

## VOLUME TWO

### PART I: PRE-BOMBING

#### CHAPTER III: WHAT WENT WRONG?

##### 3.0 The CSIS Act

This section provides a general overview of the *Canadian Security Intelligence Service Act*<sup>1</sup> (*CSIS Act*) and an in-depth look at some of the key sections of the *CSIS Act*.

The government's decision to create a new civilian intelligence service was rooted in the scandals that had plagued the RCMP Security Service (SS) and the resulting McDonald Commission<sup>2</sup> into those activities. The result was a new organization and a new act, the *CSIS Act*, which propelled a change in culture, dramatically affecting CSIS operations and administration and the overall relationship between intelligence and evidence in Canada.

[W]e arrived at the *CSIS Act* in 1984, which ... gave it a legal mandate and provided for review and accountability mechanisms.<sup>3</sup>

On June 21, 1984, the *CSIS Act* was passed. The legislation created a framework for CSIS, a service without police powers and separate from the RCMP. It granted CSIS an explicit statutory charter, something that was rare among western democracies at the time.<sup>4</sup> The *CSIS Act* granted sole responsibility for security intelligence investigations to CSIS. It also imposed a requirement of obtaining judicially authorized warrants in order to employ the use of intercepts. CSIS was not given any enforcement powers.<sup>5</sup> Finally, the *CSIS Act* created two new review bodies for CSIS. The Security Intelligence Review Committee (SIRC) was established to provide external review and the Inspector General (IG) position was established to provide internal review. The role of these review bodies

---

<sup>1</sup> R.S.C. 1985, c. C-23.

<sup>2</sup> Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report – vol. 2 (Ottawa: Supply and Services Canada, 1981) [McDonald Commission, *Freedom and Security under the Law*].

<sup>3</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, pp. 1434-1435.

<sup>4</sup> Since 1975, the RCMP Security Service had drawn its mandate from a broadly worded Cabinet directive. Prior to that, the RCMP Security Service derived its authority from the power given to the Governor-in-Council in the *RCMP Act* to assign functions within the Force.

<sup>5</sup> Philip Rosen, "The Canadian Security Intelligence Service", revised January 24, 2000, online: Parliament of Canada <http://www.parl.gc.ca/information/library/PRBpubs/8247-e.pdf> (accessed October 27, 2009).

was to act as watchdogs to ensure that CSIS activities remained within the law, to avoid a previous problem of the RCMP SS as highlighted by the McDonald Commission.

The *CSIS Act* attempted to address the twin requirements of security and democracy, as recommended by the McDonald Commission. Geoffrey O'Brien described security intelligence agencies as having four parts: "...mandate, powers, controls and review." The mandate and powers allow for what you can investigate and how. The controls and review deal with "the requirements of democracy," ensuring that the Service acts according to what society wants and within "the norms of society."<sup>6</sup>

### **Key Sections of the Act**

The CSIS Act has a number of key sections:

#### **Section 2**

Section 2 of the *CSIS Act* contains the relevant definitions for the Act. Of particular note is the definition of threats to the security of Canada which defines CSIS's mandate:

"threats to the security of Canada" means

- (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
- (b) foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
- (c) 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, religious or ideological objective within Canada or a foreign state, and

---

<sup>6</sup> Testimony of Geoffrey O'Brien, vol. 17, March 6, 2007, p. 1542.

(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

The definition in the *CSIS Act* above is relatively short, in comparison, for example, to the three page long definition of “terrorist activity” found in the *Anti-terrorism Act*.<sup>7</sup> While the definition in the *CSIS Act* does overlap with criminal acts such as espionage, or the use of acts of serious violence, the definition also encompasses activities which are not crimes or may not be considered crimes.<sup>8</sup>

CSIS is therefore mandated to investigate a broader spectrum of threats than those covered by criminal legislation, and yet terrorism, as well as other activities considered criminal, also falls within CSIS’s threat definition. This therefore results in an overlap in mandates between CSIS and the RCMP.

## Section 6

Section 6 of the *CSIS Act* bestows authority of direction of the Service on the Director of the Service “...under the direction of the Minister.” Section 6(2) provides that the Minister may issue directives to the Service as a means of providing that direction. According to Reid Morden, who served as a Director of the Service, the independence of CSIS was “...carefully calibrated by the fact that the Act deliberately gives the Minister direct oversight and supervision of the Service.”<sup>9</sup>

## Section 12

Section 12 of the *CSIS Act* provides the legislative authority for CSIS to retain the information it gathers. It also contains an important and controversial qualifier in the term “strictly necessary”:

The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.<sup>10</sup>

<sup>7</sup> S.C. 2001, c. 41. See Testimony of Geoffrey O’Brian, vol. 16, March 5, 2007, p. 1529.

<sup>8</sup> Testimony of Geoffrey O’Brian, vol. 16, March 5, 2007, p. 1529.

<sup>9</sup> Testimony of Reid Morden, vol. 88, December 4, 2007, p. 11458.

<sup>10</sup> *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 12 [*CSIS Act*].

CSIS understood this qualifier to respond to concerns by the McDonald Commission about the RCMP Security Service practices in collecting and retaining information on Canadians indiscriminately.<sup>11</sup>

Section 12 permits CSIS to collect information which it then turns into intelligence. It is from this section that CSIS developed policies, not only with regard to the retention of intelligence, but equally importantly, for dealing with evidence. This led to a *de facto* prohibition on CSIS collecting evidence, and eventually to policies that led to information that might be considered evidence being routinely erased, notably intercepts and intelligence officer notes.<sup>12</sup> It was due to the absence of any mention of evidence in s.12 that Archie Barr wrote the oft-quoted memo stating that it would no longer be CSIS policy to retain evidentiary recordings:

As the CSIS Act contains no requirement for collection by the Service of information for evidentiary purposes, no such capacity will be provided for within CSIS facilities.<sup>13</sup>

The correct interpretation of this section was debated throughout the Inquiry. CSIS witnesses consistently maintained that the “strictly necessary” qualifier applied to what CSIS can “analyze and retain” as well as “collect”:

One of the outcomes of the McDonald Royal Commission, was a concern that was shared by the government that the new organization, the new Security Intelligence organization would have strict limits on what it could collect – what it collected in terms of private information on Canadians. So there were statutory limitations placed upon what we could collect and what we could retain. And the section of the Act specifically says that we can – we could only collect and retain information that is strictly necessary in our effort to advise government on threats to the security of Canada. So that was a very, very distinct and strong limitation on what we could do with our information.<sup>14</sup>

The Supreme Court of Canada, in *Charkaoui*,<sup>15</sup> has definitively rejected this interpretation, pointing out that both grammatically and logically “strictly necessary” in s.12 refers only to collecting, and not to analysis or retention. Nevertheless, historically, SIRC accepted and supported the CSIS interpretation that limited its ability to retain information. Consequently, 800,000 files inherited from the RCMP Security Service were disposed of by CSIS in due course.<sup>16</sup>

---

<sup>11</sup> Testimony of Reid Morden, vol. 88, December 4, 2007, p. 11430.

<sup>12</sup> Testimony of Reid Morden, vol. 88, December 4, 2007, p. 11430.

<sup>13</sup> Exhibit P-101 CAA0040.

<sup>14</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, pp. 6119-6120.

<sup>15</sup> *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326.

<sup>16</sup> Testimony of Kent Roach, vol. 81, November 22, 2007, p. 10395.

In retrospect, some senior CSIS members, including James (“Jim”) Warren, have questioned the extreme focus placed on s.12, the “strictly necessary” qualifier and the overly cautious limitation to collect only intelligence:

[T]he pendulum perhaps had swung too far and maybe we were being overly sensitive to this issue and overly cautious ... generally pervading the service of the day – was this idea that we had to pay a lot more attention to things like the privacy of Canadians ... and especially those that weren’t suspected of being involved in subversive activities.<sup>17</sup>

### Section 18

Section 18(1) reflects the continued emphasis on secrecy that carried over from the RCMP Security Service to CSIS. It states that CSIS is not permitted to disclose information collected and, in particular, prevents the disclosure of the identity of CSIS human sources and CSIS employees involved in covert activities.

Section 18(2) does contemplate that CSIS information may need to be disclosed to law enforcement, though read in conjunction with s. 19(2), CSIS is vested with the discretion to disclose through the use of the word “may.”<sup>18</sup>

### Section 19

Section 19 of the *CSIS Act* provides the legislative authority for CSIS to lawfully disclose information it has collected.<sup>19</sup> Information collected by CSIS may not be disclosed unless disclosure is required for the fulfillment of its duties, namely threat-related advice to the Government of Canada (section 12), security screening and security advice to the immigration and citizenship program (sections 13 to 15), and foreign intelligence information (section 16). CSIS needs to disclose this type of information to the government in order to fulfill its mandate.

Section 19(2) also outlines circumstances in which information collected, that is not specifically related to the CSIS mandate, may also be disclosed. Of particular note is section 19(2)(a), which provides for the passage of information from CSIS to law enforcement; an issue of great concern throughout the Air India investigation. The section notes that information gathered by CSIS may have value to law enforcement and that it “...can lawfully disclose that information to the relevant police force and prosecutors” despite the secrecy mandated in s. 18:<sup>20</sup>

---

<sup>17</sup> Testimony of James Warren, vol. 48, September 19, 2007, p. 5941.

<sup>18</sup> Testimony of Kent Roach, vol. 80, November 21, 2007, pp. 10230-10231.

<sup>19</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, p. 1555.

<sup>20</sup> Testimony of Kent Roach, vol. 80, November 21, 2007, pp. 10230-10231.

The Service *may* disclose information ... where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or province, to a police officer having jurisdiction to investigate the alleged contravention and to the Attorney General of Canada and the Attorney General of the province in which proceedings of the alleged contravention may be taken.<sup>21</sup>

Section 19(2)(b) is similar to s. 19(2)(a) except that it refers to CSIS information relating to international affairs. Similarly, s. 19(2)(c) is in relation to CSIS information of interest to national defence.<sup>22</sup>

Because s. 19(2) is permissive through the use of the word “may”, the question of when information should be passed soon became a hotly debated issue. Policy and operational requirements are at the heart of the problem. The actual CSIS response depends on a CSIS-only analysis of “...when is it appropriate to pass information of that nature, in what circumstances are there policy reasons for doing so,” and whether there are “...operational reasons for doing so.”<sup>23</sup> What is clear is that, despite the Pitfield Committee’s description of the stark dichotomy between intelligence and evidence, the *CSIS Act* has always contemplated a relationship between intelligence and evidence and there has never been a “statutory wall” between the two.<sup>24</sup>

## Section 21

Section 21 of the *CSIS Act* provides for the Service’s warrant powers. The section makes clear that every warrant must first receive approval by the Minister and, once that approval has been received, the warrant application must be brought before a judge of the Federal Court.<sup>25</sup>

## Review Bodies

Part III of the *CSIS Act* provides for review bodies, which are designed to make sure that CSIS acts within the law. These review bodies were created by the *CSIS Act* and did not exist in any form within the old RCMP Security Service.

The system created is one of review and not oversight. Oversight implies inspection of current operations and involvement in the critique of current operations. Instead, the *CSIS Act* created the SIRC and the Inspector General (IG)’s office to look retrospectively at CSIS’s performance. The idea of the review programs was to allow the Minister to be held more accountable without deeply involving the Minister in all the operational details.<sup>26</sup>

<sup>21</sup> *CSIS Act*, ss. 19(2), 19(2)(a) [Emphasis added].

<sup>22</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, pp. 1555-1556.

<sup>23</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, p. 1557.

<sup>24</sup> Testimony of Kent Roach, vol. 80, November 21, 2007, p. 10231. See Volume Two of this Report: Part 1, Pre-Bombing, Chapter III, What Went Wrong?, for a full discussion of these issues.

<sup>25</sup> The definition of “judge”, for the purpose of the *CSIS Act*, is found in section 2 of the Act.

<sup>26</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, pp. 1438-1439.

