The Second CSIS Internal Security Case, May 92 (TOP SECRET) (91/92-15)

The Assault on Dr. Hassan AL-TURABI, November 92 (SECRET) (92/93-07)

CSIS Activities with respect to Citizenship Security Screening, July 92 (SECRET) (91/92-12)

C. Case Histories

In 1992-93, SIRC reached decisions in three cases pursuant to complaints made under *sections 41* and *42* of the *CSIS Act*.

Security Clearance — Case 1

The complainant questioned the right of the Service and its predecessor, the RCMP, to have information on him for a period of 25 years.

The Committee concluded that the Service did not use its powers in an unreasonable or unnecessary fashion.

Security Clearance — Case 2

The complainant argued that the Service investigated him and that the Department of Immigration used the information the Service obtained from that inquiry.

The Committee's role in the circumstances of this case was to decide whether the Service's activities for the purpose of providing advice were properly and adequately carried out.

The Committee concluded that the Service would have been more professional had it clearly indicated its working hypothesis, when providing advice to the Department of Employment and Immigration.

Immigration — Case 3

The Review Committee investigated the basis for a Report made by the Minister of Employment and Immigration and the Solicitor General of Canada pursuant to *section 39(5)* of the *Immigration Act*, *section 43* of the *CSIS Act* and the Committee's Rules of Procedure.

The Solicitor General of Canada and the Minister of Employment and Immigration made a report stating that the complainant had engaged, or that there were reasonable grounds to believe that he would engage, in acts of subversion as described in *paragraph 19(1)(e)* of the *Immigration Act*. They proposed that the Review Committee recommend that a certificate be issued because the complainant was a person described in *paragraphs 19(1)(g)*, and *27(1)(c)* of the *Immigration Act*.

In light of evidence showing that the complainant is a member of an organization which could engage in acts of violence that would or might endanger the lives or safety of persons in Canada, the Committee concluded that a certificate should be issued in accordance with *section 40(1)* of the *Immigration Act*.

D. SIRC Staff Directory

The following is a directory of the SIRC staff as of September 15, 1993, when this report went to the printers.

Maurice Archdeacon, Executive Director . . . . . (613) 990-6839
Pierrette Chénier, Secretary 990-8442

Maurice M. Klein, Director of Research
(Counter-Terrorism) 990-8445
Luc Beaudry, Research Officer 990-8051
Joan Keane, Research Officer 990-8443

John M. Smith, Director of Research
(Counter-Intelligence) 991-9111
Michel Paquet, Research Officer 990-9244
Julie Spallin, Research Officer 991-9112

Sylvia MacKenzie, Senior Complaints Officer 993-4263

Claire Malone, Executive Assistant 990-6319

Madeleine DeCarufel, Administration Officer & Registrar 990-8052
John Caron, Records Officer 990-6838
Roger MacDow, Records Clerk 998-5258
Diane Roussel, Secretary 990-8441