The Intelligence-Law Enforcement Nexus:

A study of cooperation between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, 1984-2006, in the Context of the Air India terrorist attack

Professor Wesley Wark
Munk Centre for International Studies
The University of Toronto

Preface

The destruction of Air India flight 182 by a terrorist bomb remains one of the most important, but understudied, events in modern Canadian history. The published literature on the Air India disaster is scanty and dominated by journalistic accounts. Archival documents remain, for the most part, inaccessible due to security classifications and the absence of any systematic release policy for historically significant federal government records (apart from Cabinet documents). The main body of evidence in the public domain is a product of government mandated studies, the work of the Security Intelligence Review Committee (SIRC) and trial records surrounding efforts to prosecute the alleged perpetrators of the bombing.

Given these circumstances, any study of any aspect of the Air India tragedy conducted on the basis of public documents alone will face significant limitations. The main concern is the inevitable reliance on judgments arrived at in the government studies and by SIRC, without the opportunity to thoroughly assess the evidence on which such judgments were based.

The nature and evolution of cooperation between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police is at the heart of the story of how the Canadian government responded to the threat of Sikh terrorism and how it reacted in the aftermath of the Air India bombing. Despite the limitations of publicly available material, it is possible to arrive at some potentially important conclusions about the state of CSIS-RCMP relations between the birth of CSIS in 1984, one year prior to the Air India bombing, and the issuance of a revised agreement between CSIS and the RCMP in September 2006, meant to put a new face on the relationship between our security intelligence and security enforcement agencies.

An effective counter-terrorism policy contains many ingredients. One of these is good cooperation between intelligence and police forces. In studying the evolution of CSIS-RCMP cooperation in the context of the Air India affair we are looking to assess the quality of the relationship over a period of years, the stress points, and any problems inherited from the past that remain to be fixed.

The Rae Report

In the aftermath of the March 2005 acquittal of two defendants in the Air India bombing, and amidst on-going public controversy, the Government of Canada asked The Honourable Bob Rae to provide "independent advice on what remains to be learned about this tragedy." The Rae report, "Lessons to be Learned," was produced in late November 2005.[1] Mr. Rae zeroed in on four issues that he believed demanded further study. Three of the four areas of concern involved questions of intelligence work and cooperation between the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP). Mr. Rae believed it was important to establish whether the intelligence assessment process worked adequately and whether any systemic issues emerged that have not been resolved. His review, moreover, had led him to believe that "problems" existed in the relationship between CSIS and the RCMP that may have affected intelligence gathering and criminal investigations. Mr. Rae also felt that the history of the Air India tragedy illustrated the difficulties that exist in trying to establish a link between security intelligence and evidence that can be used in criminal proceedings.[2] He advocated the establishment of a further policy-oriented public inquiry into the lessons of Air India that would take up the issues he identified and provide answers to them relevant to Canada's current efforts to combat terrorism.[3]

Mr. Rae's recommendation was speedily accepted and he was appointed to head such a public inquiry in November 2005. That inquiry was abandoned by the newly elected Conservative government in 2006, which delivered on its own promise to hold a full judicial inquiry into the Air India bombing. On May 1, 2006, the Honourable John C. Major was appointed as Commissioner to conduct an inquiry into the bombing of Air India Flight 182. His appointment directed that he give consideration to the findings of previous studies of the issue, including the Rae report. The terms of reference for Justice Major's inquiry drew on the Rae report by identifying deficiencies in threat assessments, problems in effective cooperation between CSIS and the RCMP and the challenges of establishing linkages between security intelligence and evidence in criminal trials as among the key issues to be studied.[4]

---

1 The Honourable Bob Rae, "Lessons to be Learned," November, 2005. Available online at www.publicsafety.gc.ca
2 ibid., p. 22
3 ibid., p. 31
4 Order in Council, Privy Council, 2006-293, May 1, 2006

In both the Rae report and the terms of reference for Justice Major's Inquiry issues of intelligence threat assessments, CSIS-RCMP cooperation, and the continuum between intelligence and evidence are all treated as separate and distinct issues. In this research report I will endeavour to probe the linkages and synergies between these issues in the broad context of the evolution of CSIS-RCMP relations. Questions about the quality and use of threat assessments, about the nature of relations between our civilian security intelligence agency and our federal law enforcement agency, and regarding the transmission of intelligence information into evidence are, in my view, inseparable and are rooted in the history of our intelligence structures and policies.

Historical Background

The Canadian Security Intelligence Service was established by law in 1984. Its creation was a product of the recommendations issued by the McDonald Royal Commission, which studied the activities of the RCMP Security Service and found evidence of both illegalities in its conduct of operations, especially with regard to the monitoring and disruption of separatist groups in Quebec, and a general failure of performance when confronted with a complex range of national security threats. In removing the security intelligence function from the Royal Canadian Mounted Police, where it had resided since 1920 and, in predecessor organizations as far back as 1864, the government of the day opted for a distinct separation of powers and mandates. The creation of CSIS was meant to establish a civilian intelligence service better equipped to understand threats to national security. CSIS would be embedded in law (the CSIS Act) and its operations reviewed by both internal and independent bodies—the Inspector General and the Security Intelligence Review Committee respectively. At the same time, it was understood that the RCMP would continue to play a role in investigations of national security offences.

While there is evidence to suggest that problems in relations between the newly created CSIS and an RCMP shorn of its security intelligence function were anticipated, it is fair to say that the major concern in the early years of CSIS was with establishing its civilian character and getting it up and running. These early years, of course, overlapped with the tragic events of the Air India bombing, which occurred only a year after the birth of CSIS.

The security intelligence system that was established with the creation of CSIS was a radical departure for Canada from past practice. It aligned the Canadian approach more closely to that of Britain and other Commonwealth countries, where a separation of mandates between security intelligence and law enforcement was reflected in separate agencies. At the same time, the new system distanced Canada from the institutional set up of its American ally, where the Federal Bureau of Investigation contained both a law enforcement and security intelligence function. By the mid-1980s, Canadian intelligence alliance connections had shifted their centre of gravity from a long embrace of British practice and partnership, dating back to World War Two, to a close relationship with the United States intelligence community. Opportunities for learning lessons at the outset about how to make the new system work were, accordingly, reduced. Moreover, the idea of constructing a security intelligence system on the basis of individual departments and agencies each pursuing specialized and distinct mandates with little centralisation or control suited the historical pattern of Canadian intelligence practice dating back to World War Two. A Cold War nomenclature came to stick as a descriptor of the Canadian system—it was based on "silos"--self-contained and autonomous units of secret activity with little connection between them.

Sikh terrorists struck against Air India flight 182 in June 1985 while CSIS was still in its infancy. When the Air India plane was blown out of the skies, the Canadian government suffered a grievous intelligence failure. But these historical propositions—infancy and intelligence failure—need to be kept separate in order to resist the temptation of assuming that infancy explains intelligence failure, and by extension that infancy overcome negates the need for any on-going scrutiny of the causes of intelligence failure.

The failure of intelligence is a critical dimension of the Air India story. Intelligence failure was a product of the inability of Canada's newly created intelligence and counter-terrorism service, CSIS, and its long–established federal police counterpart, the RCMP, to fully target and successfully assess the threat posed by Sikh terrorism. Without a clear intelligence picture, CSIS and the RCMP could neither prevent nor pre-empt the attack. Deficiencies in intelligence hampered the prosecution of the perpetrators involved, especially in the crucial early stages . Studying the intelligence failure at the heart of Air India forces us to ask questions about the capacity of intelligence and police agencies to cooperate successfully

and work together towards a common counter-terrorism objective. Air India also compels us to ask how well and wisely lessons were learned, specifically about the nature of intelligence and RCMP-CSIS cooperation, in the years subsequent to the events of 1985.

An effort to answer these questions will not prevent future terrorist attacks in Canada or against Canadian interests overseas. But it might serve to increase Canadian capacities and understanding in the face of future threats, help fashion realistic policies and, from a public perspective, establish realistic expectations of government performance.