The IG's office, an internal mechanism, was specifically created in order to provide the Minister's office with "...better insight into the operations."<sup>27</sup> An important aspect of the *CSIS Act* is the frequent mention of the Deputy Minister. Rarely is the role of a Deputy Minister mentioned in legislation.<sup>28</sup> In the *CSIS Act*, the Deputy Minister is given a leading role in what seems to be an effort to temper any partisan politics in the exercise of political control over CSIS operations. According to the *CSIS Act*, the Deputy Minister is to be consulted on operational policies.<sup>29</sup> As well, the Deputy Minister must be consulted on warrant applications.<sup>30</sup> Under s. 30, the IG reports to the Deputy Minister. The IG provides an annual certificate to the Minister that is meant to certify that CSIS is complying both with the law and with ministerial directives.<sup>31</sup>

On the other hand, SIRC, an external mechanism, is "...an independent, external review body which reports to the Parliament of Canada on the operations of [CSIS]."<sup>32</sup> SIRC's role is to monitor CSIS's compliance with the *CSIS Act*. SIRC is comprised of members of the Queen's Privy Council for Canada who are not members of the Senate or the House of Commons.<sup>33</sup> They are appointed through a process of all-party consultation in the House of Commons. SIRC is intended to strengthen parliamentary accountability by reporting to the Minister. SIRC also plays the important role of informing the public about the actions of CSIS.<sup>34</sup>

### **Security Offences Act**

To understand the roles and responsibilities of CSIS vis-à-vis the RCMP, it is important to understand the *Security Offences Act*.<sup>35</sup>

The *Security Offences Act* was passed at the same time as the *CSIS Act* and also arose out of the changes recommended by the McDonald Commission.<sup>36</sup> Though the *CSIS Act* removed the security intelligence duties from the RCMP and gave them to CSIS, the *Security Offences Act* granted the RCMP significant duties in relation to criminal investigations regarding national security criminal offences.<sup>37</sup>

A comparison and analysis of the *CSIS Act* in conjunction with the *Security Offences Act* show that "overlapping jurisdiction" has always existed between the two agencies in relation to terrorism investigations.<sup>38</sup>

<sup>27</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, p. 1439.

<sup>28</sup> Testimony of Geoffrey O'Brian, vol. 16, March 5, 2007, p. 1534.

<sup>29</sup> *CSIS Act*, s. 7(1).

<sup>30</sup> *CSIS Act*, s. 7(2).

<sup>31</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, p. 1439.

<sup>32</sup> Online: Security Intelligence Review Committee <<http://www.sirc-csars.gc.ca/index-eng.html>> (accessed October 27, 2009).

<sup>33</sup> *CSIS Act*, s. 34(1).

<sup>34</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, pp. 1439, 1463.

<sup>35</sup> R.S.C. 1985, c. S-7.

<sup>36</sup> Testimony of Kent Roach, vol. 80, November 21, 2007, pp. 10233-10234.

<sup>37</sup> *Security Offences Act*, R.S.C. 1985, c. S-7, s. 6 [*Security Offences Act*].

<sup>38</sup> Testimony of Kent Roach, vol. 80, November 21, 2007, p. 10235.

Section 2(a) contemplates RCMP investigation of actions, mainly *Criminal Code* offences, falling within the definition of threats to the security of Canada as defined by the *CSIS Act*:<sup>39</sup>

2. Notwithstanding any other Act of Parliament, the Attorney General of Canada may conduct proceedings in respect of an offence under any law of Canada where

(a) the alleged offence arises out of conduct constituting a threat to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*, or

The *Security Offences Act* also provides the Attorney General of Canada with a fiat that "...establishes the exclusive authority of the Attorney General of Canada."<sup>40</sup>

Finally, the *Security Offences Act* recognizes that the RCMP has "the primary responsibility" in relation to offences that also constitute a threat to the security of Canada.<sup>41</sup>

### 3.1 Internal CSIS Structure

The primary mandate of CSIS was to collect, analyze and disseminate intelligence to advise the Government of Canada on threats to national security. The RCMP, along with Ministers and other government agencies, relied on CSIS threat assessments to develop appropriate policy and operational responses to any national security threats.

The Commission investigated the adequacy of the CSIS threat assessment process in the period leading up to the Air India and Narita bombings. The questions asked were:

- How was CSIS organized?
- What did CSIS know?
- What went wrong?

This chapter presents the answers to these questions as uncovered by the Commission's investigation into the Government's action in the pre-bombing period.

#### How Was CSIS Organized? CSIS Threat Assessment Structure

CSIS was a highly centralized organization with a specific mandate to investigate and advise the Government of Canada on threats to the security of Canada.

---

<sup>39</sup> Testimony of Kent Roach, vol. 80, November 21, 2007, pp. 10233-10234.

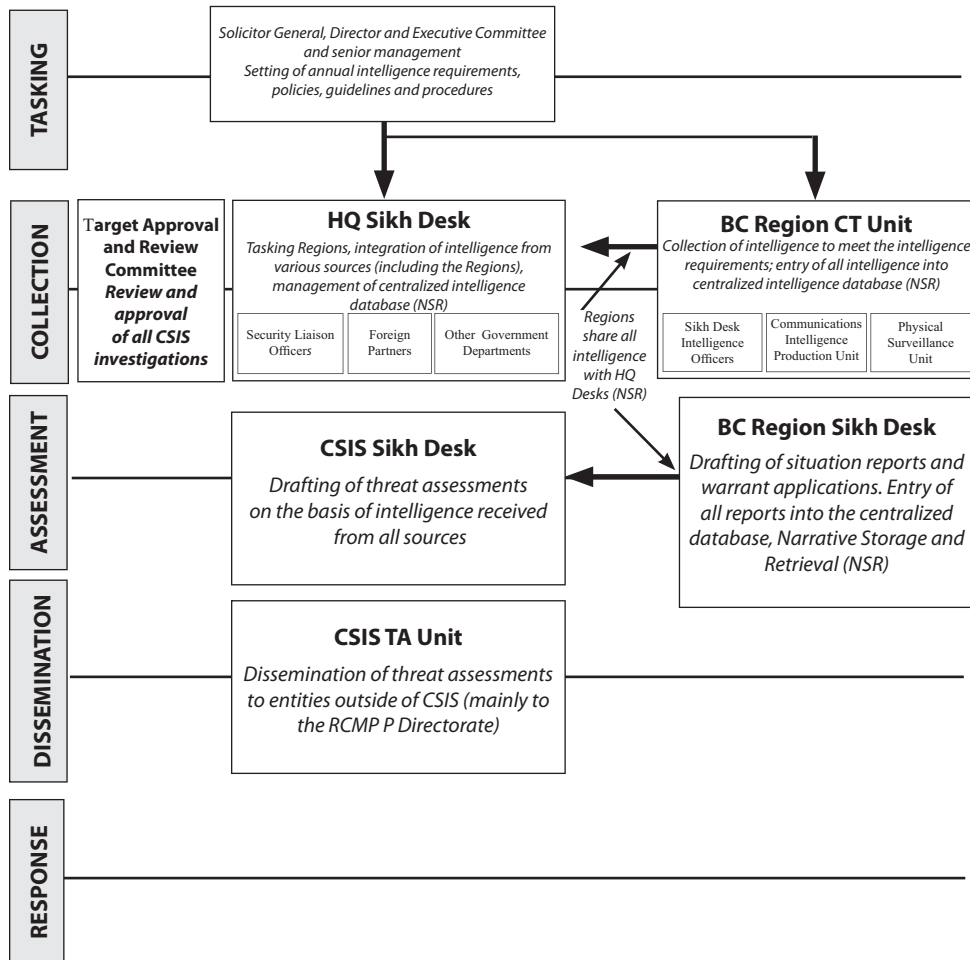
<sup>40</sup> *Security Offences Act*, s. 4.

<sup>41</sup> *Security Offences Act*, s. 6.



CSIS Headquarters (HQ) coordinated overall CSIS investigations by developing operational policies and setting annual intelligence requirements. The regional offices undertook the intelligence collection efforts to meet these requirements but had relative autonomy over the assignment of resources for this purpose. HQ was responsible for maintaining a centralized intelligence database to ensure that intelligence collected from various sources on related investigations was properly assembled.

The roles and responsibilities of the various units involved in the CSIS assessment of the threats of Sikh extremism in the pre-bombing period are described below, with a focus on each unit's role in each component of the intelligence cycle: tasking, collection, analysis and dissemination.



**Figure 1: Organization of CSIS Units involved in Sikh Extremism Investigation**

### ***Solicitor General***

The Solicitor General provided guidance and oversight over “tasking” priorities for CSIS operations. The security intelligence activities of CSIS operated under political control, as recommended by both the McKenzie and McDonald Commissions:

Two Royal Commissions in the past fifteen years ... concluded that security intelligence work was different from law enforcement and that security intelligence activity needs more government direction than is appropriate for police work. Police have in the criminal law, as CSIS has in statute, clear direction from Parliament as to their proper targets; but the job of the police, in every case, is to seek to gather evidence, lay charges and bring matters before the Court. So far as police work is concerned the laying of charges normally can and should take place without government direction.

Security intelligence investigation in relation to a particular target is often long-term and recourse to the criminal courts is only one of a number of possibilities for dealing with a threat. The ultimate choice of the method of dealing with any threat must be the responsibility of the Government. Government direction is also required in relation to the attitude to be taken towards various foreign governments and agencies in a rapidly changing international environment.<sup>42</sup>

The *CSIS Act* enshrined political accountability. Ministerial approval was a requirement for all CSIS warrants, which authorized CSIS's most intrusive investigative techniques.<sup>43</sup> The Solicitor General could issue directions to the CSIS Director regarding the control and management of CSIS.<sup>44</sup> The CSIS Director was directed to consult with the Deputy Solicitor General on CSIS's operational policies and investigations.<sup>45</sup> Ministerial approval was also required for all cooperative agreements between CSIS and other Canadian government and foreign agencies.

The Solicitor General position was filled by the Honourable Robert Kaplan from March 3, 1980 to September 16, 1984 and by the Honourable Elmer MacKay from September 17, 1984 to August 19, 1985. Minister Kaplan issued three key Ministerial Directives:

---

<sup>42</sup> Exhibit P-101 CAF0030, p. 1.

<sup>43</sup> *CSIS Act*, s. 21.

<sup>44</sup> *CSIS Act*, s. 6(2).

<sup>45</sup> *CSIS Act*, s. 7.

- (a) the 1980 Directive on tape retention policy;
- (b) the 1984 Directive on the division of CSIS and RCMP responsibilities after CSIS's creation; and
- (c) the 1984 Directive advising that all RCMP SS Directives, policies and guidelines not inconsistent with the *CSIS Act* were to remain in effect.<sup>46</sup>

Minister MacKay was involved in several post-separation issues. In general, however, the department of the Solicitor General issued general policies and left the RCMP and CSIS to work out the operational details of implementing these policies on their own.

### ***Target Approval and Review Committee***

The Target Approval and Review Committee (TARC) was responsible for assessing and approving all CSIS targets and, in doing so, acted as an approval body for CSIS's collection efforts. The Committee included the CSIS Director, the Deputy Director National Requirements, legal staff and representatives from the Solicitor General's office. The TARC would consider whether the investigative means chosen were proportional to the gravity and imminence of the threat. Care was taken to balance the intrusiveness of the investigation with respect for the rights and freedoms of those being investigated. The TARC would also consider whether resources were available for the processing of the warrant.<sup>47</sup>

This system ensured a measure of political oversight, right from the start, for all CSIS investigations against organizations and individuals. All CSIS targets were thus considered and approved by very senior management, a process that, although time-consuming and bureaucratic, ensured the political oversight that the McKenzie and McDonald Commissions had envisioned.

### ***CSIS Director and Senior Executive Committee at HQ***

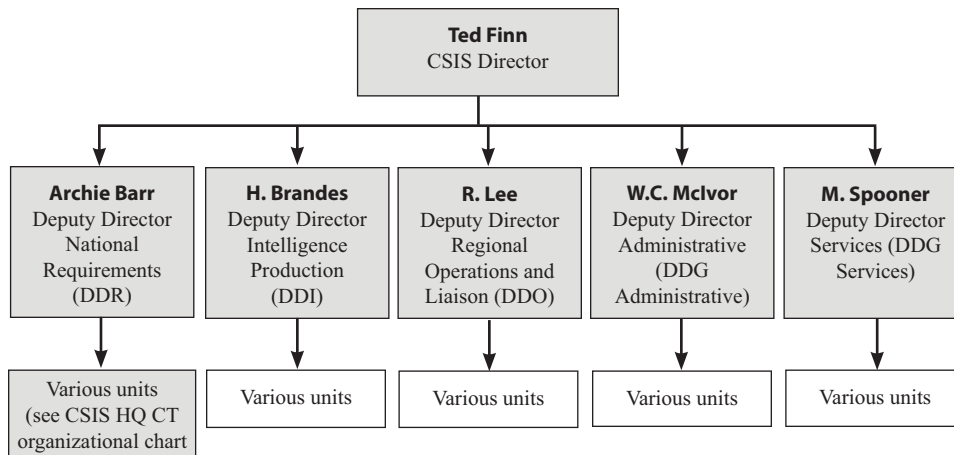
The CSIS Director and the Senior Executive Committee, consisting of five deputy directors, were responsible for setting the tasking priorities for CSIS, as well as for providing tasking guidance for the collection, analysis and dissemination of CSIS's intelligence product.

