A. Areas of Special Interest for 1999–2000

Project Sidewinder

Report #125

BACKGROUND TO THE COMMITTEE'S REVIEW

In September and October 1999 a series of newspaper articles appeared about a RCMP–CSIS project with the codename "Sidewinder." According to the reports, Sidewinder was a "top secret government project" launched in 1995 and staffed by a joint team of "civilian and police analysts and investigators" from both CSIS and the RCMP. The overarching theme of the media reports was that the project had been the subject of improper political interference damaging to the national interest.[1]

The principal assertions in the media were:

- that the goal of Sidewinder was to gather and analyze intelligence about efforts by the Chinese Government and Asian criminal gangs to influence Canadian business and politics;
- that the Project was terminated before completion because the Service anticipated political resistance;
- that CSIS improperly destroyed all copies of Sidewinder's final report, as well as drafts, correspondence and other related documents;
- that ending the joint project in 1997 was premature and subsequently hobbled the government's ability to deal with emerging threats to the country;
- that the Sidewinder team's request for additional resources, and its recommendation to CSIS/RCMP management to launch a formal investigation into the alleged activities were answered by the project being terminated and the team being disbanded;
- that the mismanagement of Project Sidewinder had significantly harmed overall relations between CSIS and the RCMP.

SCOPE AND METHODOLOGY OF THE AUDIT

The Committee's review of Project Sidewinder encompassed all available documentation created or collected by CSIS since the project's inception; interviews with Service and RCMP officers involved in preparing Sidewinder reports; correspondence with and interviews of outside parties offering information or documentation to the Committee; and an examination of all relevant documents in the Service's files.

In view of the Committee's mandate to review the activities of CSIS, our efforts were necessarily focused on the Service's actions. Nevertheless, the Committee did gain access to some, though not all, Sidewinder-relevant files held by the RCMP, specifically those relating to project administration and report drafting. In addition, we were able to interview RCMP officials.

Of all the Sidewinder documents reviewed, the lion's share originated from RCMP and not from Service files. In the period following the completion of the first draft report in 1997, the Service had disposed of most of the Sidewinder documentation in its possession. In response to a query from the Committee, the Service said that its action was appropriate and fully in accordance with standing CSIS practice for the disposal of files. This matter is discussed more fully below.

THE GENESIS OF SIDEWINDER

Only the second joint project of intelligence analysis ever undertaken by CSIS and the RCMP, the organizations signed a "Joint Analytical Plan" for Sidewinder in March 1996. Making use of public, open-source information, and data already at hand in CSIS and

Main Points

- The Committee found no evidence of political interference as alleged. None of the documents or records reviewed, interviews conducted or representations received evidenced such interference, actual or anticipated. Project Sidewinder was not terminated; it was delayed when its product was found to be inadequate.

- With respect to the Sidewinder first draft report, we found the draft to be deeply flawed in almost all respects. The report did not meet the most elementary standards of professional and analytical rigour. The actions the Service took to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality were appropriate.

- The Committee found no evidence of any substantial and immediate threat of the sort envisaged in the first Sidewinder draft, no evidence that a threat was being ignored through negligence or design, and no evidence that the Government had not been appropriately warned of substantive threats where such existed. Both CSIS and the RCMP continue to investigate similar threats separately.

- The Committee found no indication that the disagreements between CSIS and the RCMP, which arose during the course of Project Sidewinder, had caused, or were symptomatic of, difficulties in other areas of the inter-agency relationship.

- The Service disposed of what it regarded as "transitory documents" related to the Sidewinder first draft report. It is unable to locate other documents the Committee regards as clearly non-transitory and has stated that these were not disposed of but rather "misfiled." However, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder; nor is there any evidence that raw information, kept in Service files and in part used by the Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

RCMP files and those of co-operating agencies, the project was to assess the threat to Canadian security from certain foreign interests. Four people were assigned to work on the project; two analysts from each agency. During the course of the project, expected to take several months, the team would produce interim "intelligence briefs" updating the Government and allied agency clients on national and international links, and intelligence trends disclosed during the analytical process.

The final report would include link diagrams, flow charts and personal profiles. The Sidewinder team would also prepare, "as required," a multi-media presentation highlighting threats to Canada identified as a result of the project. According to the plan, the principal, or at least initial, clients for the project were to be RCMP and CSIS management, with the Service side of the project being managed by the Requirements, Analysis & Production Branch (RAP). RAP products are typically disseminated to a wider readership within government and, where appropriate, the intelligence services of allied countries. One can assume, therefore, that at least on the CSIS side, products of Sidewinder research were expected to reach a wider readership.

Sidewinder team members began by developing a "collection plan"—which data to collect and how.

Under the plan, information of interest was to be identified by cross-referencing information in RCMP and CSIS computer databases. Team analysts would make use of existing CSIS and RCMP files, and the assistance of two other government departments would be solicited to supplement the information base. Records checks would be run through departmental databases, and domestic law enforcement agencies with expertise in the area would also be consulted.

THE ILL-FATED FIRST DRAFT

According to the plan, the project was to complete its analysis by mid-November 1996. However, the available records appear to bear out what the Service told the Committee, that, irrespective of the plan, "little action was taken beyond the production of an initial draft which proved to be unacceptable." Even in this, there was a delay of some six months.

The RCMP told the Committee that the frequent turnover of CSIS personnel dedicated to the project contributed to the delay. For its part, the Service told us that the staffing changes were the result of internal reorganization, transfers and retirements, all unrelated to Sidewinder itself.

The first draft, completed in May 1997, arrived at two key conclusions: that the potential threats warranted the deployment of additional government resources, and that the authorities (RCMP/CSIS) should take the steps necessary to alert operational managers in the RCMP and CSIS to the need to investigate further.

According to the RCMP, the two agencies were scheduled to examine the paper in a "joint review board" on June 9, 1997. Prior to the joint board, however, the Service convened its own internal review, and then shelved the report because, according to the Director General RAP, its findings were "based on innuendo, and unsupported by facts." The RCMP objected to the circumvention of the joint board review procedure and encouraged the analyst/authors of the first draft to prepare a facting binder in support of the report's assertions. Work on Project Sidewinder was suspended, while discussions between the Service and the RCMP about its future continued.