The Lineaments of Intelligence Failure

The causes of intelligence failure have attracted considerable scholarly attention in the literature of intelligence studies. Employing case study techniques and detailed analysis of available documentation, on episodes ranging from the Battle of Jutland in May 1916, to Operation Barbarossa and Pearl Harbor in 1941, the Cuban Missile Crisis in 1962, the Yom Kippur War in 1973 and, in a contemporary vein, threat assessments on Iraq's supposed weapons of mass destruction program in 2002-03, scholars have come up with a rich tapestry of ideas on the root causes of intelligence failure.[5] Much of this analysis has been guided by an understanding of how the intelligence process works. In this regard the concept of the "intelligence cycle" has been of heuristic value. The intelligence cycle dissects the critical activities of an intelligence system, identifying these as tasking, collection, analysis and dissemination.[6]

Intelligence failures are a product of the systemic breakdown of one or more of these critical activities. Each part of the process is complex, demanding and fragile. Their totality, which is meant to prioritize tasks for

---

5 On intelligence and the Battle of Jutland in 1916, see Patrick Beesly, Room 40: British Naval Intelligence 19145-1918 (New York: Harcourt, Brace, Jovanovich, 1982, ch. 10. The most recent analysis of Operation Barbarossa is David Murphy, What Stalin Knew (Yale University Press, 2006). On Pearl Harbor, the classic account by Roberta Wohlstetter, Pearl Harbor: Warning and Decision (Stanford University Press, 1962) remains outstanding. The Cuban Missile Crisis is examined in James G. Blight and David Welch, eds., Intelligence and the Cuban Missile Crisis (London: Frank Cass, 1998). Israeli intelligence failure in the run-up to the Yom Kippur war has been analysed incisively by Avi Shlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," World Politics, 28, no. 3 (April 1976), 348-80. Studies of the failure of intelligence with regard to Iraq WMD are now legion, but one of the best accounts is Lawrence Freedman, "War in Iraq: Selling the Threat," Survival, 46, no. 2 (Summer 2004), 7-50.

6 See the definition employed by the Central Intelligence Agency, "The Intelligence Cycle," at www.cia.gov/cia/publications/facttell/intelligence_cycle.html

intelligence services and generate accurate information that is suitably and promptly communicated to decision-makers, is subject to a high risk of failure. In historical case studies of intelligence failure, a cascading effect is often present. Poor tasking will contribute to inadequate collection, which will in turn rob assessment of sufficient capacity to develop sophisticated judgments. A hollowed out intelligence process will generally fail to create the dissemination (and feedback) channels so vital to establishing the usefulness of intelligence and aiding policy-making.

Intelligence failures inevitably contribute to flawed policy and inadequate operational responses. But an important distinction between intelligence, policy and operations needs to be maintained, while accepting the blurred boundaries between them. Intelligence failures reveal pathologies of knowledge and learning, They are all about the sources of misperception. Policy failures and operations outcomes may be rooted in intelligence misjudgement and error but are not uniquely determined by them.

Unhappily, intelligence failures may be ubiquitous. One of the seminal discussions of intelligence finds that, "Intelligence failures are not only inevitable, they are natural." Richard Betts builds to this fatalistic conclusion by way of careful reasoning about the inevitable presence of pathologies of judgement, ambiguity and ambivalence surrounding information flows, the imperfections of bureaucratic structures, and the phenomenon of political decision-makers driven to consider themselves their own best intelligence analysts. Betts ends by stating: "My survey of the intractability of the inadequacy of intelligence, and its inseparability from mistakes in decision, suggests one final conclusion that is perhaps most outrageously fatalistic of all: tolerance for disaster."[7]

The main difficulty with this argument, apart from its unpalatable nature, is that tolerance for disaster can blunt efforts to improve systems and performance and learn lessons from the past. What does emerge usefully from the work of Richard Betts and a host of other writers on intelligence failure is an appreciation of the complexities of intelligence work and the sources of failure: an appreciation that focuses on analytical misjudgment as a central and perennial factor.

---

7 Richard Betts, "Analysis, War and Decision: Why Intelligence Failures are Inevitable," World Politics, 31, no.1 (October 1978), 89

There is nothing determinative about this finding, but the literature on intelligence failure can serve as a guide to investigations into the intelligence dimension of Air India. It provides us with a investigative road map, with tasking, collection, assessment and dissemination all marked out as potential zones of error. It also suggests that we pay close attention to intelligence assessment –both the product and the institutional setting--as the key to intelligence performance.

The Seaborn Report

The very first post-mortem conducted by the Canadian government into the events of Air India was directed by the newly established office of the Security and Intelligence Coordinator, a post held by Blair Seaborn. Mr. Seaborn had a long and distinguished career with the Department of External Affairs before assuming the post of Coordinator, a career which included substantial exposure to intelligence activities, particularly while serving overseas. Yet the "Seaborn" Report," in actual fact a product of the coordinating mechanism of the Interdepartmental Committee on Security and Intelligence, downplayed the significance of the role of intelligence with regard to both Air India and future terrorist attacks.

The Seaborn report, issued on September 24, 1985, noted that the Canadian authorities were alert to the general possibility that Air India could be a target of Sikh terrorism but lacked any specific intelligence on this threat.[8] In a brief discussion, the report found no fault with the intelligence system, but also cast doubt on its wider utility. It argued that intelligence on specific terrorist targets was "rarely forthcoming," and that efforts to improve intelligence collection were likely to have only marginal use.[9] According to the Seaborn report, intelligence could not be relied on "as the principal, let alone the sole, means of countering terrorism."[10] Instead the task of intelligence was to assist in determining appropriate levels of security, a function deemed "important," that would rely on good assessment and dissemination.

---

8 Interdepartmental Committee on Security and Intelligence, "Report on Security Arrangements Affecting Airports and Airlines in Canada," September 24,1985, p. 1. Hereafter cited as "Seaborn Report." Available onlne at www.psepc.gc.ca/prg/ns/airs/ai_rep-en.asp

9 ibid., p. 2

10 ibid

Effective counter-terrorism was not to rely on intelligence, but rather on "a regime of sufficiently rigorous security in respect of likely targets to deter a terrorist or similar incident from achieving success."[11] The remainder, and bulk, of the report dealt with airport and airline security issues.

There are echoes, probably unconscious ones, in this initial post mortem of some of the analysis arrived at years earlier by Richard Betts. Expectations of intelligence performance must be grounded in reality, failures anticipated, attention paid to analytical and dissemination processes.

But the minimalist position on intelligence taken in the Seaborn report also reflected contemporary government attitudes towards the intelligence function. The absence of any substantial expectations about intelligence performance blunted any serious critique of intelligence shortcomings or any close look at the effectiveness of CSIS-RCMP cooperation. The Seaborn report was compiled at a time when the post bombing investigation was still in its early phases and no "hard" information was available on the perpetrators, or even the exact nature of the destruction of Air India Flight 182. Moreover the report was the product of a committee and of a system that depended on input from the key intelligence agencies, including the RCMP and the Canadian Security Intelligence Service. The power and authority of the Security and Intelligence Coordinator were untested. All of these factors may have constrained a fuller understanding of the role of intelligence and limited any impulse towards sustained and probing criticism. However, the actual dynamics behind the work of ICSI and the compilation of the Seaborn report cannot be ascertained on the basis of public documentation, as the relevant records, assuming they exist, are not in the public domain.

The first two recommendations of the Seaborn report faithfully convey a sense of the limited intelligence function. They urged that the key government agencies, Transport Canada, CSIS and the RCMP should have the requisite assessment capacity and that threat assessments and dissemination channels should be regularly reviewed by an interdepartmental committee led by the Department of the Solicitor General.[12] It is not known from the public record whether even these

---

11 ibid
12 ibid., Annex B, p. 9

modest proposals for adjustments to capabilities and bureaucratic operations were followed through.

SIRC: The Early Reports

The CSIS Act had established an independent review mechanism for the new agency, in the form of the Security Intelligence Review Committee. SIRC prepared an annual report card for the Minister and Parliament on CSIS's fidelity to its mandate, the law and Ministerial direction. Early SIRC reports, beginning in 1985, called some attention to CSIS-RCMP cooperation, on occasion using the phrase "healthy tension" to describe the state of affairs. The most pointed concern expressed by SIRC in the early years emerged in the third annual report, produced in the Fall of 1987, in which it noted the need for scrutiny of the existing CSIS-RCMP Memorandum of Understanding, and greater Ministerial involvement.[13] As far as SIRC was concerned, the roles of CSIS and the RCMP were complementary. The greatest friction was likely to occur in regard to counter-terrorist cases, where the RCMP's mandate to conduct national security investigations and CSIS's mandate to collect security intelligence might well overlap. SIRC wanted, at best, some fine-tuning of the system to make sure that cooperation flourished in practice as it should in theory.