At the head of CSIS was the Director, who reported to the Solicitor General and, in the original structure of CSIS created by the Security Intelligence Transition (SIT) Group, was supported by five deputy directors.

---

<sup>46</sup> Exhibit P-101 CAA0812. These Ministerial Directives are Exhibit P-101 CAA0011, CAA0081 and CAA0091 respectively.

<sup>47</sup> Exhibit P-437: Statement of Archie Barr, p. 5; Exhibit P-101 CAD0003, p. 8.



**Figure 2: Organization of CSIS HQ Executive Committee**

\*Highlighted units were involved in the Sikh extremism investigation.

The first CSIS Director, Ted Finn, was a civilian with no operational intelligence experience, unlike his five deputy directors who had risen up through the RCMP SS ranks. The five deputy director structure was considered important to ensure Finn was properly supported, while avoiding concentrating power in the hands of one deputy director who could effectively usurp Finn's role.

One of the structures of the CSIS hierarchy was that there were five Deputy Directors with purposely overlapping responsibilities. Among other things, this reflected the concern that the ex-RCMP officers being appointed as Deputy Directors might effectively usurp the duties of the civilian Director. No one Deputy Director therefore had complete control of any sphere of operations.<sup>48</sup>

This "overlapping" executive structure did, however, create difficulties, as responsibility for various functions remained unclear. The role of the Deputy Director of National Requirements, Archie Barr, became so important that Barr soon became the *de facto* lead deputy director.<sup>49</sup>

In 1984-85, the CSIS HQ Senior Executive Committee had the following primary responsibilities:

<sup>48</sup> Exhibit P-437: Statement of Archie Barr, p. 5.

<sup>49</sup> Today that position is called the Deputy Director Operations (DDO).

- Setting of annual Intelligence Requirements (IRs), as assigned to the CSIS Director,<sup>50</sup> under the direction of the Solicitor General.<sup>51</sup> Archie Barr, the Deputy Director of National Requirements was responsible for determining the intelligence targets that CSIS would focus on. Ray Lees, the Deputy Director, Regional Operations and Liaison was responsible for ensuring that the regional investigations did in fact meet the national IRs.
- Development of policies, procedures and guidelines (including the conversion of those inherited from the RCMP SS) to enable CSIS to carry out its mandate as defined by the *CSIS Act*.
- Ensuring that the Government of Canada received timely and relevant advice on threats to the security of Canada. H. Brandes, the Deputy Director of Intelligence Production, managed the units responsible for producing and disseminating assessed intelligence to various users. The assessed intelligence could take many forms, including briefings to advise Ministers and threat assessments to inform the operational responses by the RCMP and other government departments, both formal and informal.

### ***CSIS HQ Counter Terrorism (CT) Units***

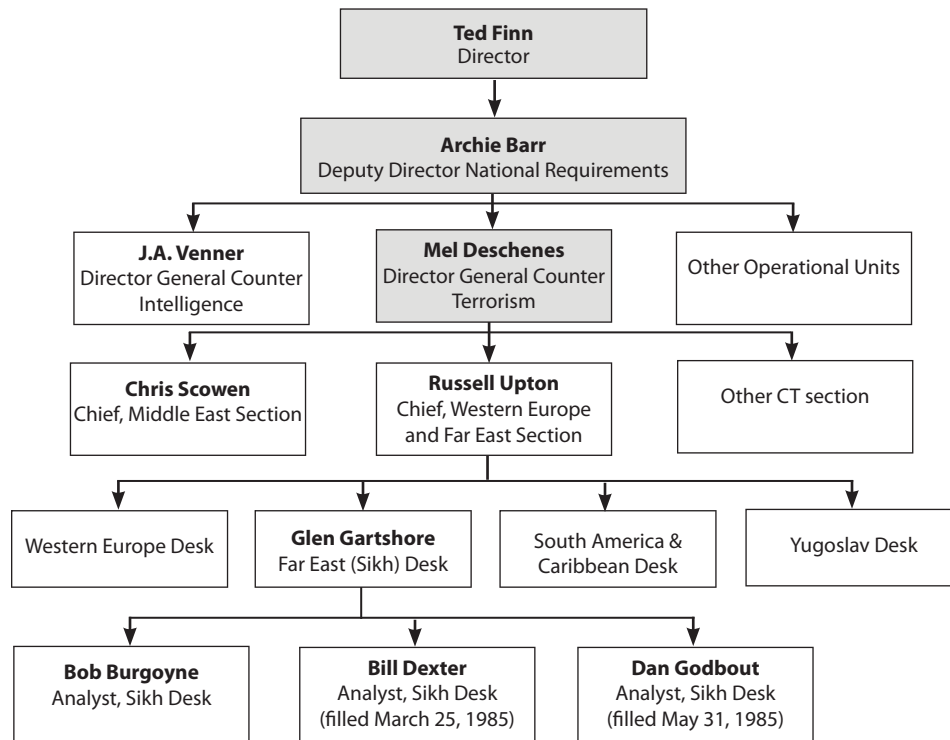
CSIS HQ Counter Terrorism (CT) Units had the primary role of integrating and analyzing intelligence collected by CSIS and its partners for the production of threat assessments. The CT Units were also responsible for ensuring the HQ tasking priorities were met by the Regions and for assisting the Regions' collection efforts by developing operational guidelines and supporting the Regions' applications for approval of various investigative powers.

All CSIS CT investigations were managed by Mel Deschenes, the Director General of CT. Deschenes reported directly to Archie Barr and was supported by three Section Heads who managed the work of numerous CT intelligence analysts.

---

<sup>50</sup> Section 6(1) of The *CSIS Act* grants the CSIS Director, under the direction of the Minister, control and management of CSIS and all matters connected therewith. The CSIS Director in 1985 was Ted Finn.

<sup>51</sup> Section 6(2) of The *CSIS Act* grants the responsible Minister the power to issue to the CSIS Director, written directions with respect to CSIS. At the time of the Air India bombing, the responsible Minister was the Solicitor General. In the present day, the responsible Minister is the Minister of Public Safety.



**Figure 3: Organization of CSIS HQ CT Units on Sikh Extremism Investigation**

Barr was actively involved in the operation of CSIS's CT investigations. Barr was responsible for developing operational policy and managing several operational divisions, including Counter-Intelligence (CI), CT, technical communications and foreign liaison. Barr had been involved with the SIT Group and was committed to ensuring CSIS operated in a manner that respected its new mandate. He was an active manager, involving himself in adjusting CSIS's practices to meet the new, more-intensive warrant requirements, and personally presented warrant applications to the Federal Court.

As Director General (DG) CT, Deschenes's portfolio was extensive, covering all counterterrorism investigations undertaken by CSIS. The CT investigations were divided into three geographic areas, each with its own Chief. Chris Scowen, Chief of the Middle East Section was the *de facto* lead Deputy DG CT, although this would not be formalized until August 1985. Scowen would fill in as the Acting DG CT whenever Deschenes was not available.<sup>52</sup> Deschenes was, in fact, absent during the week prior to the bombing. Accordingly, many, if not most, of the operational policy decisions in relation to the Sikh extremism investigation were made by Scowen (not Deschenes), in conjunction with Barr.

<sup>52</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, pp. 6127-6128.

Russell Upton was the Chief of the Europe and Far East Section at CSIS HQ, the section with the desk which eventually came to be known as the “Sikh Desk”. Upton reported directly to Deschenes up until the time of the bombing. Upton had four sections under his command, one of which was the Western Europe and Pacific Rim Section. In the fall of 1984, the work of this section was increasingly focused on Sikh extremism issues and was referred to as the “Sikh Desk.” This was a somewhat inaccurate characterization, as the Desk responsibilities were far broader than simply an assessment of the threat posed by Sikh extremists, and this desk retained several other continuing commitments related to its previous, broader title.

The Sikh Desk was led by Glen Gartshore. At the creation of CSIS, there was nominally provision for three analyst positions at the Sikh Desk. One of those positions was immediately filled by Robert (“Bob”) Burgoyne. Burgoyne soon became CSIS HQ’s “Sikh expert,” despite having started at the desk with no background in this area. The remaining analyst positions remained vacant for most of the pre-bombing period. One of the vacant analyst positions was filled in March 1985 by Bill Dexter (returned from French language training), with the final position filled in late May 1985 by Dan Godbout.<sup>53</sup> The Sikh Desk tasked the Regions and their investigators to collect the information needed to better assess and report on the threat of Sikh extremism in Canada.<sup>54</sup> CSIS HQ would receive information from liaison officers abroad, from domestic partners (such as the RCMP, CSE and Foreign Affairs) and well as from foreign intelligence agencies.<sup>55</sup> The Sikh Desk would integrate and analyze the information received from all sources, extract the tactical information and then task the Regions in response to perceived intelligence deficiencies or, alternatively, switch the focus of an investigation. The information received would be used to prepare threat assessments that would be disseminated within and outside CSIS.<sup>56</sup>

In 1984-85, the managers and analysts in the Counter Terrorism Units at CSIS HQ had the following primary responsibilities:

- The DG CT (Deschenes) and Section Chiefs (Upton and Scowen) were responsible for developing operational policy and allocating resources amongst competing CT investigations;
- The Sections were responsible for transmitting operational policy and the national IRs to all CSIS Regions and ensuring that the IRs were met;
- The Sikh Desk (Gartshore and Burgoyne) was responsible for tasking the Regions to satisfy the IRs and for assisting the Regions in their investigations. The Sikh Desk assisted with the approval process for TARC applications and warrant applications against selected targets. The Desks coordinated with the Warrant Acquisition

<sup>53</sup> Exhibit P-101 CAD0153, p. 3.

<sup>54</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, pp. 3462-3463.

<sup>55</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, pp. 3466, 3469-3470.

<sup>56</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2508.

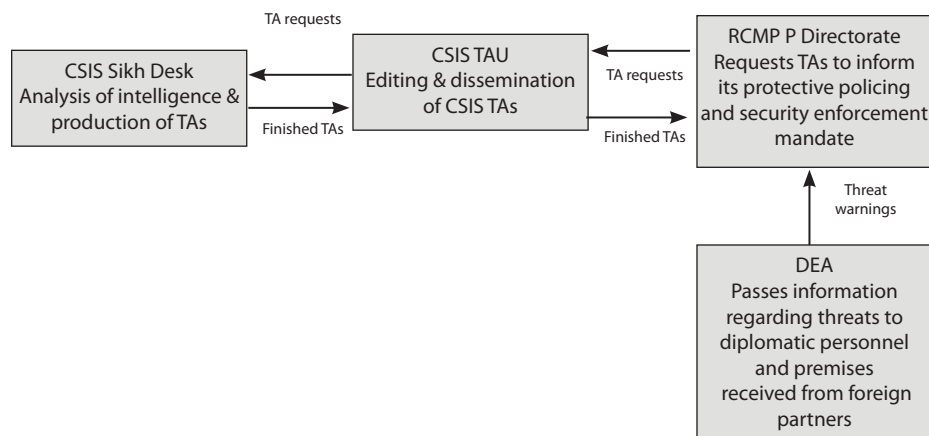
Control and Requirements (WAC&R) Unit of the Communications Intelligence Production (CIP) Division to process warrant applications submitted by the Regions.

- The Sikh Desk was responsible for integrating intelligence received from various sources, including the Regions, Security Liaison Officers (SLOs), foreign partners and other Canadian government departments and agencies (including the RCMP, DEA, CSE).

The Sikh Desk was responsible for analyzing all intelligence to produce threat assessments to advise Ministers or inform the operational responses by other government agencies, in particular the RCMP. The Desks coordinated with the Threat Assessment Unit (TAU), which was responsible for the dissemination of CSIS threat assessments outside of CSIS.

### ***Threat Assessment Unit***

The Threat Assessment Unit (TAU) was a two-person unit at CSIS HQ that was responsible for dissemination of CSIS threat assessments to other government agencies.



**Figure 4: Information Flow through the Threat Assessment Unit**

Threat assessments could be triggered through a request from another government agency or on CSIS's own initiative, in fulfillment of the mandate to advise government.<sup>57</sup> The agencies most commonly requesting threat assessments were the RCMP P Directorate and the DEA (through the RCMP). The RCMP P Directorate would request general updates on threats to mission personnel, on an ongoing basis, to ensure that protective policing resources were assigned to the highest priority threats or in response to specific information indicating a threat.<sup>58</sup> The DEA would pass on threat warnings from

<sup>57</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2528.