SIDEWINDER RESUMES, DIFFERENCES EMERGE

In January 1998, CSIS and the RCMP agreed to resume work on Project Sidewinder and the production of what would become the final report. The only change made in team staffing was to replace the senior Service analyst, which CSIS attributed to the internal RAP branch reorganization. The new CSIS analyst became the principal author of Project Sidewinder's final report, completed a year later.

Having resumed work, the Sidewinder team began producing new report drafts for Service and RCMP managers to consider. Disagreements between the two agencies soon arose. In May 1998, the RCMP Chief Superintendent in charge of the Force's side of the Project wrote to his equivalent at the Service (Director General RAP) about a number of factual errors he saw in the revised draft. He took issue with the draft's "Conclusion" and "Outlook" sections and asked that they be rewritten. It is apparent from the correspondence that the revised draft had taken a noticeably different tack from that of the contentious first draft.

In September 1998, a CSIS Sidewinder analyst wrote to his RCMP counterpart in the Criminal Analysis Branch requesting additional supporting information. The RCMP's Officer in Charge (OIC) responded to the request by writing to CSIS (Director General RAP) that the RCMP would provide no further information: "It is our opinion that we have provided sufficient background information in support of the materials provided by the RCMP."

In December 1998, the Deputy Director General RAP wrote the RCMP OIC pointing to innuendo in

the then-current report draft and asking that it be removed. She wrote: "We do not have factual evidence of our suspicions and the Service is uncomfortable with the obvious challenges that could be raised by the readership." She added that in her view both agencies had to concur with the inclusion of items in the joint paper, and "regrettably we [CSIS] cannot in this case."

SIDEWINDER FINAL REPORT

In January 1999, the Sidewinder final report was completed, which both agencies approved for distribution. CSIS informed us that the RCMP officially accepted the revised report and a copy of it bears the note "Good Report" penned by the responsible RCMP Chief Superintendent. In response to Committee queries, however, that official wrote that the Force was "not fully satisfied with the final report" because unlike the first draft it "fails to raise key strategic questions and to outline some of the more interesting avenues for research."

> With respect to allegations of political interference in the course of Project Sidewinder, the Committee could find no evidence

The Committee has read both Sidewinder versions and the differences between the two are considerable—the quality and depth of analysis in the final version is far higher than in the draft. Clearly a great deal went on between completing the first draft and releasing the final report many months later.

The essential issues for the Committee, therefore, were whether the Service's actions were appropriate during this time, in line with policy and Ministerial Direction and within the law; and whether the Government, Parliament and the people of Canada were properly served by the advice they received from the agency responsible for assessing threats to Canada and Canadians.

FINDINGS OF THE COMMITTEE

Was There Political Interference?

A media report early in the public discussion of Sidewinder asserted that the project was shut down in mid-stream because CSIS anticipated political resistance. Immediately obvious to the Committee was that the first claim, that Sidewinder was terminated, was simply wrong. Work on Project Sidewinder was suspended temporarily in June 1997 and restarted in early 1998.

The Committee could find no evidence of political interference as alleged. None of the documents or records we reviewed or received evidenced such interference, actual or potential. None of the CSIS and RCMP employees we interviewed had knowledge of political interference or interference by other agencies in Sidewinder or in other related investigations. None of the other parties who came forward to contribute to our review had knowledge of interference or offered substantiating information of any kind.

Was the Service Right to Shelve the First Draft Report?

The Committee studied the first draft report and found it to be deeply flawed and unpersuasive in almost all respects. Whole sections employ leaps of logic and non-sequiturs to the point of incoherence; the paper is rich with the language of scare-mongering and conspiracy theory. Exemplifying the report's general lack of rigour are gross syntactical, grammatical and spelling errors too numerous to count.

It is apparent to the Committee that, at its core, the Sidewinder first draft lacked essential definitional

clarity: if one purports to examine the extent of illegal and threat-based activities allegedly taking place alongside entirely legal and benign ones, it is vital to be able to tell the difference between the two. Sidewinder's first draft drew no such distinctions, providing instead a loose, disordered compendium of "facts" connected by insinuations and unfounded assertions.

The Committee believes that the Service correctly assessed the first draft and took appropriate actions to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality. The Committee believes further that both actions were consistent with the Service's responsibility to assess threats to Canada and Canadians rigorously and in a professional manner and provide objective advice to Government based on those assessments. As it stood in May 1997, Project Sidewinder's first draft report failed to meet those standards.

Did Sidewinder Harm the CSIS–RCMP Co-operative Relationship?

That the CSIS–RCMP relationship continues to be productive and fruitful is vital to the safety and security of Canadians, and monitoring the quality of the Service's co-operative arrangements with the RCMP is of on-going concern to the Committee.[2] Although the Committee's review of Project Sidewinder revealed significant differences of opinion and institutional perspective between the Service and the RCMP over the project, we saw no evidence that the difficulties encountered here were symptomatic of a more widespread problem. Nevertheless, the Committee did attempt to identify the sources of friction and obtain each agency's views of the most significant problems.

The difficulties began after the joint analytic team completed the Sidewinder first draft report. Simply put, RCMP management believed the first draft was good work that went some way to proving the initial thesis, whereas the management of CSIS thought the report's findings were based on innuendo and were not supported by the facts. The Service insisted on a radical rewrite.

CSIS managers told the Committee that among other things, difficulties arose from the inability of the team of analysts to take criticism well, from the fact that the report offered broad recommendations for action when RAP reports typically stopped at analysis and because the report's recommendations were an attempt by some in the RCMP to obtain more resources.

The RCMP's diagnosis was quite different. In interviews and correspondence with the Committee, RCMP management responsible for the project expressed frustration with the Service's approach to the approval mechanism for the joint report which both organizations had agreed to at the outset of Sidewinder. They said that their own analytical reports often came with recommendations and that it was evident that a difference of opinion existed on what constituted good strategic analysis. Finally, the RCMP expressed the view that Service management seemed prepared to ignore the results of a full and impartial joint review.

As noted above, the Committee believes that Project Sidewinder has inflicted no lasting damage to the broader CSIS–RCMP relationship.

Did Shelving Sidewinder's First Draft Imperil Canada's National Security?