In general, SIRC's concern in the early years of observing CSIS was to ensure that the new agency met the objectives laid down by the McDonald Commission and the subsequent CSIS Act, especially to ensure that it growing into an effective civilian intelligence service. Theoretical and practical issues of how the new agency would interact with the RCMP in its national security mandate were peripheral to this central concern.

The Osbaldeston Report

In another indication that CSIS-RCMP cooperation was not seen to be a core issue at the time, the report of an Independent Advisory Team, established by the Solicitor General following concerns about CSIS' early performance, focused attention on critical deficits in leadership, human resource management and training, targeting, and intelligence

---

13 Security Intelligence Review Committee, Annual Report, 1986-1987, p. 29. Available online at www.sirc-csars.gc.ca

production. Questions concerning the nature of the CSIS-RCMP relationship did not emerge in the study chaired by Gordon Osbaldeston, completed in October 1987.[14]

Parliamentary Review of the CSIS Act

Similarly, the mandated Parliamentary review of the CSIS Act, conducted in 1989-1990, gave only passing attention to questions of CSIS-RCMP cooperation. It noted some concerns with cooperation below the headquarters level, but also pronounced itself satisfied with the general spirit and intent of the existing CSIS-RCMP Memorandum of Understanding (MOU), revised in 1989.[15] The Committee's report did flag a concern about the "serious technical problems to be overcome regarding the process by which intelligence generated by CSIS can be transformed into criminal evidence," but also commended the establishment of a "technical" committee in the Department of Justice to study these problems on an on-going basis.[16] Not a single one of the Committee's 117 recommendations referred specifically to CSIS-RCMP relations.

In the early years of CSIS's existence, which overlap with the Air India bombing and the first phase of investigative activity into the attack, the cumulative record of study by a variety of review bodies suggests that relatively little attention was paid to either the question of intelligence failure or the specific dynamics of CSIS-RCMP relations.

SIRC'S 1992 Study of AIR INDIA

There would, in fact, be a seven year wait following the Seaborn Report until any further systematic, external study of the intelligence underpinnings of the Air India attacks was undertaken. SIRC had maintained a watching brief on Air India while the RCMP investigation proceeded, but in November 1992 completed a massive study entitled "CSIS Activities in Regard to the Destruction of Air India Flight 182."[17] .

---

14 Solicitor General Canada, "People and Process in Transition: Report to the Solicitor General by the Independent Advisory Team on the Canadian Security Intelligence Service, October 1987

15 House of Commons, Report of the Special Committee on the Review of the CSIS Act and the Security Offences Act, "In Flux But not in Crisis," September 1990, p. 105.

16 Ibid.

17 Security Intelligence Review Committee, "CSIS Activities in Regard to the Destruction of Air India Flight 182 on June 23, 1985," November 16, 1992. Originally classified Top Secret. ATIP version courtesy of the ATIP office, SIRC

The SIRC report had the advantage over Seaborn of time, a clearer understanding of the likely causes of the Air India attack, dedicated independent resources, and a determination, stemming from the review body's mandate, to put CSIS performance under a spotlight.

The SIRC study discovered that the problem of Sikh extremism had been scrutinized by CSIS's predecessor, the RCMP Security Service, beginning in late 1974. [18] Some concern was maintained following the establishment of three so-called "Khalistan Consulates" in Canada to promote the idea of an independent Sikh homeland.[19] But the event that prompted significant attention to the threat of Sikh extremism in Canada, was the reaction of Sikh Canadians to the Indian government's assault on the Sikh Golden Temple at Amritsar in June 1984.[20] All of this was brewing as the Canadian Security Intelligence Service was launched on July 16, 1984. Sikh extremism in Canada became one of the first targets of the newly minted CSIS. One of the earliest channels of CSIS reporting on threats to the RCMP was opened by assessments provided to the RCMP VIP Security branch in this period.[21]

Further early forms of CSIS-RCMP cooperation on Sikh extremism emerged as the one year anniversary of the Amristar massacre approached in June 1985. On May 6, 1985, an interdepartmental working group was established consisting of members of the RCMP, CSIS, External Affairs (now DFAIT) and the Ministry of the Solicitor General.[22] The mandate of this working group was to consider risks associated with the anniversary and the level of protection afforded to Indian diplomatic personnel and establishments in Canada.[23]

CSIS-RCMP cooperation in the weeks immediately preceding the Air India bombing had a regional dimension as well. Both agencies engaged in decentralized operations, with regional offices playing a major role in intelligence collection for CSIS and criminal investigation for the RCMP. A CSIS surveillance team from the BC region had Talwinder Singh Parmar, a prominent self-styled Sikh preacher and proponent of an independent Khalistan, in their sights and shared some of their findings with E division

---

18 ibid., p. 4
19 ibid
20 ibid., p. 8
21 ibid., p. 10, 12
22 The Rae Report places the date as May 17, 1985 (p. 6)
23 ibid., p. 18

of the RCMP, based in Vancouver, which had its own VIP security and NCIS (National Criminal Intelligence Service) offices. Among the information shared was the surveillance of a Parmar trip to Nanaimo which involved a journey into the woods by Parmar and Inderjit Singh Reyat and the subsequent detection of a "loud report," thought at the time to be a rifle shot, but later discovered to be the testing of an explosive device.[24] Reyat was eventually to be convicted of manslaughter for his role in the Air India bombing. Parmar, killed in an encounter with Indian police in 1992, was to be characterized as the main perpetrator of the attack.

The SIRC analysis of the archival records makes clear that both CSIS and the RCMP were engaged by the threat posed by Sikh extremism, that CSIS information was flowing to the RCMP, and that the RCMP had sufficient appetite for such reporting to ask independently for updated threat assessments. Altogether some 70 threat assessments concerning Sikh extremism and aviation security were disseminated by CSIS to other government agencies in the period from the founding of CSIS on July 14, 1984 to June 1, 1985. Most of these assessments went to the RCMP VIP Security branch.[25] SIRC concluded both that CSIS had no specific information in advance of the threat to Air India flight 182 and that no significant gap existed prior to the bombing in CSIS-RCMP exchanges of information.[26]

It is equally clear from the SIRC study that CSIS's capacity to fully exploit technical surveillance of Talwinder Singh Parmar was lacking (primarily due to lack of linguistic talent) and that the resources devoted to sustaining full-time physical surveillance of Mr. Parmar in the critical period prior to the Air India bombing were inadequate. There are, in the lineaments of the Air India bombing, clear indications of a failure of intelligence collection.

Questions surrounding failures or weaknesses of assessment are more speculative, but it seems evident that early CSIS threat assessments lacked specificity, and suffered from a set of uncritical presumptions about the nature and targets of any Sikh terrorism. It was presumed that the most likely target for any violent reaction to mark the anniversary of Amristar

---

24 ibid., p. 22
25 ibid., p. 27
26 ibid., p. 28

would be the Indian Prime Minister's son, Rajiv Gandhi, during his visit to the United States in early June. Such a reading was fed by the concerns of US security agencies, above all the FBI, who were themselves seized by this fear and in touch through liaison channels with the Canadian authorities.

When it came to the issue of aviation security, the traditional concern about hijacking was uppermost in the minds of Canadian security officials and may have blunted more imaginative consideration of alternative threat scenarios, such as an effort to bomb a plane in flight. Such warnings as circulated about threats to civil aviation seem to have been affected by a "cry-wolf" syndrome. A series of alerts, many originating from the Indian government, all without apparent foundation, ultimately may have resulted in a kind of fatigue about such threats.

SIRC found no indication of serious problems of cooperation between CSIS and the RCMP prior to the disaster and was emphatic in its conclusion on that point. [27] With Air India, we are in the presence of an intelligence failure marked by the usual cascading effect of inadequate collection and weak assessment, but we are not, at least according to SIRC, in the presence of any systemic breakdown of inter-agency relations on the dissemination front.

The real issue of CSIS-RMCP cooperation emerges over concerns about the handling of the investigative phase of operations following the bombing itself. A memorandum of understanding had been signed between the nascent CSIS and the RCMP on July 17, 1984, to govern the transfer and sharing of information.[28] This first CSIS-RCMP MOU was based on the express need for full and mutual sharing of intelligence on national security threats and offenses, real or potential. It delineated the respective mandates of the two agencies and also identified the need for care and control over the dissemination of intelligence and the right to protect sources of information. If there was any tension in the document, it was an inherent tension involving the desire to share information while respecting distinct mandates and distinct sensitivities over sources.