<sup>58</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3444.



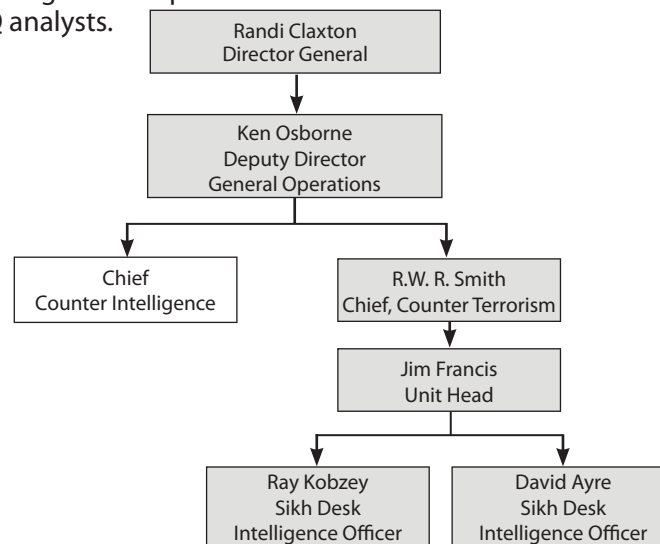
the Government of India.<sup>59</sup> The normal channel for diplomatic information on threats would be from the Indian Mission to External Affairs, to the RCMP P Directorate (VIP Security Branch), to the CSIS TAU.<sup>60</sup>

Upon receipt of a request for a threat assessment, the TAU at CSIS Headquarters would forward the request to the appropriate operational desk, which would then draft the assessment. In relation to a Sikh threat, the Sikh Desk would consider the available intelligence and draft a threat assessment, including as much relevant information and analysis as it felt appropriate. The Sikh Desk, usually Burgoyne, would submit the draft TA to the TAU, which would edit it to remove any information not deemed suitable for dissemination outside of CSIS. The TAU, as needed, might also substitute vocabulary more common to the police. Throughout this process, the TAU would remain in contact with the Sikh desk.

The TA Unit would enter the original TA request information, and resulting threat assessment, into the Narrative Storage and Retrieval (NSR) system for future reference.<sup>61</sup> The members of TAU were not expected to be expert in any one subject or geographical area but, instead, were tasked to respond to TA requests from all government agencies, as well as to disseminate TAs produced by CSIS in a manner deemed appropriate for use outside CSIS.

### **BC Region CT Units**

The BC Region CT Units had the primary responsibility for collecting intelligence to meet the Intelligence Requirements and inform the threat assessments produced by HQ analysts.



**Figure 5: Organization of BC Region Units on Sikh Extremism**

<sup>59</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3461; Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3549-3550.

<sup>60</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2540-2541.

<sup>61</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2528.

## Investigation

Sikh extremist sentiment was prevalent in the BC Region in 1984-85, and that Region was a key focus of the intelligence collection effort. The BC Region was led by Randil Claxton, the Director General (DG BC). Although the Regions were relatively autonomous, Claxton would periodically discuss the investigation with CSIS HQ through Ray Lees, the HQ DDO who was responsible for ensuring regional investigations met the Intelligence Requirements.<sup>62</sup> Claxton oversaw the work of various managers and investigators involved in the Sikh extremism investigation.

While the Regions relied on CSIS HQ for the annual IRs, they maintained a high degree of autonomy over the management of their investigations. All regional personnel, including the translators, transcribers, physical surveillance units and investigators, reported directly to Claxton, who had the authority to place his resources where he felt he would get the best return.<sup>63</sup>

Ken Osborne was the Deputy Director General Operations (DDG Ops) at BC Region. He was responsible for allocating resources amongst competing CI, CT and other investigations carried out in the Region. Robert Smith was the Chief of CT and managed various CT units. Jim Francis was one of the Unit Heads. He managed four or five two-man intelligence officer (IO) Desks<sup>64</sup> one of which was responsible for the investigation into Sikh extremism. The two IOs assigned to the Sikh Desk were Ray Kobzey and David Ayre.

In 1984-85, the managers and investigators in the Counter Terrorism Units at BC Region had the following primary responsibilities:

- The DG BC (Claxton) was responsible for allocating resources to meet the annual Intelligence Requirements set by CSIS HQ.
- The Chief, Counter Terrorism (Smith) was responsible for allocating resources amongst competing CT investigations in the Region. These resources included Physical Surveillance Units (PSU) and Communications Intelligence Production (CIP) personnel (translators, transcribers and intelligence monitors).
- The Unit Head (Francis) was responsible for ensuring that intelligence collected by the regional investigations was properly disseminated within CSIS by transmission to the CSIS HQ Sikh Desk and entry into CSIS's centralized database, the Narrative Storage and Retrieval (NSR) system.

---

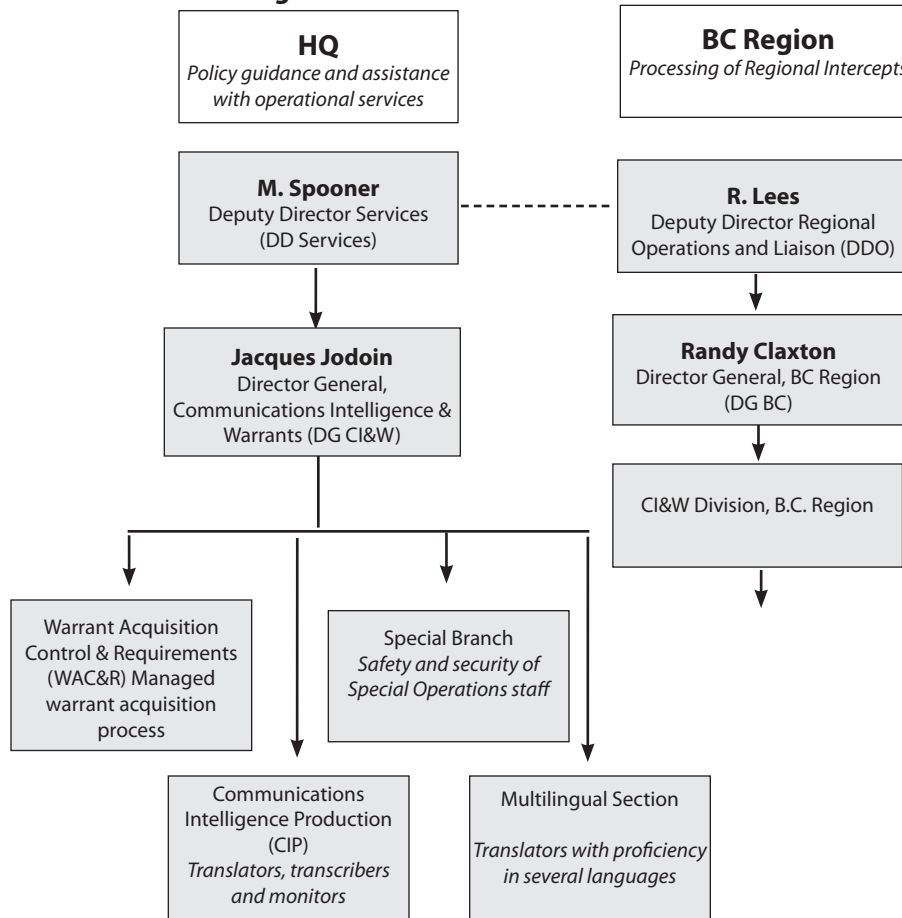
<sup>62</sup> Exhibit P-437: Statement of Archie Barr, p. 5.

<sup>63</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6127.

<sup>64</sup> Exhibit P-101 CAD0115, pp. 4-5.

- The Intelligence Officers (Kobzey and Ayre) were responsible for collecting, assessing and reporting to Headquarters information relevant to the Intelligence Requirements through a range of investigative techniques. The IOs worked closely with the PSU, translators and transcribers.

### Communications Intelligence and Warrants



**Figure 6: Organization of CSIS CI&W Divisions at HQ and BC Region**

At HQ, the Communications Intelligence and Warrants Section (CI&W) was responsible for the management and processing of technical intercepts. The section was part of the operational support services and came under the command of Deputy Director M. Spooner.<sup>65</sup> Jacques Jodoin was the Director General, Communications Intelligence and Warrants (DG CI&W), from 1984 to 1988.<sup>66</sup>

<sup>65</sup> Testimony of Jacques Jodoin, vol. 49, September 20, 2007, pp. 6072-6073.

<sup>66</sup> Testimony of Jacques Jodoin, vol. 49, September 20, 2007, p. 6032.

The CI&W Section was composed of four units. The main section, the Warrant Acquisition Control & Requirements Unit (WAC&R), was responsible for warrant acquisition and had a staff of seven people. They created the policy for the process of warrant applications. A second section, Communications Intelligence Production, was composed of transcribers and translators. They were responsible for taking raw product off machines and writing reports. There were 75 employees in that section servicing the Ottawa region. A third section, the Special Branch, or Special Unit, was quite small and dealt with the safety and security of the technicians who surreptitiously installed intercept technology. The fourth section was called the Multilingual Section and contained 20 translators with proficiency in about 28 languages. They translated written material, as opposed to communication intercepts.<sup>67</sup>

Each region also had its own CI&W division, which mirrored the structure which existed at HQ. CI&W was considered a support service and was managed separately from the operational sections (such as CT and CI), although it worked closely with them. Although Jodoin provided indirect overall supervision and policy guidance from HQ, the regional CI&Ws reported to their regional Director General.<sup>68</sup> Jodoin would communicate policies directly with the regional DGs<sup>69</sup>, but the responsibility to decide whether and how to implement these policies within the regional CI&W Units remained with the regional DGs, such as Claxton.

## 3.2 The CSIS Investigations into Sikh Extremism

### What Did CSIS Know?

At the time of the Air India bombing, CSIS had collected a wealth of intelligence about the Sikh extremist movement in Canada. RCMP Security Service (SS) officers, later CSIS investigators, had been aware of the threat of Sikh extremism within Canada since 1981 and continued to monitor the growing threat through the following years. Major investigations were underway in the BC, Toronto and Windsor regions, with the national investigation coordinated by the Sikh Desk at CSIS HQ. This section describes the CSIS investigation into Sikh extremism which demonstrates the intelligence known by CSIS at the time of the Air India tragedy. On this basis, it will then be possible to assess whether CSIS handled this information properly in analyzing and responding to the threat of Sikh extremism in Canada.

### HQ Investigation

#### *Growing Awareness of Sikh Extremism in Canada*

The RCMP Security Service first became aware of Sikh extremism in late 1974 when Dr. Jagjit Singh Chauhan, widely viewed as the founder of the Khalistan

<sup>67</sup> Testimony of Jacques Jodoin, vol. 23, May 4, 2007, pp. 2242-2243.

<sup>68</sup> Testimony of Jacques Jodoin, vol. 49, September 20, 2007, p. 6071.

<sup>69</sup> Testimony of Jacques Jodoin, vol. 49, September 20, 2007, p. 6073.

movement, created “Khalistan Consulates” in Toronto, Vancouver and Winnipeg. At the time, the Khalistan movement was not considered by the Security Service to constitute a threat to the security of Canada.<sup>70</sup>

The investigation into Sikh extremism by the RCMP SS began in the fall of 1981.<sup>71</sup> Glen Gartshore, head of the Western Europe/Pacific Rim Desk at HQ, testified that he first became aware of the issue of Sikh extremism when the Government of India (GOI) made representations to the Department of External Affairs concerning activities being carried out in Canada. A particular concern for the GOI was a group of Sikhs in Winnipeg promoting an independent state of Khalistan through the creation and distribution of “Khalistan passports” and “Khalistan currency.” Though the concerns raised by the GOI were in relation to activities in Winnipeg, the RCMP SS investigation focused mainly on activities in Ontario and British Columbia.<sup>72</sup>

Between 1981 and 1984, a number of Sikh extremism events in Canada were noted in the continuing low-level RCMP SS investigation:

- March 18, 1982: Kuldip Singh Samra became enraged after his bid to overturn an election at a local Sikh temple was denied by a judge. He opened fire in an Osgoode Hall courtroom in Toronto killing two men and putting a third in a wheelchair.
- May 8, 1982: Dr. Gurdian Singh Dhillon, the Government of India High Commissioner to Canada, was met at Vancouver Airport by a group of Sikhs who chanted and pelted him with eggs.
- October 16, 1982: 500 protesters marched to the Indian Consulate in Vancouver.
- November 14, 1982: Metro Toronto Police Constable Christopher Fernandes was shot at a Sikh demonstration outside the Indian Consulate in Toronto.
- June 29, 1983: Talwinder Singh Parmar was arrested in West Germany pending extradition to India where he was accused of murdering two police officers.<sup>73</sup>
- July 6, 1984: Parmar was released from German prison and returned immediately to Canada because the German government would not extradite him to India.
- July 18, 1984: While visiting Winnipeg, the acting Indian High Commissioner was assaulted by five Sikhs.