Some media reports about Sidewinder in late 1999 portrayed the rejection of the Sidewinder first draft report and its subsequent revision as having blinded the Government to certain emerging threats, such as the abuse of the immigration process. The Committee found no evidence of any kind that such was the case.

Although the delivery of the Sidewinder final report effectively marked an end to the joint effort, both CSIS and the RCMP have continued, separately, to explore and analyze the potential threats to Canada.

Is There a Substantial Threat to Canada That Has Been Ignored?

The *CSIS Act* sets out the threats to national security the Service is responsible for looking into. Measured against these definitions, the Committee's review revealed no "smoking guns," no evidence of substantial and immediate threat, and no evidence that a threat was being ignored through negligence or design.

Did CSIS dispose of documents improperly?

At the outset of our review, the Committee was informed that CSIS had disposed of almost all documents[3] related to producing the first draft of the Sidewinder report (documents pertaining to the final report had been retained and were reviewed.)[4] The question for the Committee was whether these actions were appropriate and carried out in accordance with policy and law.

> The Service's document control procedures lack rigour and its reviews have not been as effective as the Service and we would have wished

In response to Committee inquiries, the Service stated that the disposal of working documents was standard practice for all analytical reports prepared by RAP (the anchor for the CSIS end of the joint project) and was fully in accordance with Government policy. The essence of the Service's case was that the documents disposed of fell into the category of "temporary or transitory records," used in preparing an analytical collaboration, and as such were not retained beyond their need in accordance with National Archives of Canada policy.

Subsequently, however, the Committee determined that some documents the Service was not able to provide to the Committee were not transitory in nature—specifically, inter-agency correspondence concerning the drafts, as well as the signed agreement between the RCMP and the Service setting out terms of reference for the original joint Project.[5]

When the Committee made the National Archivist aware of these particulars, he wrote to us that the Service had already responded satisfactorily to his own inquiries. When we brought the matter to the attention of the Service, it stated that those particular missing documents had not been disposed of like the others, rather they had been "misfiled" and so could not be located.

Because almost none of the Sidewinder first draft documents were to be found at the Service, the Committee is not in a position to render a judgement on the appropriateness of the original disposal. Some were legitimately disposed of and the balance were lost—but we are unable to determine with any certainty which was which.

The Committee finds the evident confusion over the documents' whereabouts disconcerting. The essential trade of security intelligence is meticulous document control and information management. We reiterate our comments made in the "Lost Documents" study (*see* page 9) that the Service's document control procedures lack rigour and its reviews of its practices in this area have not been as effective as the Service and we would have wished.

Notwithstanding our concerns over the Service's handling of some of the Sidewinder documents, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder. In any case, the Committee found no evidence that raw information, kept in Service files and used by the

Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

MAIN POINTS AND CONCLUSIONS

With respect to allegations of political interference in the course of Project Sidewinder, the Committee could find no evidence. None of the documents or records reviewed, interviews conducted or representations received evidenced such interference, actual or anticipated. Project Sidewinder was not terminated; it was delayed when its product was found to be inadequate.

With respect to the Sidewinder first draft report, the Committee found the draft to be deeply flawed in almost all respects. The report did not meet the most elementary standards of professional and analytical rigour. The actions the Service took to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality were appropriate.

The Committee found no evidence of substantial and immediate threat of the sort envisaged in the first Sidewinder draft, no evidence that a threat was being ignored through negligence or design, and no evidence that the Government had not been appropriately warned of substantive threats where such existed. Both CSIS and the RCMP continue to investigate similar threats separately.

The Committee found no indication that the disagreements between CSIS and the RCMP, which arose during the course of Project Sidewinder, had caused difficulties in other parts of the inter-agency relationship.

The Service disposed of what it regarded as "transitory documents" related to the first draft Sidewinder report. It is unable to locate other documents the Committee regards as clearly non-transitory and has stated that these were not disposed of but rather "misfiled." However, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder; nor is there any evidence that raw information, kept in Service files and in part used by the Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

In conclusion, the Committee considers the vital lesson of Project Sidewinder to be this: It is the Service's responsibility to assess threats to Canada and Canadians rigorously, and in a professional manner, and provide objective advice to Government based on those assessments. The Committee is fully in accord with initiatives to bring the respective skills of CSIS and the RCMP together on appropriate projects. At the same time, the Service also has responsibility to ensure that this advice is of the highest possible quality. The Sidewinder first draft report did not meet that standard, and renewed efforts succeeded in producing a much-improved final product.

Lost Documents—A Serious Breach of Security

Report #126

BACKGROUND TO THE INCIDENT

On October 10, 1999, the vehicle of a CSIS Headquarters employee was vandalized in the Greater Toronto area. Inside the vehicle were a number of CSIS documents, several of which were classified. These were among the items stolen. The police were notified when the break-in was discovered, and the employee later reported the theft to a supervisor at the Service.

The police investigation revealed that the theft had been committed by petty thieves intent on supporting a drug habit, and that in all likelihood they had discarded the classified documents unread in a garbage dumpster, which was subsequently emptied at a landfill site. The documents were not recovered.

Following an investigation by the Service's Internal Security Branch—standard procedure in such cases—the employee was dismissed from the Service and more minor administrative actions were taken against other Service officers tangentially involved in the incident. In addition, the Service altered some of its procedures for document control and strengthened its internal "security awareness" program.

The Committee's review encompassed all elements of the incident: the circumstances that led to the Internal Security investigation, the manner in which the investigation was carried out, the results it yielded and all factors that would aid in assessing whether the incident pointed to systemic security problems within the Service.

FINDINGS OF THE COMMITTEE

Was There Warning of the Employee's Inappropriate Behaviour?

Our review of the Service's security records showed no previous security violations by the employee beyond those of a minor nature. Nothing in CSIS files presaged the employee's behaviour and the serious security breach that ensued.

Potential Damage to the Service and to the Security of Canada

With a view to assessing the potential damage to national security should the classified documents be found and released, the Committee examined copies of the lost material. The Service's own damage assessment concluded that although some of the information in the reports was dated, or had already become public knowledge, the potential for damage was high. The information contained would have revealed the existence of certain CSIS investigations and, more critically in the Service's view, the nature of CSIS operational limitations. The Service's assessment noted two important factors serving to moderate the potential damage: no sources were identified nor were any operations compromised.