The CSIS-RCMP MOU was backed up by a Ministerial directive to CSIS penned by the Solicitor General, Bob Kaplan, on July 29, 1984, and copied

---

27 ibid., pp. 35, 36.
28 The 1984 MOU is reproduced as Annex A in the SIRC study of 1992.

to the Commissioner of the RCMP.[29] As SIRC comments, the Ministerial directive "made it clear that the separation of the security intelligence role from the RCMP must not inhibit the passage of information between the RCMP and CSIS."[30] The problem was that the theory of information sharing in the aftermath of a national security incident had never been tested in practice, nor had CSIS and the RCMP enjoyed much time to allow their separate identities in the national security field to mature.

Closing the gap between theory and practice should have been a responsibility of the senior management of CSIS at the time. SIRC was critical of a failure on the part of the CSIS director and his deputy directors to communicate any clear guidance to the organization on how to "plug in" with the police investigation immediately after the destruction of Air India Flight 182.[31] Instead, ad hoc responses from the regional offices of CSIS filled the gap, with the CSIS BC region playing the most important role. [32] From the regional offices situation reports and accounts of cooperation with the RCMP flowed into headquarters. SIRC concluded that operational level cooperation between CSIS and the RCMP "appeared to be good" in the immediate aftermath of the Air India attack.[33] At the senior official level, one disquieting item of correspondence between CSIS and the RCMP was captured and noted by SIRC, but the available evidence suggested that it had no long-term effect on the working relationship between the two agencies.

The critical issue of how information derived from CSIS sources might be used by the RCMP was brought to the fore by RCMP efforts to draw on CSIS material in affidavits in support of warrants for communications intercepts on key suspects, including Parmar and Reyat. The RCMP's desire to advance its investigation came into conflict with CSIS' concern to protect its sources and methods. CSIS's initial view was that its material should be used by the RCMP to provide "investigative leads" only and should not be brought into the legal domain in applications for warrants. SIRC notes that "lengthy negotiations" took place over this issue in late 1985 (October and November), but that they resulted in an agreement on use of CSIS information by the RCMP as well as RCMP access to CSIS

---

29 The Ministerial Directive, "Bill C-9 and the Conduct of RCMP Security Responsibilities," is included as Annex B of the SIRC 1992 study.
30 Ibid., p. 38
31 ibid., pp. 41, 56
32 ibid., p. 42
33 ibid., p. 44

files for "analysis" purposes. This agreement was reached in November or December 1985.[34] The specifics of the resolution of this issue were conveyed in a briefing given by the RCMP Commissioner to SIRC on February 11, 1992. The Commissioner noted that "CSIS provided the Force with authority to use their information in pursuit of search warrants with the understanding that the information would be paraphrased in a certain manner so as to protect the identity of CSIS sources and methods of operations." [35]

A final chapter in the SIRC 1992 study involved the controversial issue of the erasure of intercept tapes generated by CSIS in the course of their surveillance of Talwinder Singh Parmar between March and July 1985. It is fair to say that SIRC found surveillance tape policy in disarray in 1985. That disarray was a product of an effort to both distance CSIS from the evidentiary role of the former RCMP Security Service while at the same time carrying on communications intercept policy in modified form from RCMP days. Disarray in policy was matched by wholly inadequate resources to process the intelligence take from the Parmar electronic surveillance, as the CSIS BC region had no suitable translator to handle Punjabi. Two days before the Air India bombing, approximately 100 audio surveillance tapes remained untranslated.[36]

In the aftermath of the Air India bombing, only 54 of a total of 210 Parmar audio surveillance tapes survived erasure, undertaken according to contemporary CSIS policy, such as it was. Those that survived did so, in effect, accidentally. Fifty tapes were retained because while they had been reviewed by an RCMP investigator they were not deemed to have been studied by CSIS independently for their intelligence value. Four tapes were retained for technical voice print analysis.

The question of information lost through erasure remains open, though in theory, and according to CSIS statements, all the erased tapes were first processed, which means they were listened to, translated and transcribed. SIRC believes it "unlikely that any information in the erased tapes indicating plans to bomb the aircraft would have escaped the attention of the monitors, translators and investigators." SIRC goes on to say that: "The RCMP determined from the translator/transcriber logs of the erased

---

34 ibid., pp. 55 and 63. Note that testimony from Reid Morden, CSIS Director, and the RCMP Commissioner differ on the date.

35 Ibid., p. 63

36 ibid., p. 75

tapes and from the 54 tapes retained and reviewed by them after the disaster, that no significant criminal information was revealed."[37]

Nevertheless, CSIS policy on surveillance tapes at the time was inadequate to serve both the agency's needs and those of the RCMP. It took four years to modify the policy, but a new set of instructions was issued by CSIS in 1989 and subsequently modified by Ministerial direction in April 1991. The revised policy appeared to set clear guidelines for surveillance tape processing and retention. It also established the circumstances in which CSIS would retain surveillance information for transmission to the RCMP. These circumstances were defined as involving a case where the RCMP could not otherwise obtain its own independent evidence and where "exceptional" conditions regarding the seriousness of the information were weighed in conjunction with the potential impact of its use on CSIS sources, methods and "third-party" relations.[38] SIRC pronounced itself satisfied that "the recent policy fills many of the gaps that existed under the early policy."[39]

In sum, the SIRC 1992 study found no "smoking gun" when it came to CSIS-RCMP relations either before the attack on Air India or in the investigative phase up until the time of its report. What it did find were agencies confronted with a wholly unexpected situation that had to translate theoretical policies on information sharing and joint work into on-the-ground collaborative practice. On the whole, they seem to have done so successfully, despite occasional personality conflicts and some rather drawn-out negotiations over access to and use of CSIS information.

What SIRC did discover was a low quality of performance when it came to threat assessments on the part of CSIS. The threat assessments that CSIS issued in the period leading up to the Air India bombing were lacking in specifics and failed to probe alternative threat scenarios, especially when it came to the possibility of terrorist bomb attacks against Air India flights. For example? The SIRC report suggested that the quality of CSIS threat assessment had improved considerably between 1985 and 1992. With the creation of CSIS and the transfer of security intelligence function to that agency in 1984, any potential on the part of the RCMP to use remaining in-house assessment capabilities to challenge CSIS findings was considerably diminished. The RCMP, post 1984, was meant

---

37 ibid., p. 90
38 ibid., p. 87
39 ibid., p. 88

to be a recipient of security intelligence assessment from CSIS, not an independent generator of such intelligence assessments.

Although the SIRC report, in its public redacted version, drew no hard conclusions on the matter, it is clear that deficiencies in intelligence collection, including inadequate physical surveillance coverage and the inability to utilize wiretap surveillance on a timely basis, also affected intelligence reporting before the bombing. Collection and assessment of intelligence are synergistic tasks. Deficiencies in one will feed deficiencies in the other. In the case of the intelligence effort prior to the bombing, it seems clear that CSIS had recognized the threat posed by Sikh extremism in Canada and had been able to identify key targets for surveillance. What the service was not able to do was to get beyond general appreciations of the threat, or to take full advantage of the intelligence gathering operations it had launched. The Air India bombing was the product of an intelligence failure, although it may well fit the profile of the kind of failure that Richard Betts deems inevitable. Air India Flight 182 was not the end result of any significant failure of CSIS-RCMP cooperation.

SIRC'S 1998 Study of CSIS-RCMP Relations

Six years after the completion of its Air India study, SIRC conducted a follow-up investigation of CSIS-RCMP relations. The review was stimulated by on-going concerns on the part of SIRC regarding potential conflict between the services, and was conducted in two parts. Part One studied headquarters-level cooperation between the two services, and was completed in October 1998. A Part Two study, completed the following year, dealt with cooperation at the regional level. Only the Part One study is currently in the public domain in redacted form.