---

<sup>70</sup> Exhibit P-101 CAA1086, p. 2.

<sup>71</sup> Testimony of Glen Gartshore, vol. 31, May 22, 2007, p. 3518.

<sup>72</sup> Exhibit P-101 CAA1086, p. 2.

<sup>73</sup> Exhibit P-101 CAA1046, Annex A.

### ***1984 Application for Level 2 Monitoring Coverage***

On April 11, 1984, Gartshore wrote to Staff Sergeant Russell Upton, his superior, to apply for level 2 coverage for Sikh extremism in Canada.<sup>74</sup> Level 2 monitoring allowed for investigators to talk to people in the community to help evaluate what was happening in Canada.<sup>75</sup> The concern was that communal violence in India involving Sikhs, including acts of terrorism, would spill over into Canada.<sup>76</sup> The RCMP SS was particularly concerned for the safety of Indian missions in Canada and the level 2 monitoring application was intended to help keep track of that threat.

### ***Analyst Joins the Western Europe & Pacific Rim Desk***

In the spring of 1984, analyst Bob Burgoyne joined Gartshore on the Western Europe & Pacific Rim Desk in the position of analyst, after working in counterterrorism and counter-intelligence (CI) on the Yugoslav Desk. At the time, the concerns of the Western Europe & Pacific Rim Desk were tied to the ongoing Cold War. Burgoyne had CI responsibilities relating to European-based terrorist groups. In connection with the Asian sub-continent, however, he was responsible for Sikh extremism and this soon became his main focus. Nevertheless, until the fall of 1984, Burgoyne retained other important responsibilities including Western terrorist groups and the Tamil Tigers from Sri Lanka.<sup>77</sup>

Burgoyne's Desk head, Gartshore, provided the first briefing on the threats the Desk would be monitoring. At the time, level 2 coverage was in place for the Khalistan Liberation Movement. Talwinder Singh Parmar was a key player in that movement and was already one of the key targets, even though he had been incarcerated in West Germany since 1983.<sup>78</sup>

Burgoyne began to educate himself on Sikh issues. He studied the subject in his spare time and relied on the Liaison Officer (LO) in New Delhi for daily or weekly updates on events in India which could have a bearing on Sikh activities in Canada. Approximately six months after he began working on Sikh extremism, Burgoyne was described as the "Sikh expert". He told the Commission that he put in a lot of extra time to learn the area, but was not at all comfortable with such a description, even though when it came to expertise on Sikh issues at HQ he "...was pretty well it."<sup>79</sup>

---

<sup>74</sup> Exhibit P-101 CAF0072b.

<sup>75</sup> Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3518-3519. According to Bob Burgoyne, level 1 permitted investigation of open sources and bio-data, level 2 permitted physical surveillance and redirection of an existing human source, level 3 permitted development of human sources and level 4 permitted full-scale interception of private communications (with a warrant) and mail opening: Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3410.

<sup>76</sup> Exhibit P-101 CAF0118.

<sup>77</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3396-3397.

<sup>78</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3396.

<sup>79</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3403-3404.

Throughout the period leading up to the bombing, Burgoyne continued to be portrayed as the Sikh expert, despite the fact that he was a junior officer who had only been on the desk a relatively short time. At one point he was asked to brief an official from the Department of External Affairs who was about to be transferred to India. The official reacted with surprise when he learned that Burgoyne did not speak Punjabi. Burgoyne told the Commission that, though he had a “pretty good handle” on activities in Canada, he would have been “absolutely” more knowledgeable had he been able to speak the language.<sup>80</sup>

### ***Sikh Extremism File Created***

On April 17, 1984, a “Sikh Extremism” file was created,<sup>81</sup> in response to violence in India coupled with intelligence that Sikh terrorists might become active internationally.<sup>82</sup> Burgoyne wrote: “We remain extremely concerned over the possibility of Sikh terrorists travelling to Canada and/or possible eruptions of Sikh community violence in Canada, brought about by related developments in India.”<sup>83</sup> Indeed, intelligence received in late April suggested that a group of 36 Sikhs was being sent to North America to kill moderate Sikh leaders, prominent Hindu leaders, and carry out attacks on Indian government diplomatic personnel.<sup>84</sup>

Two events in the next few months would raise the profile of Sikh extremism in Canada. On June 6, 1984, Indian government troops stormed the Golden Temple in Amritsar, the holiest Sikh temple. A few weeks later, in early July, Parmar was released from a German jail and promptly returned to Canada.

### ***Operation Bluestar and the Assault on the Golden Temple***

Sant Jarnail Singh Bhindranwale was widely considered to enjoy the tacit support of the ruling Indian government as a counterweight to the Akali Dal, a widely popular Sikh nationalist movement. Bhindranwale rapidly transformed himself into the leader of the Khalistan movement. Months before the raid on the Golden Temple, he and his followers moved into the complex. Amid rumours that the Indian government was planning to invade, he began to amass arms and fortify the Temple. On June 2, 1984, Indian PM Indira Gandhi authorized “Operation Bluestar.” All transportation in and out of the Punjab was halted. The border with Pakistan was closed; telephone lines and other means of communication were cut. On June 5<sup>th</sup>, tanks moved into the complex and opened fire. On June 6<sup>th</sup>, the attack was over and the Government was in control of the Golden Temple. The Government reported that nearly 500 Sikhs had been killed, however nearly 2000 remained unaccounted for. Sant Bhindranwale was

---

<sup>80</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3405-3406.

<sup>81</sup> Exhibit P-101 CAB0054, p. 1.

<sup>82</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3412-3413.

<sup>83</sup> Exhibit P-101 CAB0054, p. 1.

<sup>84</sup> Exhibit P-101 CAF0102, p. 3.



among those who were killed.<sup>85</sup> Sikhs around the world reacted in horror to the storming of the Golden Temple. Sant Bhindranwale and those who died in the action became martyrs in the eyes of Khalistan idealists.<sup>86</sup>

#### ***Level 4 Authorization for Sikh Extremism***

In response to the storming of the Golden Temple and the violent and escalating tensions worldwide, the RCMP SS Operational Priorities Review Committee (OPRC) granted the authority for a full level 4 investigation into Sikh extremism on June 27, 1984.<sup>87</sup> This was the highest level of investigative authority. It allowed the most intrusive techniques such as physical surveillance and the ability to obtain a warrant for interception of private communications. At the same time, the name of the file was changed from “Sikh Extremism”, which was felt to be too general a term, to “Alleged Sikh Terrorist Groups in Canada.”<sup>88</sup>

The RCMP SS was concerned for the safety of Indian diplomats and their missions in Canada. Indeed, a foreign source provided the RCMP SS with its assessment that, following the attack on the Golden Temple, there was a significant threat in the coming weeks of an attempt to either kidnap or murder Indian official personnel, Air India employees or the staff at Indian tourist offices in Canada.<sup>89</sup>

Also of great concern were unconfirmed reports that Canadian Sikhs were providing weapons and funds to Sikh extremists in the Punjab. As well, mass demonstrations were being staged in Canada, mostly in Vancouver and Toronto. Intelligence indicated that clandestine meetings of Sikhs had been held in Toronto to plan protests and attract attention to the Sikh cause. Sikhs in Toronto “...publicly announced the formation of a Canadian arm of [a] Sikh government-in-exile, and disclosed their intention to directly support terrorist action targeted against the Government of India.” Intelligence also suggested that there were Canadian-made plans to send assassination squads to attack PM Indira Gandhi and the High Commissioners to Canada, the US, and the UK.<sup>90</sup>

#### ***Initial Knowledge of the Babbar Khalsa***

On June 6, 1984, RCMP P Directorate, VIP Division, reported that a threatening phone call had been received by the Indian High Commission in London, UK, stating that the Indian Consul General in Vancouver and/or his family would be kidnapped or killed by the “Barbara Khalsa” group. As this report demonstrates, at the time, even knowledge of the group’s proper name was lacking.<sup>91</sup>

---

<sup>85</sup> Exhibit P-101 CAA1087, p. 11.

<sup>86</sup> Exhibit P-101 CAA1046, p. 4.

<sup>87</sup> Exhibit P-101 CAF0102, p. 1; Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3520-3521.

<sup>88</sup> Exhibit P-101 CAF0102, p. 1.

<sup>89</sup> Exhibit P-101 CAB0061, pp. 2-3.

<sup>90</sup> Exhibit P-101 CAF0102, p. 3.

<sup>91</sup> Exhibit P-101 CAB0068, p. 1.



A few days later, Burgoyne wrote a memo to Gartshore regarding the Security Service's knowledge of the, now correctly named, Babbar Khalsa (BK) in Canada. The Security Service had previously received reports from Indian authorities about a BK presence in Vancouver. However, the RCMP SS was unable to confirm the existence of the BK in Vancouver or anywhere else in Canada.<sup>92</sup> At the time, that was the extent of the Security Service's knowledge of the BK.<sup>93</sup>

### ***Parmar's Return to Canada and the Creation of CSIS***

Talwinder Singh Parmar was imprisoned in West Germany as of June 29, 1983, pending extradition to India pursuant to a warrant for his alleged involvement in the murder of two police officers.<sup>94</sup> On July 6, 1984, however, he was released from jail.<sup>95</sup> Two reasons for this release were in circulation. One reason was that insufficient evidence had been provided by the Indian government to support his extradition from Germany.<sup>96</sup> The other was that, due to the recent tension and violence in India, West German officials felt that Parmar would not receive a fair trial in India.<sup>97</sup> Whatever the actual cause for his release, the result was that Parmar, who had long been considered a key Khalistan leader, was set free and returned to Vancouver.

Upon his release, Parmar was immediately characterized by the GOI as "... the most dangerous Sikh terrorist presently at large." The GOI communicated its concern to Canadian officials that Parmar posed a threat to the security of Indian VIPs in Canada.<sup>98</sup>

The RCMP SS, and in particular Burgoyne, registered concern about what effect Parmar would have on the Sikh community in Canada. Since Parmar was covered by a level 4 investigative authority, Burgoyne tasked the BC Region to attempt an interview with him<sup>99</sup> to cover points such as the formation of Babbar Khalsa in Vancouver, the Khalistan "government-in-exile" and to clarify what he meant by publicly warning the Indian Government that they would pay a price for what they did in Amritsar. At the very least, it was thought that having the interview might neutralize his activities in the Vancouver area.<sup>100</sup>

It was at this point in July 1984 that the RCMP SS was replaced by CSIS.

As soon as Parmar arrived back in Canada, he launched a nationwide campaign in an attempt to establish himself as the Sikh leader in Canada.<sup>101</sup> His actions were an immediate cause for concern and were documented in a memo written by Burgoyne:

---

<sup>92</sup> Exhibit P-101 CAB0061, pp. 1-2.

<sup>93</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, pp. 3454-3455.

<sup>94</sup> Exhibit P-101 CAB0114, p. 1.

<sup>95</sup> Exhibit P-101 CAF0100, p. 1.

<sup>96</sup> Exhibit P-101 CAA1087, pp. 15-16.

<sup>97</sup> Exhibit P-101 CAB0114, p. 1.

<sup>98</sup> Exhibit P-101 CAF0100, p. 1.

<sup>99</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3414-3415.

<sup>100</sup> Exhibit P-101 CAF0100, p. 2.

<sup>101</sup> Exhibit P-101 CAB0114, p. 1.

Parmar wants to be acclaimed the “Holy Man” in North America, thereby gaining control and/or direction of the various organizations and Sikhs in general. While in Calgary, Parmar strongly suggested that local Sikhs unite, fight and kill, in order to revenge the attack on the Golden Temple in Punjab.... Parmar appears willing to support or assist terrorist acts in the name of the Khalistan state.<sup>102</sup>

Burgoyne wrote the memo to highlight his concerns to Mel Deschenes, the DG CT of the newly-constituted CSIS, and so that the information would be circulated to other government departments.<sup>103</sup> However, it is unknown whether the DG CT shared Burgoyne’s concerns and what, if any, external government departments were informed about Parmar and his activities.