Based on our review of the documents, we concurred with the Service's view: the documents held the potential to expose the country unnecessarily to security threats.

Problematic document management

In the course of its investigation, Internal Security had considerable difficulty determining the precise content of one item, and thus had to make an educated guess at what the employee held at the time of the burglary. This apparent lapse helped nudge the Committee toward the conclusion that there may have been a problem in CSIS internal document control procedures generally. The Service's explanation for the gap in information was that at the time the document was removed from CSIS premises by the employee, it had not been entered into the corporate file system.

Although not directly related to this security breach, a second document control issue emerged subsequent to the incident. The Committee learned about a case of unauthorized possession of documents. After seeking explanations from two operational branches about their respective control procedures, the Service investigation concluded that the case was an isolated one and that no changes in procedure were required.

To prevent either problem from recurring, the Service has reiterated to its personnel the importance of following proper document control and authorization procedures.

Other Issues Raised by the "Lost Documents" Affair

As noted earlier, several other employees were involved—albeit peripherally—in the incident. Although the Service's internal investigation showed that most media allegations of procedural non-compliance were unfounded, in the Committee's opinion the incident highlighted a lack of rigour in the Service's control over the removal from its premises of documents by officers. The Service has since taken steps to address these gaps.

Policies and the Human Factor

It is evident to the Committee that institutional scrutiny of the incident by us and the Office of the Inspector General, intense media interest, and the Service's own inquiries drew unprecedented attention to the Service's internal security mechanisms. As a result, changes have been made. Nevertheless, it is CSIS' view—and we agree—that no amount of regulation or policy can rule out the possibility of such incidents occurring. Intelligent intelligence work ultimately depends on conscientious people, as well as on strict rules.

"LOST DOCUMENTS" MATTER IN PERSPECTIVE

Previous Internal Security Cases

As part of the Committee's review, we asked CSIS for information about previous internal security investigations and outcomes. Our analysis took into consideration the sea change in national and international security environments in the last fifteen years, and concomitant adjustments in CSIS policies and practices particularly in reporting security breaches.

Although we were unable to identify any single case identical to this most recent one, we did note that a wide range of penalties had been imposed on offending employees—including termination of employment—in cases that shared some of the same elements.

The Committee's review of security breach historical records gave rise to two observations. First, that changes to CSIS internal security policy and practices were often driven by security breach incidents, not considered analysis and review of procedures. The Service's approach to internal security was essentially reactive, notwithstanding internal and central Government agency policies that mandate periodic reviews.

Second, several of the cases in the Service's records have caused the Committee to consider new audit and review procedures so as to ensure that Members have as complete an understanding as possible of such events, as and when they occur.

The Service's handling of the investigation

The Service's own "lost documents" investigation was conducted in a competent and professional manner, ultimately revealing how its classified materials went astray. Internal Security Branch staff maintained a focused and coordinated approach to handling the many issues and questions raised by the incident. CSIS Headquarters gave clear direction to Toronto Region which, in turn, successfully enlisted the very important co-operation of local law enforcement agencies—co-operation crucial to learning the probable fate of the documents. Finally, the policies and guidelines in place for performing and consolidating damage assessments by various operational branches proved effective.

> No amount of regulation or policy can rule out the possibility of such incidents . . . intelligence work depends on conscientious people, as well as on strict rules

CONCLUSION

As already noted, the Service's internal security policy framework has been in place for a number of years, with change usually stimulated by a security intelligence breach at home ("lost documents") or abroad—the Aldrich Ames CIA case being one of the more notorious examples.

Although this most recent incident cannot be traced to faulty internal security policies, it has served to highlight a lack of rigour in certain of the Service's

procedures for implementing those policies. We are aware that the Service periodically conducts its own internal review of security procedures. Nevertheless, security breaches in recent years involving CSIS materials (and commented upon in these pages) suggests that these internal reviews have not been as effective as the Service and the Committee would have wished. The Committee will continue to monitor this area of Service operations closely.

Threats from a Foreign Conflict

Report #124

BACKGROUND TO THE STUDY

The focus of this study is a CSIS investigation of possible threats emanating from a conflict abroad. Canada is susceptible to the spillover from foreign wars and civil strife for a number of reasons: its open society and relatively porous borders, its activist international policies and robust defence alliances, and the presence in Canada of various "homeland" communities. It is in the nature of homeland conflicts that attempts are sometimes made by one or other of the warring parties to enlist the support (moral, political and financial) of compatriots in Canada.

In this instance, the perceived threat arose chiefly from the activities of foreign intelligence services operating in Canada. These included suspected attempts to raise funds, collect information on homeland communities, foment civil unrest in Canada, and illegally procure weapons and technology.

As with every review of a homeland conflict investigation, the Committee directs special attention to gauging the impact of the Service's investigation on the homeland communities themselves. Whenever the Service targets domestic groups or conducts interviews within homeland communities, we wish to ensure that it acted appropriately and entirely within the law.

The audit covers the two-year period from April 1997 through March 1999. The Committee examined all the information generated and retained by the investigation, the targeting authorities requested and warrant powers obtained, and the use made by the Service of information from human sources including its community interviews.

FINDINGS OF THE COMMITTEE

The Committee determined that the Service had sufficient grounds to conduct the investigation and to employ the investigative methods permitted in the targeting authorities and Court warrants. The level of investigation was proportionate to the seriousness of the threat and, with one exception, only information strictly necessary to the investigation was collected.

Three issues drew the Committee's attention:

- an overly general targeting authority;
- community interviews;
- retention of unnecessary information.

An Overly General Targeting Authority

The Service obtained two authorizations, and it was the second and most intrusive that raised some concerns. It set out to investigate the activities of foreign intelligence services, which could lead to the targeting of foreign diplomats and an individual resident in Canada thought to be associated with those agents. The intent was to learn the extent to which the intelligence officers or their associates were engaged in clandestine or illegal activities that constituted a threat to Canada.

Although the targeting authority in question stated that the investigation was required in order to assess three categories of threat—espionage, foreign influenced activities and politically motivated violence (subsections 2(a), (b) and (c) of the *Act*, respectively)—with one of the targets named in the Request for Targeting Authority (RTA), only one of the threat categories cited could reasonably be said to apply.