The SIRC 1998 study began with a review of the existing Memorandum of Understanding between the two services, which dated back to 1990. It noted that the Liaison Officer program established to cement relations between the two services and operate as the principal channel for the controlled transmission of information had been a success. But the SIRC study also remarked on the potential impact of the Supreme Court decision of 1991, R. v. Stinchcombe. The actual case heard by the Supreme Court had nothing to do with security intelligence matters, but in adjudicating it, the Supreme Court came down with a very strong statement on the obligation of the Crown to disclose to defence counsel all information in

its possession about a case, so as to "ensure that justice is done."[40] As SIRC related, "The impact of that decision is that all CSIS intelligence disclosures to the RCMP, regardless of whether they would be entered for evidentiary purposes by the Crown, are subject to disclosure to the Courts."[41]

The Stinchcombe decision, in fact, threatened the delicate trade-off at the heart of CSIS-RCMP information sharing. This trade-off involved mechanisms to protect CSIS- originated information when transferred into RCMP hands, via caveats on its use. Seven years after Stinchcombe both services were still mulling over the need for either legislative changes or further revisions to the MOU. Stinchcombe appeared to have the effect of further cementing CSIS's self-image as an intelligence service that collected information for national security purposes, not evidence. It potentially deepened the RCMP's difficulties in sustaining the flow of intelligence, deemed worthwhile as investigative leads, from CSIS. From the vantage point of a review of files between January and August 1997, SIRC restricted itself to a comment that, "while this development has not stopped the flow of information between the two agencies, it has exacerbated some of the concerns on both sides, particularly at the divisional/regional level." [42]

SIRC also expressed an interest in the efforts, led by the RCMP, to create a joint task force to investigate transnational criminal activity. SIRC saw this problem through the prism of potential friction between the two services impacting on information flows. What it really revealed were competing conceptions of the role of the two services in the field of threat assessments. CSIS wished to define its role in transnational crime as providing strategic level assessments, while the RCMP would focus on case-specific issues. That such a division of labour might not be realistic was understood by SIRC, though it had no solution to offer other than a plea to avoid disagreement.[43]

Sidewinder

Unbeknownst to SIRC at the time, the joint transnational criminal project that they had studied in 1997 and reported on in 1998 was a ticking time-bomb. The time-bomb would be project "Sidewinder," a joint RCMP-CSIS

---

40 R. v. Stinchcombe, File 21904, 1991 3 S.C.R. 326

41 SIRC, "CSIS Cooperation with the RCMP, Part 1." October 16, 1998. SIRC Study 1998-04. ATIP version made available by the SIRC ATIP office, p. 9.

42 Ibid., p. 10

43 ibid., p. 21

effort to study the threat posed by Chinese criminal activity possibly related to Chinese state-run foreign espionage. CSIS and the RCMP developed an analytical plan in March 1996 that called for each service to deploy two analysts to form a joint team to produce intelligence briefs on the threat. A "Sidewinder" threat assessment was both long in its production and contentious. A first draft report was prepared in late Spring 1997 but was rejected by CSIS on the grounds that it was "based on innuendo, unsupported by facts." This raised the ire of the RCMP and stalled the project until early in 1998. Work was resumed in January 1998, but disagreements soon emerged again. CSIS took charge of the project and finished a report in January 1999, but it apparently failed to meet full RCMP approval. The internal rancour produced by the project was so great that it led to leaks to the media and members of Parliament, culminating in a series of Globe and Mail articles in September and October 1999 alleging political interference in the handling of the Sidewinder project.

At this point SIRC stepped in with its own study. These were very serious allegations, quite apart from what Sidewinder might tell SIRC about the already sensitive and long familiar issue of CSIS-RCMP cooperation.

SIRC was scathing about the quality of the first draft of the Sidewinder report and essentially agreed with the CSIS decision to shelve it. More difficult to fathom was SIRC's insistence that there was nothing in the history of the project that indicated broader problems between CSIS and the RCMP. In fact, as a joint analytical effort, Sidewinder was unique. The SIRC report itself makes clear the depth of dissatisfaction created by the experience of the project's outcome, especially on the part of the RCMP. The chilling effect was clear in a statement made to SIRC by an RCMP Chief Superintendent that the RCMP would undertake future joint assessments with CSIS, but only "with a much more detailed agreement" and with a "clear working protocol." Such joint assessments, furthermore, "will only be undertaken with CSIS [material redacted] "where both agencies can really benefit from and contribute to a joint project." [44] This was a death knell.

The SIRC study of Project Sidewinder was produced on September 6, 2000. In coming to the defence of CSIS's role in the affair, SIRC muted concerns about the viability of future joint analytical work and reinforced

---

44 SIRC, "Project Sidewinder," SIRC Study 1999-10, September 6, 2000, p. 11. ATIP Version provided by SIRC ATIP office.

a view of CSIS as being the security intelligence assessment top dog. The view was understandable. The CSIS Act had made the Service top dog when it came to national security threat assessments. Nothing in the experience of the history of the service since 1984 suggested it should or could be otherwise. While the service's intelligence collection and assessment performance prior to the Air India bombing had not been stellar, this weakness was seen as a product of immaturity, not of systemic constraints.

What SIRC failed to remark was the idea that Canadian intelligence performance, whether over Air India or Project Sidewinder, might be aided by a degree of competitive intelligence and by a challenge environment. From the very beginning of CSIS's existence, the overwhelming emphasis had been on securing its independence and separate mandate as a civilian security service. Overlap, duplication, and friction with the RCMP were all to be avoided like the plague. Information had to be made to flow between CSIS and the RCMP, but the assumption was that the flow was linear and mostly one-way. CSIS intelligence would flow to the RCMP as needed, primarily to serve as investigative leads to assist the RCMP in its law enforcement mandate. CSIS and the RCMP were to be silos, with an information ramp between them.

The emphasis on the separate and unique mandates of CSIS and the RCMP was understandable, even necessary, but came with hidden costs. They were only to be revealed in the aftermath of the September 11 attacks, when Canada was confronted with security threats from transnational terrorism on a scale never before anticipated.

On the MOU Trail

Efforts to establish both the legal and policy framework for CSIS-RCMP cooperation have consistently focused on the framing of formal documents known as "Memorandum of Understanding" signed by the heads of both agencies. The first of these was laid down in 1984; the most recent dates from September of 2006. They provide, individually and collectively, a template for understanding the aspirations underpinning CSIS-RCMP relations. The history of their composition, to the extent available in the public domain, provides some of the clearest indications of the sources of tension between the two agencies and the distinctive nature of their self-conceptions.

The July 1984 MOU was the prototype.[45] It was focused simply on provisions for the sharing of information between the two agencies, justified by reason of their separate but conjoined legal mandates. Full sharing of information was established as the principle, but hedged by restrictions on the sharing of third party information and on the use of shared information without prior authorisation. The MOU established that "neither CSIS nor the RCMP shall have unrestricted right of access to the operational records of the other agency." The watchword was share, but share as dictated by legal mandates and share with some caution. The 1984 MOU was an accurate reflection of the concerns of the day, based above all in the McDonald Commission's insistence on the need for proper legal regimes to surround security and intelligence work, and for the separation of mandates and powers between a civilian security service and the RCMP.

The 1984 MOU required that the Director of CSIS and the Commissioner of the RCMP develop policy guidelines to implement the memorandum. It was backed up by a robust Ministerial Directive from Bob Kaplan, the Solicitor General, in late July 1984. As the Kaplan directive put it, the organizational separation of CSIS from the RCMP meant that "the formal and informal coordinating mechanisms of a common RCMP structure and the commonality of purpose and outlook which encouraged a high degree of coordination between intelligence and action (enforcement, protection) within the RCMP, will need to be supplanted by other arrangements and understandings between the RCMP and CSIS."[46] The Kaplan directive called on the RCMP to overcome the fragmentation resulting from the separation of security intelligence and law enforcement by building liaison arrangements with CSIS. These liaison arrangements would provide the institutional mechanism for information sharing. Kaplan recognized the potential for overlap of duties and duplication of effort; The Minister also understood that it might not always be possible to demarcate "security intelligence" investigations from "security enforcement" investigations. Close cooperation would have to be the solution.

The major weakness, in retrospect, of the 1984 MOU and the Kaplan directive was in its emphasis on a linear, one-way flow of intelligence

---

45 The July 1984 CSIS-RCMP MOU is included as Appendix A of the Security Intelligence Review 1985," November 16, 1992.

46 Ministerial directive, "Bill C-9 and the Conduct of RCMP Security Responsibilities," dated 10 July, 1984. Bob Kaplan, Solicitor General, to the Director of CSIS, July 239, 1984. Both documents are included as Appendix B of the SIRC 1992 study of Air India, *ibid*.

from CSIS to the RCMP. Not only was CSIS distinguished by way of its monopoly on threat assessments and security intelligence, it was also assumed that the RCMP would have relatively little to contribute of a security intelligence nature from its own sources and knowledge. What this left begging, admittedly for the future, were two issues:

1. whether CSIS could do a fully effective job without security intelligence input from the RCMP (the assumption at the time was yes)

2. how the RCMP could act as a "security enforcement" agency without the benefit of its own intelligence and threat assessments (the assumption was simply that this was CSIS's job)

According to the SIRC, in the first years after separation CSIS and the RCMP signed a total of 17 MOUs, some presumably on more detailed issues of cooperation. The next comprehensive re-framing of the MOU came in 1989-90, when the previous documents were amalgamated into one and revised in April 1990.