### ***Tasking Role of the HQ Desk***

The Western Europe & Pacific Rim Desk (which later became known as the Sikh Desk) was responsible for tasking the regional offices of CSIS.<sup>104</sup> This was not done without supervision, as most directions required that management sign off first. This sign-off was usually provided by Upton, the head of the Europe and Pacific Rim Section, which housed the Western Europe & Pacific Rim Desk.

Burgoyne testified that, from the fall of 1984 until the spring of 1985, the Sikh extremism investigation occupied most of his time, as the area of investigation was new and there was a need to gather as much information as possible. His role at HQ, and indeed the role of the Desk, was that of the gatekeeper of information as well as the decision-maker about which target approvals would be sought. In cases where an application to the Target Approval Review Committee (TARC) was deemed necessary, the Desk would write the submission. TARC was formerly known as the Operational Priorities Review Committee (OPRC) in the RCMP SS.<sup>105</sup>

Another aspect of the Desk’s role was in connection with RCMP requests for threat assessments. In order to respond to these requests, and to produce informed threat assessments, the Desk needed information from the field and directed the regions accordingly.<sup>106</sup> For example, on July 10, 1984, the Desk asked the regions to determine whether or not the BK was an “...identifiable organizational entity in Canada, and the extent to which they individually, or collectively, pose a threat to Indian diplomatic personnel and property”.<sup>107</sup> The intelligence officers in the various regions were to investigate the existence of the BK in their area and report back to the Desk in a timely manner.

<sup>102</sup> Exhibit P-101 CAB0114, p. 1-2.

<sup>103</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3416.

<sup>104</sup> Tasking was the process by which CSIS HQ would direct investigations by asking for more information to complete holes in the overall investigation. This direction was not specific to allow for regional autonomy.

<sup>105</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3400, 3408-3409.

<sup>106</sup> Testimony of Glen Gartshore, vol. 31, May 22, 2007, p. 3527.

<sup>107</sup> Exhibit P-101 CAF0099, p. 1.

The Desk also needed information from abroad and therefore would also task SLOs (security liaison officers, previously known as liaison officers (LOs) in the RCMP SS).<sup>108</sup> Through SLOs, they would request general information from allied intelligence services and would also share CSIS information. After the storming of the Golden Temple, Burgoyne began making greater demands for information about events transpiring in the Punjab, especially in relation to information needed for threat assessments. The SLO in New Delhi would send information on a regular basis.<sup>109</sup>

Tasking documents show that the range of concerns held by HQ was broader than just Parmar or the BK.<sup>110</sup> There were numerous names of organizations, often first identified by the Government of India, and the Desk would have to determine whether they existed in Canada and, if so, whether they posed a threat.<sup>111</sup>

### ***Renaming of the Desk to Focus on Sikh Extremism***

During the fall of 1984, due to the heightened threat of Sikh extremism, the Western Europe & Pacific Rim Desk was renamed the Sikh Desk. This occurred at the same time as the approval of the level 4 authorization on Parmar and at a time when Sikh extremism issues had begun to dominate Burgoyne's responsibilities. On the creation of the Sikh Desk, Burgoyne's other duties were passed to other CSIS employees, allowing him to concentrate almost entirely on the Sikh issue.<sup>112</sup>

### ***Subject Evaluation Report on Parmar***

While the Sikh extremism investigation had received a level 2 approval in April 1984 and a level 4 approval just after the raid on the Golden Temple, an individual level 4 approval was preferred for individual targets once they had been identified. To that end, on September 17, 1984, the DG CT submitted a Subject Evaluation Report on Parmar to the TARC to obtain a level 4 authorization on him, a step that was required in order to proceed with a warrant application. The application was recommended by Deschenes, but it was written by Burgoyne with input from the regions, particularly BC Region. The document indicates that the threat to Indian missions in Canada at the time was now considered high, and that Parmar was identified early on as a key individual among those fomenting Sikh unrest in Canada, particularly in British Columbia.<sup>113</sup>

After the level 4 approval on Parmar, the Sikh Desk supported BC Region's urgent application for a warrant to intercept the communications of Parmar. The application was submitted in October 1984, but its approval was unfortunately delayed for five months.<sup>114</sup>

---

<sup>108</sup> Liaison officers in the RCMP SS were known as Los; in CSIS they were renamed security liaison officers or SLOs.

<sup>109</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3408-3409.

<sup>110</sup> See, for example, Exhibit P-101 CAF0103 and CAF0120.

<sup>111</sup> Testimony of Glen Gartshore, vol. 31, May 22, 2007, p. 3531.

<sup>112</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3399.

<sup>113</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3400-3401, 3417-3418.

<sup>114</sup> See Section 1.3 (Pre-bombing), Parmar Warrant.

### ***Profiles Developed on Key Sikh Extremists***

In early October 1984, David Ayre, a CSIS BC Region intelligence officer, produced profiles of Surjan Singh Gill and Ajaib Singh Bagri in response to a request for further information from HQ.<sup>115</sup> The description of Gill is startling:

Gill is purportedly the brains behind the Babbar Khalsa Group ... and its titular leader, Talvinder Singh Parmar ... Gill orchestrates all of Parmar's activities and seems to go with him whenever he departs from Vancouver... Gill is a highly emotional individual who has been noted acting in a frenetic manner. He was observed by myself hacking away with a ceremonial sword at an effigy of Indira Gandhi outside the Indian Consular offices, just before the invasion of the Golden Temple. Gill's eyes were glazed, he had a look of hate on his face, and he was yelling incoherently whilst he was flailing away.<sup>116</sup>

Perhaps most disturbing is Ayre's analysis of Gill's potential as a terrorist:

Given the proper set of circumstances and stimuli, I feel that Gill can be considered a dangerous threat to Canadian security.<sup>117</sup>

A similar description of Bagri was also provided, though Ayre qualified the description by revealing that CSIS had so far been unable to obtain much local information on him:

Bagri is a close consort of Parmar and Gill and seems to be heavily involved in the Babbar Khalsa Group. As a terrorist threat, I feel he rates quite highly, especially when you look at the statements he made in New York during the World Sikh Organization meeting.... I feel that he has a propensity to commit a terrorist act given the right set of circumstances.<sup>118</sup>

The profiles were a result of Upton's direct intervention and his expression of dissatisfaction with the BC Region's original bare-bones assessment of the targets.<sup>119</sup> Upton noted that the more robust profiles produced were exactly what was needed by the Desk for accurate assessments of the situation.<sup>120</sup>

---

115 See Exhibit P-101 CAF0104.

116 Exhibit P-101 CAF0104, pp. 1- 2.

117 Exhibit P-101 CAF0104, p. 2.

118 Exhibit P-101 CAF0104, p. 3.

119 See Exhibit P-101 CAB0138 and Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3578-3581.

120 See Exhibit P-101 CAF0106 and Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3583-3584.

### ***Trying to Find Parmar and Bagri***

On October 15, 1984, CSIS received information about a potential hijacking involving Canadian and UK Sikhs. Ajaib Singh Bagri was listed as one of the members of the hijacking “committee”. At the time it was known that Bagri was a member of the BK, close to Parmar, and had been assessed by BC Region as a person who was capable of terrorist acts.<sup>121</sup>

Of particular concern was the fact that neither Parmar nor Bagri had been seen in BC Region for quite some time, and that CSIS had no idea where they were. The Desk tasked both BC and Toronto regions to “...exhaust all possible avenues in a final attempt to locate the present whereabouts of Talwinder Singh Parmar ... and Ajaib Singh Bagri ....”<sup>122</sup>

So alarming was the information concerning the hijacking plot that, although BC and Toronto were given the specific tasking, all the other regions were copied as well. It was considered policy to advise all the regions when such information was received, the reasoning being that it increased the possibility that spinoff information from other regions might be brought to the attention of HQ.<sup>123</sup> In contrast to this treatment of “alarming” information, seemingly innocuous information would not be copied to other regions, thereby eliminating the potential for spinoff material. Though the material may have been available through a search of NSR, relevant but not “alarming” material could easily be missed because attention was not drawn to it through copies to the regions. This is one example of HQ playing a gatekeeper role in determining which information was deemed important enough to be brought to the attention of other regions. This subjective procedure, by which material was shared or not shared, created a potential for the loss of valuable information from other regions that might have been able to provide additional context or intelligence.

### ***Parmar Implicated in Indira Gandhi Assassination***

On October 31, 1984, Indian PM Indira Gandhi was assassinated in India by two of her Sikh bodyguards. Immediately, there began to be speculation in the Indian press that the assassination was orchestrated from abroad and that Parmar was involved.<sup>124</sup> Upton wrote a memo to Gartshore reflecting on this turn of events and its impact on the importance of the warrant that had just been applied for to intercept Parmar’s communications:

Subject: Talwinder Singh Parmar et al. Glen, attached is a copy of External’s message from Delhi dated 84/11/13. Once again Parmar’s name comes up. You can bet your bottom dollar that eventually a Canadian connection will be made here. This lends to the need for our warrant on Parmar ....<sup>125</sup>

<sup>121</sup> Exhibit P-101 CAF0127, pp. 1, 3.

<sup>122</sup> Exhibit P-101 CAF0127, p. 3.

<sup>123</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3589.

<sup>124</sup> Exhibit P-101 CAB0168.

<sup>125</sup> Exhibit P-101 CAB0167.

The Desk and Upton became very anxious for more information, particularly for source information on Parmar, which would not be forthcoming for a number of months.<sup>126</sup>

### ***Sikh Extremism File Compartmentalized***

Also in October 1984, the Desk became concerned that the authority to investigate Sikh extremism was becoming tenuous. The original coverage granted was for one year, with the expectation that as more information was gathered, files would be opened on specific targets, either groups (such as the BK) or individuals. In early 1985, the Sikh extremism file was shut down and replaced by specific files reflecting the move towards more focused investigations.<sup>127</sup>

By January 1985, the Sikh Desk was putting increasing pressure on the regions to identify separate Sikh extremist organizations of interest to CSIS. Specifically singled out were the BK, the Sikh Student Federation (later known as the International Sikh Youth Federation (ISYF)), the Khalistan Liberation Movement, the World Sikh Organization, the Akhand Kirtani Jatha and the North American Sikh Youth Organization International.<sup>128</sup> The tasking was meant to allow for an assessment of resources needed and an evaluation of the appropriate focus to be applied to the investigations.<sup>129</sup> In the case of the BK, however, an application was already before the TARC for a level 4 approval and the submission dealing with the Sikh Student Federation was in progress.

One potential problem with the greater specialization of the file was that it increased compartmentalization. While, previously, all information would come under "Sikh Extremism", information was now to be filed based on a narrow focus, such as BK or ISYF. This compartmentalization meant that linkages between groups or persons could be missed, especially if the "need-to-know" principle excluded an analyst working on one organization from access to another organization's file, despite the possibility of important interconnections. With Burgoyne as the only analyst on the Sikh Desk, it is highly unlikely that this possibility existed in late 1984 and early 1985. However, once more analysts were added to the Desk, just prior to the bombing and in the post-bombing stage, this possibility existed not only at HQ but in the regions as well. Though the Commission does not have evidence to show that particular information was missed due to this organization of files and the use of the "need-to-know" principle, it is known that connections that could have been made were not. For example, the Sikh Desk did not recognize that code words used in the Windsor area (Bob Burgoyne's file) were the same as those used in the days before the bombing by Parmar in BC (Bill Dexter's file). The connection was not made until

---

<sup>126</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3598. See also Section 1.3 (Pre-bombing), Parmar Warrant.

<sup>127</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3420-3421.

<sup>128</sup> Exhibit P-101 CAF0107, pp. 1-2.