Current Ministerial Direction is careful to set various thresholds and standards that must be met for each type of threat. In the view of the Committee, all RTAs should specify how the threats any particular target is alleged to represent conform to these criteria.

> **The Committee recommends that RTAs be structured and written to identify clearly the reasons for targeting each target named, under each threat definition cited.**

Community Interviews

In general, the Service's contacts with individuals of homeland communities were conducted appropriately. The Committee did identify one instance where a CSIS investigator appeared to counsel an individual about whether to organize or participate in public demonstrations. Nothing we learned about the matter led us to doubt the officer's good intentions, however, we urged CSIS to remind officers that their task is to gather information, not to offer political direction.

Retention of Unnecessary Information

The Committee's review of CSIS databases identified only one instance where the "strictly necessary" test for collecting information was not met. The information was clearly of a personal nature and had no investigative value. We strongly advised the Service of our concerns. The Service has agreed with this finding and ordered the information deleted from its database.

Terrorist Fundraising

Report #122

BACKGROUND

Beginning with the Halifax G8 Summit in 1995, the international community has paid increasing attention to the issues of illicit transborder fundraising in support of terrorism. In 1996, the G8 nations adopted a series of measures designed to curb the improper use of "organizations, groups or associations, including those with charitable, social, or cultural goals, by terrorists using them as a cover for their own activities."[6] With the same goal in mind, the United Nations is expected in 2000 to adopt the International Convention on the Suppression of the Financing of Terrorism.

Relative prosperity, openness and diversity make Canada an ideal place for organizations devoted to using terrorism to achieve political ends to obtain needed funds through illicit means. Although a number

Management of Targeting

Target Approval and Review Committee

CSIS' capacity to target (or launch an investigation into) the activities of a person, group or organization is governed by policies that rigorously control the procedures and techniques to be employed. The Target Approval and Review Committee (TARC) is the senior operational committee within CSIS charged with considering and approving applications by Service officers to launch investigations. TARC is chaired by the Director of CSIS and includes senior CSIS officers and representatives of the Department of Justice and the Ministry of the Solicitor General.

Levels of Investigation

There are three levels of investigation, with Level 3 being the most intrusive and accompanied by the most stringent legal controls and management challenges. Level 2 investigations may include personal interviews and limited physical surveillance. Level 1 investigations are for short durations and allow CSIS to collect information from open sources and from records held by foreign police, security or intelligence organizations.

Issue-Related Targeting

An issue-related targeting authority allows CSIS to investigate the activities of a person, group or organization that may on reasonable grounds be suspected of constituting a threat to the security of Canada and that are related to, or emanate from, that specific issue.

of countries, including the United States and United Kingdom, have implemented legislation proscribing known terrorist organizations and criminalizing all of their fundraising activities, Canada, for various reasons, has refrained from taking a similar step.[7]

The Government's efforts to deal with this growing international problem have focused on more effective exchanges of information among Canadian agencies, and more stringent enforcement of existing laws and regulations. At the centre of the Government's new initiative was the creation in 1996 of the *Interdepartmental Working Group on Countering Terrorist-Support Activities* (IWG). This body brings the regulatory, investigative and information collection skills of the RCMP, Citizenship and Immigration Canada, the departments of Foreign Affairs, Transport, Justice, Finance, and National Defence—as well as CSIS—to bear on the problem of terrorist fundraising.

The Service plays an advisory role to the Government through the mechanism of the IWG, and provides information about alleged terrorist fundraising in Canada directly to the relevant federal departments. The purpose of the Committee's study was to examine several facets of the Service's work in addressing the problems of terrorist fundraising in Canada.

METHODOLOGY OF THE AUDIT

The Committee's audit encompassed three types of source data:

- all relevant files documenting communications and exchanges of information between CSIS and the Government of Canada for the period from March 1, 1995 through March 31, 1999;
- interviews with relevant CSIS officers and their interlocutors in various departments of government;
- a selected sample of relevant Service investigations were subject to a thorough review, including all relevant targeting documents, operational files, warrant files and information received from foreign agencies.

Our goals were twofold: to determine the effectiveness of Service advice and co-operation in assisting the Government's efforts to curb terrorist fundraising, and to ensure that all CSIS actions were appropriate and in conformity with the law.

FINDINGS OF THE COMMITTEE

Service Investigations of Terrorist Fundraising

The Service stated that, as a result of its investigations linked to international terrorism, it had uncovered several Canadian organizations suspected of facilitating terrorist fundraising objectives. Our own review of these investigations showed that CSIS did have sufficient information to believe that the links to international terrorist groups and to their fundraising efforts constituted a threat to the security of Canada.

Information-sharing

Information-sharing between CSIS and client departments has been ongoing for some time, although the Committee noted that a hiatus in relations with one department lasted several months. The lines of communication with that department have remained open ever since. CSIS and its departmental clients both expressed satisfaction with the liaison relationship. Recipients of Service reports said that the information had been most useful as "investigative leads" assisting in determining how and where to follow up.

The Committee's review of the information-sharing process identified a number of difficulties and potential obstacles:

- the use of CSIS information in court proceedings;
- the nature of the advice to government.

The Use of CSIS Information in Court Proceedings

In providing information to client departments, the Service has experienced problems handling information of potential evidentiary value similar to those the Committee has encountered in other CSIS liaison relationships.[8] Current Canadian law makes it difficult to protect classified intelligence from disclosure in legal proceedings where the information is used to support prosecution. CSIS is concerned to protect domestic and international sources and, in the absence of modifications to current law, client departments' ability to use the Service's information in court will continue to be constrained.

The Nature of the Advice to Government

After examining CSIS files, the Committee noted that the Service was selective in the information it gave to the client departments. In response to a query from the Committee, the Service stated that it refrained from distributing information that could adversely impact the security of human sources, Service operations or relations with third parties, for example allied intelligence agencies.