The April 1990 MOU marked no radical departure from the principles set out in 1984. The emphasis continued to be on the need for information sharing between two agencies with legally distinct mandates and functions. CSIS was identified as the sole source for national security intelligence, as captured in the wording of the first principle for information exchange:

"the RCMP **will rely** [*emphasis added*] on the CSIS for intelligence relevant to national security offences."[47]

The RCMP's role as informational source was characterized differently: "The RCMP **will provide** *[emphasis added]* to the CSIS information relevant to the CSIS mandate."[48]

An effort was made in the 1990 MOU to draw out the distinctions between CSIS intelligence and RCMP law enforcement work. The MOU noted that

---

47 Memorandum of Understanding Between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police," April 1990., p. 3 Attached as Appendix A to SIRC 1998 Study on "CSIS Cooperation with the RCMP, Part 1"

48 ibid.

while CSIS may from time to time provide the RCMP with information that will have value as evidence, CSIS "does not normally collect information for evidentiary purposes" and that such use would be exceptional and would require prior CSIS approval.[49] Moreover, in a later part of the MOU, categories of information that the RCMP was to share with CSIS drew attention to "detailed case-related information relevant to the security-related responsibilities of the CSIS." [50]

The liaison channels authorized in Bob Kaplan's Ministerial directive of July 1984 were reaffirmed and were tightened up by specific protocols over channels of sharing and dispute resolution and through the creation of a "Senior Liaison Committee," which would have both a policy and an arbitration function.[51]

No revisions occurred to the MOU between April 1990 and September 2006. Some efforts at redrafting were undertaken in 2000 and again in 2002, but went nowhere largely because they were not a high priority for CSIS and failed to satisfy the RCMP, which viewed such efforts as both inadequate and ineffective in addressing contemporary security issues.

It was not until the advent of the Rae investigation into the Air India bombing that both the RCMP and CSIS were stimulated to return to the drafting table. The senior management of both CSIS and the RCMP engaged in on-going discussions between April and October 2005 on the subject of "modernizing" the relationship between the two bodies. The Director of CSIS and the RCMP Commissioner met twice in this period with their senior managers in attendance to personally address this issue. The upshot was a revised CSIS-RCMP MOU, eventually signed on September 29, 2006.

The September 2006 MOU reaffirmed the need for CSIS-RCMP cooperation within the framework of their "distinct yet complementary roles." [52] The relationship between the two agencies was now defined as a "partnership, providing mutual assistance with respect to each other's mandate."[53] As

---

49 ibid., p. 9
50 ibid., p. 10
51 ibid., p. 18
52 Memorandum of Understanding between CSIS and the RCMP, September 29, 2006, p. 1 Courtesy of the Commission of Inquiry into the Investigation of Air India Flight 182, public production # 1374
53 ibid

had been the case throughout the history of the CSIS-RCMP MOUs, the key was finding ways to operationalise the agreement. In this respect, the 2006 MOU did offer something new. In place of an exchange of Liaison officers that had apparently fallen by the wayside, the MOU created a senior level coordinating committee to manage the interaction of the two services on the investigative front, to develop a common terrorist threat assessment, and to develop joint training.

Gone from the 2006 MOU was the language which spelled out the RCMP's "reliance" on CSIS for intelligence and the inference that CSIS would be the main supplier of strategic level information to the RCMP, while the RCMP might contribute tactical, case-oriented information to assist CSIS in its operations.

The thorny issue of transmitting CSIS intelligence into evidence for law enforcement purposes was dealt with in the 2006 MOU by a combination of traditional formulae and new safeguards. The 2006 MOU reflected the now deeply entrenched concern on the part of CSIS about disclosure of their intelligence in the course of judicial proceedings. These disclosure concerns had been heightened by the Stinchcombe decision and had continued to dog CSIS-RCMP relations since 1991. The 2006 MOU asserted two longstanding, but competing principles. One was that CSIS information provided to the RCMP may have "potential value as evidence in the investigation or prosecution of a criminal offence." [54] The other was that CSIS "does not normally collect information or intelligence for evidentiary purposes"—a reflection of its different mandate and different legal grounds for commencing intelligence collection activities against threats to the security of Canada.[55]

The 2006 MOU emphasized the reality of the Stinchcombe environment, in which any information in the possession of the RCMP, no matter what its genesis or intended use in criminal proceedings, might be subject to the laws of disclosure in court. It also invoked the powers of sections of the Canada Evidence Act, generally known as public interest immunity, to provide the government, as needed, with tools to prevent the disclosure of sensitive information in court.

---

54 ibid., para 21
55 ibid

Behind the scenes at least one document prepared by the RCMP during the course of the MOU revision was skeptical about the implications of the use of the public interest immunity clauses (Section 38) of the Canada Evidence Act, arguing that it might involve considerable delay or even the derailment of criminal proceedings. In such a scenario, CSIS-RCMP sharing of intelligence was nullified. An in-house research paper prepared by the RCMP compared disclosure protections available to Canada with those available to its closest intelligence allies. The powers available in Canada were seen as a double-edged sword. The document is worth quoting:

> "When considering the Charter of Rights and Freedoms and the broad right to disclosure in Stinchcombe, section 38 represents a compromise. Information that is injurious to the national interest can still be ordered disclosed if the public interest in disclosure outweighs the public interest in non-disclosure. When section 38 certification is used as a last resort to bar disclosure, key prosecution evidence may then be ruled inadmissible or the charges against an accused may be stayed."[56]

At the end of the process of turning intelligence into evidence lay the prospect of stalled or aborted trails. Only experience, of which Canada was short, would tell. But the process had to be made to work, no matter what the outcome. To that end, the 2006 MOU called attention to the need for joint training and secondments between the two agencies to share knowledge and "enhance understanding of each other's mandate, responsibilities and methodologies."[57] Joint training was new as a concept. Secondments had long been practised but had led to friction between the two services and complaints from CSIS about the under-utilisation of its officers. The 2006 MOU was designed to restore functionality to the secondment process.

The 2006 CSIS-RCMP MOU, like all its predecessors, was nothing more than a piece of paper signed admittedly by the CSIS Director and the RCMP Commissioner. Its test would come with operational experience and with real-world events. It's too soon to say whether the 2006 MOU

---

56 RCMP National Security Support Branch, "Information Sharing Among the 'Five Eyes,' September 6, 2005, pp. 10-11. ATIP version courtesy of the RCMP.

57 CSIS-RCMP 2006 MOU, para. 24

works to achieve its objectives. What can be said is that the objectives themselves are firmly rooted in a substantially altered understanding of the relationship between CSIS and the RCMP. The relationship had moved, over the course of 22 years, from silos to partnership.

The original 1984 MOU described the silo arrangement, with CSIS and the RCMP connected by an informational ramp. CSIS was, in many respects, the tall silo, with its lofty strategic intelligence gaze. The RCMP was the stumpy silo, engaged on in-the-trenches tactical intelligence and case work. The informational ramp flowed one-way.

This system brought no benefits at the time of the Air India terrorist attack. It is impossible to say with certainty whether a different system could have prevented, through better intelligence work, the attacks on Air India , or it could have netted the main instigators in the aftermath of the attack.

Lessons were not quickly learned about the inadequacies of the post 1984 system of domestic intelligence and security that Canadians built for themselves. Lessons were not learned because expectations were relatively low concerning the role and value of intelligence in counter-terrorism, because of the assumption that the attacks on Air India had come at an unfortunate moment of "immaturity" on the part of CSIS and the new structures of security intelligence, and because we had invested heavily in the notion of the distinctiveness of the intelligence and law enforcement functions. We had built our own conceptual "Chinese Wall" to separate security intelligence and law enforcement.

A variety of factors worked to solve the "immaturity" problem: time, experience, new personnel intake, new leadership, the prodding of SIRC and one-off advisory studies with that conducted by Gordon Osbaldeston. Perhaps the experience of Air India was a prod, but if so it is hard to document.

Different expectations about the intelligence function and a re-thinking of the intelligence-law-enforcement relationship would only emerge in a post 9/11 environment. This can be construed as a result of a failure to learn lessons directly from the Air India disaster. But it was also a matter of evolution, experience, and a growing distance from the shaping experience of scandal and disillusion with the performance of the RCMP security service that had been the original impetus for the creation of

CSIS in 1984. Above all, the kind of relationship between CSIS and the RCMP imagined in the 2006 MOU was a direct product of the post 9/11 environment. That environment was shaped by a much greater sense of threat to national security than anything that transpired surrounding the advent of Sikh extremism and the bombing of Air India. With a greater sense of threat came a much greater sensitivity to the intelligence function and to the significance of CSIS-RCMP relations.