<sup>129</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3422; Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3525-3526.

an analyst who had been working on the Windsor file was transferred to the Sikh Desk at HQ months after the bombing and went back over the Parmar transcripts.<sup>130</sup>

#### **Level 4 on the Babbar Khalsa and its Leaders**

On January 30, 1985, the Sikh Desk submitted a subject evaluation report on the BK for the purpose of obtaining a separate level 4 authority on the organization.<sup>131</sup> The document set out CSIS's knowledge of the BK and its leaders at the time:

The Babbar Khalsa in Canada is believed to consist of approximately 20 members, all radical and potentially dangerous Sikhs. The organization is led by three individuals from British Columbia namely Surjan Singh Gill, Talwinder Singh Parmar, and Ajaib Singh Bagri.<sup>132</sup>

On the same day, Ted Finn, the Director of CSIS, authorized level 4 coverage of the BK and its leaders, Gill, Parmar and Bagri, as well as level 3 coverage of the rest of the membership.<sup>133</sup> A corrected copy of the subject evaluation report was circulated to all regions in late February. A description of the three leaders is given, and their profiles, particularly those of Gill and Bagri, are largely unchanged from the description given by Ayre four months before:

- i) Gill is reportedly the brains behind Babbar Khalsa. In 1981 [November] Gill reportedly organized a meeting to examine ways of extending assistance to the hijackers of the IAC aircraft and their families.
- ii) Parmar is the subject of an international warrant issued by the Indian government for murder and is considered to possess the greatest threat in Canada to Indian diplomatic missions and personnel. Parmar has freely admitted that while in India in 1981, he founded the Babbar Khalsa in that country.
- iii) Bagri is a close consort of Parmar and believe[s] he can be easily manipulated into committing a terrorist act. Bagri has made several heated verbal attacks on the Hindu religion, including remarks made at a Sikh convention in New York that 50,000 Hindus be killed to avenge the deaths of Sikhs killed by Indian troops in the attack on the Golden Temple in Amritsar  
....<sup>134</sup>

This absence of change in the profile emphasizes the lack of new information gathered by CSIS in the interim. As of February 21, 1985, it would appear that CSIS had gathered no new information on the BK or its members since September 1984.<sup>135</sup>

<sup>130</sup> Exhibit P-101 CAA0308, CAA0309(i).

<sup>131</sup> See Exhibit P-101 CAB0187 and Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3422-3423.

<sup>132</sup> Exhibit P-101 CAB0187, p. 2.

<sup>133</sup> Exhibit P-101 CAF0111, p. 1.

<sup>134</sup> Exhibit P-101 CAF0111, pp. 2-3.

<sup>135</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3591-3592.



### ***Lack of Parmar Photograph and Other Information***

Not only was there no new CSIS information about Parmar or his associates as of late February, 1985, CSIS memoranda also complained of the lack of a suitable photograph and a good physical description of Parmar.<sup>136</sup> This was creating difficulties for CSIS, as Parmar travelled frequently in Canada and the surveillance units were not able to easily identify him. CSIS memoranda also complained about a lack of fingerprints for the target. However, it is difficult to understand the need for fingerprints and their possible use, considering that CSIS was now a civilian organization.<sup>137</sup>

Upton testified that the difficulty in obtaining biographical data on Parmar was due to a lack of source coverage on Parmar, either directly or indirectly through persons close to him. He also confirmed that a warrant and its resulting intercept product would have helped to obtain the information needed on Parmar.<sup>138</sup>

### ***Attack on Ujjal Dosanjh***

In February, 1985, the outspoken moderate lawyer, Ujjal Dosanjh, was beaten with a pipe and nearly killed.<sup>139</sup> No one was ever convicted of the crime. CSIS was aware of the incident, but treated it as a matter for the police to investigate. At the very least, this violent incident should have served notice to both CSIS and the RCMP that Sikh extremism had become a significant threat to the safety of Canadians.

### ***April 13<sup>th</sup> Hijacking Alert***

As the celebration of the Sikh festival of Baisakhi on April 13<sup>th</sup> was fast approaching, the Government of India communicated information regarding potential upcoming threats to the Department of External Affairs. This information was in turn shared with CSIS.<sup>140</sup> Included in the threat information received was the following:

Unconfirmed reports of plans to hijack an Air India flight around the time of Baisakhi, with particular threat to AI-181 reaching Toronto on Saturday, April 13, 1985.<sup>141</sup>

This information was shared with the RCMP, and the Airport Security division was advised. At the same time, CSIS also produced a threat assessment for the RCMP in response to a verbal request. In this TA, CSIS stated that it believed the bomb threats were made in order to keep "...Khalistan alive in the minds of all Sikhs."<sup>142</sup> CSIS also stated that it had no information that there actually would be a hijacking. In fact, no hijacking took place.

<sup>136</sup> Exhibit P-101 CAF0123, p. 1.

<sup>137</sup> Exhibit P-101 CAF0123, p. 1; Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3594-3595.

<sup>138</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3596.

<sup>139</sup> Exhibit P-101 CAA1099, p. 1; Testimony of Ujjal Dosanjh, vol. 80, November 21, 2007, p. 10173.

<sup>140</sup> Exhibit P-101 CAB0216.

<sup>141</sup> Exhibit P-101 CAB0215(i), p. 2.

<sup>142</sup> Exhibit P-101 CAA0147, p. 1.



### ***Heightened Alert Due to Impending Golden Temple Anniversary and Gandhi Visit***

In May 1985, CSIS went on a heightened alert status. Two important events were fast approaching: the first anniversary of the storming of the Golden Temple and a visit by Prime Minister Rajiv Gandhi to the United States.<sup>143</sup> Upton testified that he was "...in and out of my DG's office frequently impressing upon him the urgency of the Sikh problem."<sup>144</sup> The Sikh Desk itself was very busy trying to gather what intelligence it could.

Due to the heightened alert, Upton requested that the Sikh Desk update its profile of Parmar with new information, since the existing profile only described activities up to August 1984.<sup>145</sup> The stated purpose for updating the profile was so that it could be circulated to government departments for operational development purposes.<sup>146</sup> It is unclear whether the profile was in fact updated or whether an updated profile was circulated within government.

### ***Level 4 on International Sikh Youth Federation and its Leaders***

Also in early May, and in response to the heightened threat and need for more and better coverage of Sikh extremism, the Sikh Desk did obtain level 4 coverage of the ISYF and its leaders, and a level 3 coverage of the membership. The ISYF had been previously known as the Sikh Student Federation.<sup>147</sup>

### ***Threat Assessment for Gandhi's Visit***

The first threat assessment in relation to the upcoming Gandhi visit was produced by CSIS on May 24, 1985.<sup>148</sup> The TA, written by members of the Sikh Desk, was sent to various agencies outside of CSIS. The TA informed recipients of CSIS's view at that point concerning Sikh extremists and the threat they posed.

One of the pieces of information that was shared dealt with a statement made by Gurmej Singh Gill, a BK member from the UK with very close ties to Canadian BK leaders. He visited Canada in January 1985, and in May 1984 he was reported to have said that, "...the names of Sikhs who refused to boycott Air India flights would be put on a 'hit list' which would be passed on to the BK in India for action." This statement, demonstrating that Sikh extremists considered Air India an alter ego for the Government of India and a legitimate target at least for economic action, was passed to the RCMP and Transport Canada, two other agencies with a role in aviation security.<sup>149</sup>

---

<sup>143</sup> Exhibit P-101 CAB0225.

<sup>144</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3599-3600.

<sup>145</sup> Exhibit P-101 CAB0212, p. 2; Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3585-3586.

<sup>146</sup> Exhibit P-101 CAB0212, p. 2.

<sup>147</sup> Exhibit P-101 CAF0117, p. 2; Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3428.

<sup>148</sup> Exhibit P-101 CAB0236(i); Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3429-3430.

<sup>149</sup> Exhibit P-101 CAB0236(i).

**May 28<sup>th</sup> Deschenes Telex**

As the dates of the anniversary of the storming of the Golden Temple and Gandhi's visit to the US drew closer, Sikh extremism was reclassified as the number one threat within CSIS.<sup>150</sup> An important telex was sent to all regions and to the Windsor district on May 28, 1985 by Mel Deschenes, the DG CT, requesting priority attention regarding Sikh extremists:

CSIS Headquarters recognizes the terrorist potential here, and is obligated to provide the government with timely and accurate intelligence and assessment of the situation as it develops. Top priority attention is now being afforded this area until at least mid 1985 06. We would therefore request that all districts and regions afford this area equal priority attention during the period in question.<sup>151</sup>

The Deschenes telex also requested a change in reporting procedure with regard to intercepts on Sikh extremists:

[W]e would ask for priority debriefing of all available sources in this area, particularly those special sources covering hard target areas. In order to advance threat assessments for the 1985 06 06 affair, and Gandhi's visit, we would ask that any, and all, special meetings of target ... groups be afforded coverage, if and when possible, and priority reporting.<sup>152</sup>

"Debriefing" and "special sources covering hard targets" were code for analyzing technical sources (i.e. wiretaps).<sup>153</sup> Instead of waiting until enough information was gathered for a robust intelligence report, intelligence reports based on intercept product were to be written daily, even if the information was minimal, and entered into the Narrative Storage and Retrieval (NSR) system so that HQ was updated along with the regional investigators.<sup>154</sup>

Impressive as this emphasis on daily reporting may seem, in practice, it was unrealistic when applied to the Parmar intercept. HQ may have attached high importance to receiving daily updates, but the cold hard fact – not addressed in Deschenes's memo – was that there were not enough translators in place to allow for daily translation of the intercept material and, in fact, BC Region completely lacked a translator. While the English language portion of the intercept could be reported on, since almost all of the significant conversations in the Parmar intercept were in Punjabi, the instruction to provide daily updates

---

<sup>150</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3789-3792.

<sup>151</sup> Exhibit P-101 CAF0124(i), p. 1.

<sup>152</sup> Exhibit P-101 CAF0124(i), p. 2.

<sup>153</sup> Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3541-3543.

<sup>154</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3791.

on the intercepted communications of the principal Sikh extremist target was meaningless. Predictably, instead of daily translation, a backlog of untranslated tapes continued to grow. This crucial intelligence failure was to be repeated on June 23<sup>rd</sup> after the bombing, when regions were once again instructed immediately to "...debrief their special sources", but BC Region still lacked the ability and resources to comply.<sup>155</sup>

### **June 1985 Events**

On June 4, 1985, CSIS surveillants observed the Duncan Blast.<sup>156</sup> Though CSIS HQ was informed, as were the RCMP and the Vancouver Police Department (VPD), there is no documentation showing that HQ requested BC Region to complete any follow-up on the event observed.<sup>157</sup>

On June 5, 1985, Upton sent out an update to all regions and Windsor district regarding the requirement of daily updates on Sikh extremism.<sup>158</sup> In the note he stated:

In conjunction with the current threat received from Sikh extremists and further to message ... of 1985 05 28, the Director General – Counter Terrorism now has a requirement to provide daily briefing to the Deputy Director National Requirements and, ultimately the Director. It is necessary to complete daily situation reports for the DG-CT. In this regard, BC, Alta, Man, Toronto, Ottawa and Quebec regions as well as Windsor district are requested to provide this Headquarters with daily reports detailing and assessing events or developments in their respective areas. These reports must reach this HQ by 1400 hours each working day until further notice. Negative reports are required.<sup>159</sup>

According to Burgoyne's testimony, the directive for daily reports and the briefings for the Deputy Director of National Requirements and the Director were in anticipation that June would be a "...very volatile month" and that "... things were going to become quite active within the community."<sup>160</sup>

Upton testified that HQ got a very favourable response from the regions in response to the request for daily reports, particularly from BC and Toronto, which included the Southwestern Ontario region including Windsor.<sup>161</sup>

June also saw a coordinated disruptive interview program of Canadian Sikhs, organized by CSIS, RCMP, municipal police forces and American authorities.<sup>162</sup>

---

<sup>155</sup> Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3542-3543.

<sup>156</sup> Details can be found in Section 1.4 (Pre-bombing), Duncan Blast.

<sup>157</sup> Details can be found in Section 1.4 (Pre-bombing), Duncan Blast.

<sup>158</sup> Exhibit P-101 CAB0256.

<sup>159</sup> Exhibit P-101 CAB0256.

<sup>160</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3432.

<sup>161</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3601.

<sup>162</sup> Exhibit P-101 CAA1099, p. 2.