RECOMMENDATIONS

Two recommendations emerged from this study. First, in respect of the nature of the Service's advice,

> **The Committee recommends that in future, CSIS advise its client departments of substantive changes to the assessments it has previously given them, which arise as a consequence of new information.**

Second, although the Committee supports legislative changes that would allow more effective use to be made of the information shared between CSIS and its client departments, such enhanced procedures could well generate an increase in the number of complaints brought to the Committee. To address such an eventuality,

Lawful Advocacy, Protest, Dissent and Sensitive Institutions

Sensitive operations invariably involve the use and direction of human sources, and, while human sources can be the most cost-efficient form of intelligence collection, their use also entails the greatest risk in terms of impact on social institutions, legitimate dissent and individual privacy.

The *CSIS Act* specifically prohibits the Service from investigating "lawful advocacy, protest or dissent" unless carried on in conjunction with threats to the security of Canada as defined in the *Act*. The Service is obligated to weigh with care the requirement for an investigation against its possible impact on the civil liberties of persons and sensitive institutions in Canada, including trade unions, the media, religious institutions and university campuses.

> **The Committee recommends that the Ministry of the Solicitor General and Privy Council Office initiate special measures to keep SIRC apprised, on a timely basis and as appropriate, of the IWG's proposals as they impact on CSIS activities.**

The Committee will continue to monitor the Service's role in providing advice to the Government of Canada about this growing threat to Canada's security and Canadian interests.

Investigation of a Domestic Threat

Report #121

METHODOLOGY OF THE AUDIT

During a previous review, the Committee learned of several CSIS source operations that sometimes involved the legitimate dissent milieu—specifically,

CSIS Role in Preventing Politically Motivated Violence

CSIS plays a pivotal role in Canada's defence against the possible threats posed by groups associated with politically motivated violence. The "threats to the security of Canada," which it is specifically charged to investigate, include "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state . . ." [section 2(c), *CSIS Act*]

In addition to informing the Government in general about the nature of security threats to Canada, CSIS' intelligence and advice is specifically directed at several government departments or agencies. The information can form the basis for immigration screening profiles used in processing immigrants. In specific cases, CSIS advice can play an instrumental role in determining the admissibility of an applicant, or in denying citizenship. Security intelligence may also serve as a basis for determining an individual's suitability to have access to classified information, as well as assisting the police in crime prevention and in criminal prosecutions.

certain protests and demonstrations. We subsequently conducted a review of the investigations.

Under the terms of the authorizations for the investigations, several individuals were targeted under sections 2(c) and 12 of the *CSIS Act* wherein the Service has the responsibility to investigate threat activities "directed to or in support of the threat or use of acts of serious violence against persons or property for the objective of achieving a political objective within Canada or a foreign state . . ."

During its investigation, CSIS collected information about the targets, as well as some information about protests and demonstrations in which the targets were involved. Information the Service obtained was used in threat assessments given to federal government clients and relevant law enforcement agencies.

During the Committee's review of the investigation—and with particular reference to CSIS policy and Ministerial Direction concerning legitimate advocacy, protest and dissent—the Committee examined all reporting by CSIS sources, all information retained on targets and protests and other incidental intelligence collected. We reviewed all relevant targeting authorities, source handling files and Service internal memoranda. In addition, the Committee interviewed CSIS personnel responsible for the investigations.

FINDINGS OF THE COMMITTEE

The Committee's review identified no violations of Service policy or Ministerial Direction. CSIS had reasonable grounds to suspect that the targets were threats to the security of Canada. None of the human sources engaged in illegal or *agent provocateur* activities, and the sources gathered information on appropriately approved targets. We saw no instances of influence by CSIS sources on the activities of legitimate groups or organizations.

Notwithstanding our general conclusions, this set of investigations was the source of some residual concerns for the Committee. During the course of investigations, which lasted several years, the Service made targeting decisions, chose investigative methods, collected information and advised government clients—all actions carried out in accordance with policy as written—which when reviewed as a whole left the Committee uneasy. Among these were:

- existing policies for managing human source investigative techniques did not ensure that executive management was fully seized with the fact that, because of unforeseen activities of the authorized targets after the original TARC approval, an organization not itself an authorized

target had become implicated in the Service's investigative activities;

- CSIS instructions that sources were only to report on "authorized subjects of investigation" was not fully implemented in practice in some instances;

- in two instances while conducting surveillance of authorized targets, the Service inadvertently collected some information on the activities of an organization. The Service did not retain the information in its active database;

- one threat assessment issued by the Service based on information gathered during these investigations did not, in the Committee's view, accord with the intent of the *Act*.

The Committee believes that these instances—admittedly few in number—point to an occasional lack of rigour in the Service's application of existing policies, which oblige it to weigh the requirement to protect civil liberties against the need to investigate potential threats. We brought these particular instances, and the Committee's overall concern about the need for rigorous weighing, to the attention of the Service.

In the Service's view, its existing policies, including the need for multiple levels of approval, adequately address the Committee's concerns. It believes it is in full compliance with Ministerial Direction which requires it to choose investigative methods and techniques proportionate to the threat, and to ensure that these are weighed against possible damage to civil liberties. The Service stated that ". . . the position that the *[CSIS] Act*, in combination with Ministerial Direction, requires evidence of 'weighing' in every single case before a targeting approval is given, is a distortion of both the *Act*, and of Ministerial Direction."

The Committee is in no doubt that, in all of its investigative activities, the Service takes the matter of civil liberties extremely seriously. However, with respect to its position on the need for evidence of weighing in "every single case," we disagree.

It is an essential principle of administrative accountability that the processes by which judgements and decisions are made can be as important as the decisions and outcomes themselves. The Committee would like to see tangible evidence that significant investigatory decisions involving the legitimate dissent milieu are adequately weighed.

> **The Committee recommends that the Service make the changes to its administrative procedures necessary to ensure that all significant investigatory decisions in the area of lawful advocacy, protest and dissent are weighed and so documented.**

The Committee believes that as well as providing an additional measure of comfort to the Review Committee, such changes would help maintain the day-to-day sensitivity of all CSIS staff to the need to protect civil liberties.

The Committee had an additional recommendation concerning the need to clarify a section of the CSIS *Operational Policy Manual* (a classified document).

A Long-Running Counter Intelligence Investigation

Report #118

BACKGROUND TO THE REVIEW

The Review Committee believes that an essential aid to ensuring the continued quality and appropriateness of CSIS activities is the periodic review of major investigations that span a number of years. We last reported on this counter intelligence operation some time ago.