Post 9/11 Developments

The Al Qaeda suicide attacks on targets in the United States on September 11, 2001 came as a shock and surprise to the Canadian intelligence community. Those attacks plunged Canada into a crisis atmosphere. In their immediate aftermath, the United States declared a global "war on terror" and Canada signed as a NATO member state an unprecedented Article V declaration of collective defence against attack. Fears of an imminent second wave of terrorist strikes sparked an intensive hunt for potential underground Al Qaeda cells throughout North America. The Canadian government scrutinized its own resources to deal with the threat of global terrorism and began a process of significant national investment in upgraded security capabilities as well as the development of new legal powers.

Both the RCMP and CSIS were major beneficiaries of new spending on national security, packaged in a "national security" budget announced by then Finance Minister Paul Martin in December 2001. This financial largesse reflected a sense of the lead role that both agencies would have to play in the face of an unprecedented and unexpected threat environment.

More significant than the budget outlay was the framing of Canada's first anti-terrorism act, passed into law in December 2001. Bill C-36 criminalised terrorism, and added new clauses to the criminal code. It created or expanded new legislative mandates for elements of the Canadian intelligence community such as the Communications Security establishment and FINTRAC (Financial Transactions Reports Analysis Centre). It significantly amended the Official Secrets Act, renamed as the Security of Information Act. The Attorney General acquired new powers with regard to the issuance of "public interest" immunity certificates. There is no doubt that the anti-terrorism act lived up to its billing as an "omnibus" piece of legislation.

It is important to note that the Anti-Terrorism Act involved no change to the mandate of either the RCMP or CSIS. No new "powers" were granted to either agency, as was frequently suggested in the media. But equally it is the case that the criminalization of terrorism broadened the scope of RCMP national security investigations, while the greater threat posed by global, transnational terrorism in the post 9/11 era fundamentally affected the intelligence priorities of CSIS, as well as the Communications Security Establishment and many other elements of the Canadian security and intelligence community.

The first phase of Canadian counter-terrorism policy after 9/11 was essentially reactive and dictated by the demands of a crisis environment. The government of Canada concentrated its energies on injections of money to boost national security capabilities, new legislation, and the Canada-US relationship, particularly in terms of border security and trade.

Reactive policy was ultimately accompanied by more strategic and long-range decision-making. As the events of 9/11 and its aftermath were absorbed and reflected on, the federal government began to conceptualise the role of intelligence differently, made major alterations to institutional structures, and set out a comprehensive strategic vision. This work accelerated with the ascension of the Paul Martin government in December 2003.

Two key themes emerged in this second wave of government reaction to the new post 9/11 security environment. One was the concept of intelligence as a "first line of defence." The other was the emergence of a doctrine of "integrated" national security practice. Both would provide the underpinnings for the declaration of CSIS-RCMP partnership framed in the CSIS-RCMP 2006 MOU.

The primacy of intelligence as a tool of national security policy was reflected in the National Security Policy document issued in April 2004. This document contained a statement never before expressed in the history of government strategic doctrine:

"Intelligence is the foundation of our ability to take effective measures to provide for the security of Canada and Canadians. To manage risk effectively, we need the best possible information about threats we face and the intentions, capabilities and activities of those who would do us harm. The best decisions regarding the scope and design of security programs, the allocation of resources and the deployment of assets cannot be made unless decision makers are as informed as possible." [58]

This new concept of the role of intelligence substantiated previous decisions taken on fiscal outlays. But it also operated alongside a determination to alter the institutional setting for intelligence work in Ottawa, a change based on an appreciation that the older model of "organizational silos" had to be surmounted. The National Security policy called attention to a series of measures already undertaken to ensure more effective intelligence work. This included the creation of a new senior Ministry, the Department of Public Safety and Emergency Preparedness Canada, the establishment of the post of National Security Advisor to the Prime Minister, and, as a focus for collective threat assessment, the construction of the Integrated Threat Assessment Centre (ITAC). ITAC's design was meant to symbolize a new way of doing intelligence in Ottawa. It would be based on collective intelligence input from a wide range of government departments and would circulate its product to "all who require them." [59] As a sign of the, at least symbolic, place that ITAC would have at the heart of government analysis, it was to report to both the Minister of Public Safety and the National Security Adviser. ITAC was also built as a new mechanism to ensure CSIS-RCMP "partnership," Not only were the two agencies seen as the main contributors to ITAC, the Centre itself was to be located in CSIS, but headed by a senior official seconded from the RCMP.

Integration was a complementary theme, highlighted as well in the 2004 National Security Strategy. The strategy paper had this to say about the importance of integration:

"The increased complexity of the threats facing Canada requires an integrated national security framework to address them. It is critical for

---

58 "Securing an Open Society: Canada's National Security Policy," April 2004, p. 15. Available online at www.pco-bcp.gc.ca

59 ibid., p. 18

our key security instruments to work together in a fully integrated way to address the security interests of Canadians."[60]

In addition to the creation of PSEPC and the post of National Security Adviser, the document also called attention to the establishment of a standing Cabinet committee on "Security, Public Safety and Emergency Preparedness."[61]

While the National Security Strategy was designed with a wider advocacy in mind, it spoke to issues crucial to change in the CSIS-RCMP relationship. The concept of "partnership" enshrined in the 2006 MOU was a re-statement of the concept of "integration" expressed in the 2004 strategy. Like the 2006 MOU, the 2004 strategy paper represented a policy departure, and laid down a new conceptual framework. Implementation of the strategy, especially in terms of achieving effective integration, remains a work in progress. Neither the 2006 MOU nor the 2004 strategy document were conceived of as efforts to learn lessons from Air India. In practice, both policies captured lessons that had to be learnt, but also had to wait until a different climate of threat appeared after 9/11.

Conclusions

The security intelligence system erected in Canada in 1984 with the creation of CSIS was a product of the immediate experience of scandal and poor performance of national security functions by the RCMP Security Service. In separating the security intelligence function from the security enforcement function, the Canadian government looked to fix the problems of the past and did so by way of a familiar Canadian institutional pattern, one rooted in a concept of intelligence and law enforcement "silos" with distinct functions and mandates. The Canadian security and intelligence community was historically decentralised, with only weak central coordination and leadership. This decentralized system was effectively reinforced with the creation of CSIS and the separation of powers and mandates between CSIS and the RCMP. Though the possibility of problems in cooperation between the two agencies was anticipated from the outset, a solution was looked to in the construction of formal Memoranda of Understanding between the agencies, backed by Ministerial directives. What the Canadian system did, in 1984 and

60 ibid., p. 9
61 The Cabinet committee has since been altered to one dealing with "Foreign Affairs and Public Safety."

after, was in effect to construct a made-in-Canada version of a "Chinese wall" between the RCMP and CSIS and then require the two agencies to surmount the wall through cooperation in information sharing and investigative practices. Effecting cooperation was largely left to the leadership and rank and file of the two agencies, with only occasional probes from outside, usually mounted by the Security Intelligence Review Committee.

At no point in the aftermath of the Air India bombing was the attack officially understood as an intelligence failure. The Seaborn report, the first postmortem, instead emphasized minimalist expectations of the role of intelligence in the face of terrorist threats. The much more substantial study of Air India embarked on by SIRC in the early 1990s, did call attention to weaknesses in CSIS intelligence, but shied away from calling Air India an intelligence failure *tout court*. The failure to call a spade a spade in public had the effect of reducing attention to the need to learn lessons from the performance of the security and intelligence community.

Although the CSIS-RCMP Memorandum of Understanding was revised and tinkered with between its initial composition in 1984 and 2002, no major, systemic changes in the relationship between the two agencies occurred. Throughout most of this 18 year period, they continued to operate as "silos" in a decentralized system. This was not primarily a product of bureaucratic rigidity, institutional insularity, or failures of leadership. It was a product of what was wanted.

What went unrecognized prior to the advent of the 9/11 era was that CSIS-RCMP cooperation had at its heart the requirement for an effective capacity for intelligence gathering, assessment and dissemination on the part of both agencies. Instead, these classic components of the intelligence cycle were deemed to be exclusively a CSIS function, and the RCMP was situated as a consumer of intelligence, rather than a student of it. Such a precise, functional division of labour was unrealistic, bound to cause problems, and had the effect of robbing CSIS of a good understanding of RCMP methodology and of robbing the RCMP of a good appreciation of how best to use intelligence for investigative purposes. Moreover, the functional division of labour laid down in 1984 robbed the system of the benefits of competitive intelligence. As Judge Richard Posner has reminded us, systems that display a capacity for competitive

intelligence ensure better diversity of insight and act as a brake on regnant preconceptions. [62]

This is not to say that the Air India disaster could have been averted by a different intelligence system, or a different division of labour between CSIS and the RCMP. Here, the admonishment of Richard Betts with regard to the inevitability of intelligence failure is a useful caution.

What can be said with confidence is that the inadequacies of the 1984 system were only fully appreciated in the aftermath of the 9/11 attacks. The effort to correct these inadequacies after 9/11 were extensive and significant, and included a new understanding of the lead role of intelligence, a new definition of a "partnership" between CSIS and the RCMP, reflected in the 2006 MOU, and greater efforts at institutional and strategic integration to overcome the prior history of the silo effect.

The temptation might be to say that changes effected in the Canadian security and intelligence system after 9/11 have resulted in a belated learning of lessons left unaccomplished after Air India. But there are two problems with this. One is that the effort to learn lessons directly from Air India was real and sustained but its limitations have to be understood in their historical context. It took the much greater domestic and international shock of the 9/11 attacks to produce an earthquake effect in the Canadian intelligence system. The 9/11 attacks and the advent of global, transnational terrorism as a principle national security threat forced change in a way that Air India failed to do.

A second problem with taking comfort from the recent changes is that they are recent and remain, in many respects, to be fully tested. This is especially true of the 2006 MOU and its invocation of "partnership." As the report of Justice O'Connor into the case of Maher Arar reminds us, there remains a great deal of work to be done to ensure that both CSIS and the RCMP respect their distinct mandates while "working together in a cooperative and integrated manner."[63] The days when that distinctiveness seemed uncomplicated and when CSIS and the RCMP were left alone to figure out ways to surmount their Chinese wall are behind us. What is ahead is a new definition of intelligence partnership and a new and more sustained monitoring, both internal and external, of CSIS-RCMP

---

62 Richard A. Posner, Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11 (New York: Roweman and Littlefield,2005), p. 155

63 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Analysis and Recommendations, especially Recommendation #1, pp. 312-15.

relations. It is also worth hoping that what is ahead for Canada is a more sustained commitment to a study of security and intelligence problems that will continue on after the Air India Inquiry closes its doors and issues its report.

The Way Forward:

The greatest challenges to the achievement of CSIS-RCMP cooperation in the future are the need to fashion a true "partnership" and to engage in genuine integration of national security activities. Progress towards these goals will need to be encouraged and scrutinized using the existing mechanisms of accountability and review available with the Government of Canada system. Parliament, the Minister, existing review bodies, both internal and independent, will all need to play a role. There will be continued work for the Office of the Auditor General in monitoring the effectiveness of CSIS and the RCMP's pursuit of partnership and integration. Nothing new need be built into the system. Instead, what is required is sustained attention and an appreciation that partnership and national security integration are not easy tasks, and not ones to be left to the agencies themselves to accomplish on their own—as was the case for much of the time covered by this report.

This report has found that one of the systemic deficiencies in intelligence, that broadly affected CSIS-RCMP capabilities and cooperation, was a product of a too rigid definition of roles and functions when it came to intelligence production. The system created in 1984 and sustained throughout the period down to the 9/11 attacks was premised on a notion of CSIS as intelligence producer and the RCMP as intelligence consumer. This notion robbed the Canadian system of a capacity for competitive intelligence judgments, robbed the RCMP of a capacity to generate intelligence to apply to their national security investigative function, or to use intelligence well, and made difficult the inter-connection between the two services. In an understandable effort to accomplish the objectives of the McDonald Commission in establishing a civilian security intelligence function, we produced an institutional environment which made sharing and cooperative endeavours more difficult than they needed to be. The sorry history of the Sidewinder affair is a testament to this problem.

With the advent of a new appreciation of the significance of intelligence, post 9/11 and a recognition that intelligence needs to be a product and manifestation of a more integrated national security system, there is an

opportunity to learn from our history and our errors. But creating a high quality, integrated national security intelligence product will take work. It will require talent, resources, and a cultural shift within the security and intelligence community towards sharing and mutual appreciation of the contributions of a wide variety of agencies. A true competitive intelligence environment requires a difficult to achieve combination of competition, respect, sharing and accommodation to distinct outlooks.

What might be done to help bring such an intelligence environment into being? This question is worthy of further and sustained thinking. But two suggestions would involve the weight of critical scrutiny, applied from different angles. The ultimate test of an intelligence product is in part its veracity, but also its usefulness and acceptance by senior decision-makers. One way to challenge the production of integrated, high-quality intelligence assessments would be to put them to the test of having to perform as a regular, high-level product for Cabinet. Another way to put the intelligence product to a test, and to broaden the competitive intelligence environment, would be to submit some intelligence assessments to review and scrutiny by a panel of security cleared expert advisers. In both cases the achievement of integration and partnership in intelligence production is shifted as a burden from the shoulders of CSIS and the RCMP alone.

CSIS and the RCMP are public institutions. Their personnel are recruited from the public, and as institutions they are ultimately accountable to the public. Their effectiveness is a matter of great public interest. If the public has high expectations of the performance of CSIS and the RCMP, it is also important that the public be in a position to realistically scrutinize and critique the conduct of these principal national security institutions. Such a capacity is made intrinsically difficult by the secrecy that must surround national security operations. Yet there is a legitimate public need to know. The Air India Inquiry reflects that public right.

The lessons that are learned from the inquiry into Air India must be lessons learned not only by government institutions but by the public at large. To accomplish this, there is a need to expand the potential of public knowledge and to make sure that it is sustained beyond the life of the Commission itself. The public needs to see that the inadequacies of past practices of intelligence production and CSIS-RCMP cooperation have been resolved. To that end, there is a requirement for a greater effort

on the part of the Government of Canada to inform the public about the on-going operations of its national security agencies and progress in achieving the objectives of partnership and integration. There is also a need for a greater public research capacity into the history of our national security institutions. The Government of Canada should be encouraged to create a dedicated funding mechanism to encourage in-depth research and writing on the Air India disaster and on other cases of terrorist threats to Canadian society. The Government should also be encouraged to release to the National Archives for open research all historical documents relating to the Canadian response to Sikh extremism, with exemptions applied only where strictly necessary on national security grounds. We need to open up both our historical and our present national security activities to greater and more informed public scrutiny. Only when we do so will we have a baseline for gauging success in the complex world of security intelligence and enforcement.

Wesley Wark

Wesley Wark is an associate professor at the University of Toronto's Munk Centre for International Studies, where he has taught since 1988. He is also a visiting research professor at the University of Ottawa's Graduate School of Public and International Affairs. He earned his degrees from Carleton University (BA), Cambridge (MA) and the London School of Economics (Ph.D). Prior to joining the University of Toronto, he held teaching appointments at McGill University and the University of Calgary.

Professor Wark is one of Canada's leading experts on intelligence and national security issues. He is a Past-President of the Canadian Association for Security and Intelligence Studies (1998-2000 and 2004-2006). He serves on the Canadian government's Advisory Council on National Security and the Advisory Committee to the Canada Border Services Agency.

He is completing a book on the history of Canada's intelligence community in its formative years from the end of World War two to the height of the Cold War, and a study of contemporary Canadian national security policy and counter-terrorism. His most recent scholarly publications include a special issue of the International Journal, published by the Canadian Institute for International Affairs/Canadian International Council, devoted to the subject of "Security in an Age of Terrorism," (Winter issue 2004/05) and an edited volume, Twenty-First Century Intelligence (London: Routledge, 2005). A new edited collection, Understanding Secret Intelligence, co-edited with Richard Aldrich and Christopher Andrew, is due out later in 2008.

He is co-director, with Mel Cappe, of a major research project funded by the Institute for Research on Public Policy on "Security and Democracy."

In 2006, he completed a study of key research issues in national security and human rights for the Canadian Human Rights Commission and served as an expert court witness on the history of Canada's official secrets legislation. In 2008 he completed an expert witness report on Canada's Marine Transportation Security Clearance Program, which is before the Federal Court.

Professor Wark is a frequent commentator in the media on security and intelligence issues and is a regular book reviewer for The Globe and Mail.