AUDIT METHODOLOGY

The Committee's inquiries and research were designed to answer certain key questions about the investigation:

- Did a threat (as defined in the *CSIS Act*) in fact exist?
- Was the nature of the Service's investigation (the level of intrusiveness, the quantity of resources deployed) proportionate to the threat?
- Were CSIS actions appropriate, in compliance with Ministerial Direction and internal policy and within the law?
- Was the advice given to the Government based on the investigation timely, balanced and accurate?

Our audit encompassed CSIS operational files for a selected set of investigations, documents supporting targeting requests and warrant applications, Service reports generated for clients throughout the Government and interviews with CSIS officers and with consumers of Service intelligence products in other departments of Government.

In addition to reviewing specific Service activities, the Committee took into account such factors as the number of known and suspected intelligence officers in Canada, and less tangible factors such as the potential damage to Canadian interests should allied governments come to believe that Canada's counter intelligence efforts were inadequate or ineffective.

CSIS and the Use of Surveillance

CSIS uses surveillance to learn about the behaviour patterns, associations, movements and "trade-craft" of groups or persons targeted for investigation. As an investigative tool, surveillance is used to detect espionage, terrorism or other threats to national security. Large amounts of personal information can be collected and retained in the course of surveillance operations. The Service's surveillance units use various techniques to gather information. In an emergency, surveillance can be used before a targeting authority has been obtained.

FINDINGS OF THE COMMITTEE

The Nature of the Threat

It is the Service's view that the target of this investigation is engaged in intelligence-related activities that manifest themselves in classical espionage, foreign influence in various aspects of Canadian society and the theft of economic and scientific information through clandestine means.

In an earlier report the Committee stated that "the threats posed by the intelligence gathering activities of this [target] [were] at th[e] time, nebulous, and sometimes hard to define." Although events since then have served to confirm that the potential for serious threat to Canadian interests is serious and genuine, the current threat as measured in concrete and confirmed activity appears to us to be limited and infrequent.

This difference of opinion between CSIS and the Committee about the nature of the threat led us to conclusions about some of the target's activities that were at odds with those of the Service. Some of the activities investigated by the Service showed the target engaged in intelligence gathering in Canada, but others did not.

In one case the Service treated as a threat activity—an attempt to influence a Canadian official—what seemed to be routine diplomatic behaviour. In another, with little corroborating information, CSIS ascribed intelligence gathering motives to apparently normal consular contacts.

The Committee's review also raised questions about some beliefs the Service has about the nature of the

threat. We are of the opinion that these beliefs are sometimes overdrawn.

Targeting Decisions

The Review Committee thoroughly examined a representative selection of Service targets approved for investigation by the CSIS Targeting and Review Committee. We reviewed the case the Service set out for each and studied warrant affidavits, supporting documentation and reports generated by the investigations.

The Committee believes each of the targeting decisions examined was justified by the evidence. However, in the Service's application to secure warrant powers against one target were a number of overstatements. In one instance, information put forward was more than a decade old and the information adduced was derived from one source's "feelings." In another, a source's speculation was quoted. Some assertions that the target engaged in "suspicious activities" appeared to us to be misleading or exaggerated. Despite these imprecisions, however, the Committee believes the evidence to proceed with targeting the individual was convincing overall.

Investigative Activities and Retention of Information

The Committee identified several instances in which the Service acted in contravention of policy or without due caution:

- some information collected by the Service did not meet the "strictly necessary" test: a membership list, reports about a public meeting and particulars about individuals who were neither targets themselves nor known to have contacts with targets;
- Service actions in regard to one target appeared to carry significant risk;
- CSIS files about one aspect of an investigation appeared to show that a source rendered assistance to a target in a manner that gave rise to the Committee's concern.

Employment of Resources

The Committee was at pains to assure itself that the resources devoted by the Service to this investigation were appropriate to the threat. While our review turned up no acute difficulties, we will continue to monitor the Service's deployment of resources in this area.

Advice to Government

The Service produces several classified publications to transmit its findings to various readerships in the Government of Canada. The Committee examined a selection of CSIS publications relating to this particular investigation, compared the statements in them to supporting information in Service files, and asked clients their views of the utility and accuracy of Service reports.

None of the clients we interviewed took issue with the accuracy, timeliness or analytical quality of the reports they received. Most considered the Service's reports to be useful background information. The Committee's review of the information in support of Service conclusions in selected CSIS reports did, however, reveal some anomalies:

- the Service stated that an action by a target was possibly for the purpose of "developing a network of agents." Our review showed that there was no documentation on file to support this premise;
- a report stating that a target had used a certain business practice to obtain proprietary advanced technology was not technically correct. In our view, the Service's information differed from the report's description;
- CSIS informed its readers that a target had engaged in a number of instances of "espionage" over a long period. In examining these instances, the Committee formed the opinion that the

evidence for some was weak, speculative or ignored reasonable, benign alternative explanations for the actions in question.

CONCLUSION

The Committee believes that the potential threat to Canadians and Canadian interests arising from the activities of this target is significant. It is vital, therefore, that the Service take special care to ensure that the analysis and reporting generated by its investigations remain precise and unbiased. The Government of Canada faces a myriad of difficult international security, economic and diplomatic issues. It deserves the best possible national security advice—clear in analysis, as transparently obtained as law and prudence permit and unencumbered by preconceptions or unfounded speculation. Our review evidenced a few instances that pointed to the Service occasionally drawing conclusions not based on the facts at hand.

> The Government deserves the best possible national security advice . . . as transparently obtained as law and prudence permit and unencumbered by unfounded speculation

Domestic Exchanges of Information (4)

Report #119

In carrying out its mandate to investigate suspected threats to the security of Canada, CSIS co-operates and exchanges information with federal and provincial departments and agencies and police forces across Canada. The Service's mandate to enter into such arrangements is set out in section 17 of the *CSIS Act*. The Service discloses information to various domestic departments and agencies "for the purposes of the performance of its duties and functions" under section 19(2) of the *Act*.

Under section 38(a)(iii) of the *Act*, the Committee is charged with the task of examining the co-operation arrangements the Service has with domestic agencies, as well as the information and intelligence it discloses under those arrangements.

METHODOLOGY OF THE EVALUATION

This review focused on CSIS' domestic exchanges of information for calendar year 1998. In addition to reviewing the Service's information exchanges in all regions, the Committee also conducted an on-site review of one regional office.

The purpose of the review was to assess whether CSIS had adhered to its arrangements with the other agencies, and whether it had collected and disclosed information in compliance with the *CSIS Act*, Ministerial Direction and CSIS operational policies. In particular, the Committee's enquiries were meant to determine if:

- the threat was balanced with the infringement on personal privacy resulting from the passage of the information;
- the exchange of information was strictly necessary to meet the Service's operational requirements as per section 12 of the *CSIS Act*;
- the exchange of information involved the unnecessary use of personal and sensitive information;
- the information exchanged was reasonable and factually accurate;
- all CSIS disclosures of information were in accordance with the preamble to subsection 19(2) of the *CSIS Act*.

COMMITTEE FINDINGS

Overall Co-operation

The Committee found that CSIS co-operation with federal departments and agencies and its relations with provincial authorities and police forces was productive. Our review also showed a general willingness between CSIS and the RCMP to share information with each other.

In one region, however, the Committee found a list of outstanding requests for information from the RCMP. We questioned the delay and learned that the region had since implemented a tracking mechanism in an effort to deal with the problem.

Exchanges and Disclosures of Information

Although the Committee found that the majority of CSIS exchanges of information in 1998 complied with policy, agreements and statutory requirements, we found some instances where, in the Committee's opinion, CSIS had retained unnecessary information.

Unnecessary Retention of Information

The Committee found that one region had collected a report that did not meet the "strictly necessary" criterion under section 12 of the *CSIS Act*. CSIS has since removed the report from its database.

In another instance, our on-site audit of one CSIS region revealed that it had retained several reports in its operational database that it had received from two agencies about planned protests and demonstrations.[9] In our view, some of the information contained in the reports did not demonstrate reasonable grounds to suspect serious violence or a possible threat to public safety. The Committee recommended that CSIS report and retain only the information required to meet its obligations with regard to threat assessments.

The Tracking System

The Committee found that, in general, CSIS' tracking of information exchanges with domestic agencies was consistent. However, we did note variations in how the regions applied the tracking procedure, and a few cases in which the tracking information was not accurately recorded. We also expressed our concern about the fact that the policy on operational reporting was still under development for an inordinate length of time.

Proliferation of Weapons of Mass Destruction

Report #120

BACKGROUND TO THE STUDY

Canada's efforts to prevent or at least slow the proliferation of weapons of mass destruction (WMD)—chemical, biological and nuclear)—to states that do not possess them are longstanding. Since the end of the Second World War, Canada has been at the forefront of every important diplomatic and political initiative aimed at creating an international regime to monitor and control the spread of such weapons, the means for delivering them and the technologies needed to build them.

Since the demise of the Soviet Union, the threat to Canadians' security from such weapons has become more diffuse and also more difficult to counter. Growing numbers of states, and even terrorist organizations, are gaining the wherewithal to purchase (or in some cases steal) the technologies and expertise needed to manufacture extremely lethal weapons that could be used against Canada or its allies.

Although Canada does not possess such weapons itself, a national infrastructure of advanced nuclear, chemical, biotechnological and electronic industries and research facilities makes the country vulnerable to illicit procurement. Many technologies used domestically for peaceful endeavours can also be used in weapons manufacture—so called "dual-use" technologies.

Stemming the improper flow of WMD and their supporting technologies has been a pillar of Canada's

foreign policy for many years. An important domestic element of this policy is the need to understand the nature of illicit and clandestine activities that may pose a threat to the security of Canada, Canadians and others. The Service has an important role in collecting and analyzing such information, stating in 1999 that "counter proliferation is one of its security intelligence priorities."[10] The goal of the Committee's review was to assess the Service's performance of its function to advise the Government in a clearly vital area.

> The Service correctly viewed the target's efforts to circumvent Canada's laws as a threat to national security

METHODOLOGY OF THE AUDIT

The Committee reviewed all files for fiscal years 1997–98 and 1998–99 held by the Service in relation to its issue-based investigation of WMD proliferation. We interviewed Service personnel, attended briefings and examined CSIS Target and Review Committee (TARC) documents in cases representative of the Service's entire counter-proliferation effort. In addition, the Committee examined a number of cases that gave insight into the Service's Counter Proliferation Unit, its methods of operation and its relationship with domestic and foreign agencies.

FINDINGS OF THE COMMITTEE

Threat from a Foreign Country

From CSIS files it was evident that, because of consistent attempts to procure WMD, a certain foreign country was a particular focus for the Service's investigative efforts. Based on an extensive review of the documentation, we concluded that CSIS had reasonable grounds to suspect a threat to the security of Canada under sections 2(a) and (b) of the *CSIS Act* and that the targeting level for the investigation was proportionate to the threat. The Committee determined that with one exception (which we brought to the Service's attention), the information collected met the "strictly necessary" test.

Threat from a Particular Target

The Committee examined the case of a particular counter-proliferation target that had recently come to our attention. We believe the Service correctly viewed the target's efforts to circumvent Canada's laws as a threat to national security.

Certain Illegal Activities

The Service received information that led it to believe some activities had taken place that constituted a threat to the security of Canada as defined in sections 2(a) and (b) of the *Act*. Subsequent CSIS investigation revealed that a violation of Canadian law had occurred and the appropriate department of the Federal Government was so advised. The Committee found that the level of investigation employed by the Service was proportionate to the threat and that CSIS had retained only strictly necessary information in its database.

The Service's Counter-proliferation Effort in General

It is evident to the Committee that the Service plays an important role in Canada's management of proliferation issues at the domestic level (co-operating with police and other enforcement agencies), and globally (acting in support of DFAIT counter-proliferation initiatives, and exchanging information with allied governments and other parts of the international antiproliferation regime). We noted that, overall, the Service's approach to proliferation matters was both strategically sound and flexibly managed. The Service was particularly concerned to give the counter-proliferation unit considerable leeway in its staffing decisions, reflecting the specialist and technical nature of the tasks being pursued.