CSIS was not directly involved in the interviews, but aided by suggesting interview subjects. In Vancouver, this resulted in a joint RCMP and US Secret Service (USSS) interview of both Parmar and Gill.<sup>163</sup>

Despite the understanding that the month of June would be a volatile one, on June 14, 1985, the RCMP requested yet another updated TA, with the expectation that the threat would be lowered "...now that 'Genocide Week' and Prime Minister Rajiv Gandhi's visit to the USA is terminating."<sup>164</sup> Upton circulated the request for updated information to all the regions and Windsor district. He also stated in his memo that "...[a] great deal of intelligence has been received from various sources which has, as yet, to be completely sorted out and fully analysed."<sup>165</sup> The TA was required for June 17<sup>th</sup>, two days after Gandhi was due to leave the US.<sup>166</sup>

Though the tension was easing, Burgoyne testified that the attitude at CSIS HQ was that the threat of Sikh extremism remained high and that the threat assessment should be maintained at that level for the near future.<sup>167</sup>

On June 18, 1985, CSIS released its final TA prior to the bombing. The TA, signed by Deschenes but actually written by Dexter, was distributed to numerous government agencies including the RCMP, External Affairs, and Transport Canada.<sup>168</sup> This TA documented the events that occurred in the previous three weeks, including investigations, demonstrations and incoming intelligence. Included in this information was reference to a plot to assassinate Prime Minister Rajiv Gandhi discovered during the arrests in New Orleans,<sup>169</sup> and to the potential for Canadian connections. As well, a concern was raised about Canadian Sikhs arming themselves, with CSIS offering the example that two Sikhs from the Windsor area were known to have purchased an Uzi machine gun in Detroit which they were likely to have brought back to Canada.<sup>170</sup>

Notably absent from this memo, particularly in light of the concern over guns, was any mention of the Duncan Blast narrative. Accordingly, the Duncan Blast events were not shared with the relevant government departments and agencies except with the RCMP at the local level. Though CSIS misinterpreted the events, it is possible that, had they shared their knowledge of the event, another agency might have seen things differently or, at least, might have asked for further information that would have led to CSIS revisiting its assessment of the significance of this crucial event.

HQ did maintain that the threat level should be continued as "high":

---

<sup>163</sup> Exhibit P-101 CAB0290.

<sup>164</sup> Exhibit P-101 CAA0215, p. 1.

<sup>165</sup> Exhibit P-101 CAA0215, p. 2.

<sup>166</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3434-3435.

<sup>167</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3434.

<sup>168</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3435. Deschenes was in Los Angeles at the time this TA was written.

<sup>169</sup> This is discussed in Section 1.12 (Pre-bombing), A "Crescendo" of Threats.

<sup>170</sup> Exhibit P-101 CAB0321, p. 3.

While the Gandhi visit and the Anniversary of the Golden Temple invasion certainly afforded ample opportunity for strike potential we must recognize that the most dangerous element of the Sikh populace were well aware that security would be optimum and the potential for a serious attack succeeding would be greatly diminished. These same extremists/terrorists are no less determined to realize their ambitions and to think that they have abandoned their cause would be somewhat naïve on our part.... For these reasons we assess the threat as being only slightly less serious than it was at the time of our last assessment.<sup>171</sup>

Nevertheless, on June 19, 1985, and despite the analysis that the most radical Sikhs might be biding their time, the requirement for daily updates from all regions was discontinued.<sup>172</sup> It seems as though CSIS and the Government of Canada were breathing a collective sigh of relief, prematurely, as it turned out.

Having looked at the investigation of Sikh extremism at the HQ level, it is instructive to examine more closely what was taking place in the field, especially in the BC Region and Windsor District.

### **BC Regional Investigation**

Although policy and analysis are housed within CSIS HQ, regional employees, primarily intelligence officers, conduct investigations including source development (technical and human), community interviews, surveillance, and related activities.

In the BC Region, Ray Kobzey and David Ayre were the two main intelligence officers dealing with the Sikh extremism investigation, working under unit head Jim Francis. Kobzey and Ayre also liaised directly with the analysts at HQ and often received direction from them.

Through Kobzey's testimony, and using additional documents, we are able to examine the CSIS BC pre-bombing investigation.<sup>173</sup>

### ***Escalating Sikh Extremism***

The issue of Sikh extremism first came to the attention of Kobzey in 1981. At the time, he was a member of the RCMP Security Service based in Vancouver and working primarily on the Latin American Desk with part-time coverage of other issues. In November 1981, local newspapers published articles about the creation of a Khalistan Consulate in Vancouver headed by Surjan Singh Gill. Kobzey stated at the Inquiry:

<sup>171</sup> Exhibit P-101 CAB0321, p. 4.

<sup>172</sup> Exhibit P-101 CAB0323.

<sup>173</sup> Raymond Kobzey appeared before the Commission on May 23, 2007 (vol. 32, pp. 3715-3777) and on May 24, 2007 (vol. 33, pp. 3779-3864).

As a consequence of that, I became interested in the issues of Sikh activism, with respect to the establishment of a homeland in Punjab to be called Khalistan by the people who were interested in creating that unique country.<sup>174</sup>

The Khalistan issue did not gain much prominence at the RCMP Security Service. However, Kobzey maintained an interest in what was happening and "...sought to pay more attention to the issues that were surfacing in the newspaper, open sources, et cetera."<sup>175</sup>

In addition to the press attention the Khalistan Consulate had created, another story surfaced in an interview in the local press. A woman expressed concern over the apparent disappearance of her husband, who had returned to India in 1980.<sup>176</sup> His name was Talwinder Singh Parmar. Kobzey kept tabs on all these events, and even interviewed Surjan Singh Gill. Subsequent to that interview, newspaper articles were written about Talwinder Singh Parmar's absence from Vancouver and his wife's concerns about his health and whereabouts.

In late 1981, Parmar was smuggled out of India and returned to Vancouver, but not without controversy. India had implicated him in the murder of two policemen and had a warrant out for his arrest. Though India formally requested his extradition, the Canadian government denied the request, stating that Parmar was a Canadian citizen and that no formal extradition treaty existed between Canada and India.<sup>177</sup>

### ***Eggs Thrown at the Indian High Commissioner***

An event that occurred soon after Parmar's return to Canada brought renewed attention to the Sikh extremists.

On May 7, 1982, responding to a tip, Kobzey and another RCMP Security Service officer, Neil Eshleman, were at the Vancouver airport for the arrival of the High Commissioner from India.<sup>178</sup> They were warned of a possible demonstration with eggs to be thrown at the High Commissioner. RCMP VIP Security was advised and was present as well. The demonstration and egg-throwing occurred as predicted.

The officers noted that about 50 to 70 members of the Sikh community were present, including children. About 35 massed in a group on the sidewalk in front of the Domestic Arrivals level, donned black robes and produced black triangular flags. Kobzey identified the group's leader as Surjan Singh Gill, and pointed this out to Cpl. Bob Grey of VIP Security Section and Insp. Rob Fowles of the Vancouver Police Department.

---

<sup>174</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3721.

<sup>175</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3722.

<sup>176</sup> Exhibit P-101 CAA1087, p. 33.

<sup>177</sup> Exhibit P-101 CAA1087, p. 33.

<sup>178</sup> These events are described in Exhibit P-101 CAB0026, pp. 1-2.

When the High Commissioner, Dr. Gurdial Singh Dhillon, was leaving under the escort of VIP Security, the crowd spotted him and surged toward him and the vehicles, throwing several eggs. Two eggs struck Dr. Dhillon on the right side of his neck, and several hit the windshield and roof of the car.

Kobzey told the Inquiry that this incident made him aware of the significance of the protesters, who had announced that they would carry out an act of violence against an internationally protected person and embarrass the Government of Canada. Kobzey went on to say that greater attention ought to be paid to monitoring Sikh activism/extremism. His intelligence report served notice to his superiors and counterparts at HQ that this event raised the spectre of future security problems, and that more attention ought to be paid to such issues along with the allocation of sufficient resources to ensure good coverage. Despite Kobzey's efforts, the RCMP Security Service maintained the Sikh extremism investigation at a low priority.

In 1984, Kobzey began to receive information regarding threats involving shootings and bombings in relation to the Khalistan issue. His assessment was that there was a potential threat to both Indian missions in Canada and to prominent moderate Sikh and Hindu leaders in Canada.<sup>179</sup>

### ***Operation Bluestar and the Invasion of the Golden Temple***

A few months later, on June 5, 1984, the invasion of the Golden Temple enraged and united Sikhs around the world. Protests immediately escalated. In Vancouver, 20,000 Sikhs protested outside the Indian Consulate, many calling for the death of Prime Minister Indira Gandhi.<sup>180</sup>

Following Operation Bluestar and the escalation of Sikh extremism, Kobzey observed changes in the Vancouver Sikh community. Through interviews with various individuals, he found that emotions were running high, particularly among community members involved in the Babbar Khalsa and the International Sikh Youth Federation in Vancouver. Many community members expressed their anguish and were vocal about the need for some kind of revenge for the invasion of the Golden Temple by the Government of India's military and for the resulting loss of life. Kobzey became very concerned:

I felt that we had the makings of a serious problem for the security of Canada, for our citizens, and possibly repercussions outside of Canada, in terms of Canadian citizens going some place and creating a problem.<sup>181</sup>

---

<sup>179</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3722-3727.

<sup>180</sup> Exhibit P-101 CAA1087, pp. 5, 11-13.

<sup>181</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3730.



### ***The Parmar Warrant***

To add to the tension, in July 1984 Parmar was released from jail in West Germany, where he had been held for over a year. He promptly returned to Vancouver. Kobzey was concerned and brought this information to the attention of his superiors at the newly created CSIS.<sup>182</sup> It was agreed that a *CSIS Act* section 21(2) warrant would be sought against Parmar. Kobzey was tasked with preparing the briefing package to submit to Burgoyne in the HQ CT.<sup>183</sup>

### ***Level 4 Application for Parmar***

Due to the urgency created by the storming of the Golden Temple, the return of Parmar and the escalating tensions in the community, Kobzey<sup>184</sup> applied for level 4 coverage of Parmar. Kobzey's application included information about Parmar's activities in India and his arrest in West Germany, which Kobzey and investigators from other CSIS regions had entered into the Narrative Storage and Retrieval (NSR) system – the national CSIS database.

The NSR provided a useful, centralized resource from which CSIS investigators across the country could access information about related investigations. For example, Parmar's infamous statement in Calgary when he "...strongly urged Sikhs to unite, fight and kill in order to revenge the attack on the Golden Temple in the Punjab" was entered into NSR by CSIS agents in Calgary and accessible by Kobzey.

The application for a level 4 investigation was made: to identify the links between Parmar and Sikh terrorist elements in India; to determine Parmar's intention towards the Khalistan liberation movement, and his intent to use violence against Indian interests in Canada and abroad; to identify and assess Parmar's prominence within the Canadian Sikh community and thereby establish the threat he posed to the Government of India and its interests in Canada; and to permit the direction of all aspects of CSIS resources against Parmar.<sup>185</sup>

Kobzey's application package was sent to HQ and the information was incorporated into the HQ application to TARC.<sup>186</sup> The HQ application contained information to which Kobzey did not have access, such as information from External Affairs and other regions. This included information that Parmar was viewed within the Canadian Sikh community as something of a hero whose influence was second only to Bhindrawale. The HQ assessment concluded that the pro-Khalistan movement in Canada could be expected to become much more significant as a result of Parmar's activities.<sup>187</sup> HQ's centralized role meant

---

<sup>182</sup> The RCMP SS had been disbanded and CSIS created on July 16, 1984.

<sup>183</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3731, 3733.

<sup>184</sup> The information in this section is drawn from Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3731-3741.

<sup>185</sup> Exhibit P-101 CAB0139, p. 4.

<sup>186</sup> See Exhibit P-101 CAB0139 for the HQ application to TARC.

<sup>187</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3739-3740; Exhibit P-101 CAB0139, p. 3.



that the level 4 application contained all the relevant information. However, the CSIS top-down approach meant that investigators such as Kobzey might not be privy to certain relevant and useful information.

### ***Warrant Application to Intercept Parmar***

In August 1984, prior to receiving level 4 approval, Kobzey began to work on a warrant application package for authority to intercept Parmar.<sup>188</sup> It took one month to prepare the material, using local files and the NSR, along with additional information from the VIIU, VIP Security, and Immigration officials, because Kobzey's other duties precluded him from working full-time on the application.

Since any warrant product on Parmar would likely need translation, the warrant application went all the way up the chain in BC Region to the DG, Randil Claxton. This ensured that Kobzey's superiors supported the warrant and that there was a commitment "...to obtain the services of a security-cleared translator to debrief the product; and that we had the space within the technical section available within their bank of equipment for them to bring the line up, should the warrant be approved."<sup>189</sup> The CI&W chief was also required to sign off on the warrant, since it would be his responsibility, if the warrant was approved, to set up the line, maintain it and debrief personnel. The CI&W Section communicated the final warrant application to HQ in late September or early October.<sup>190</sup>

Kobzey saw his role as "...preventing acts of violence against citizens or people under our protection in this country or against property or the same things happening outside of our country by our citizens."<sup>191</sup> He felt that the situation with regard to Parmar was urgent, due to the latter's violent threats, which were documented in the warrant application. These included what Kobzey characterized as sinister aspects of Parmar's preachings, including: killing 50,000 Hindus; harassment of Embassy, High Commission and Consulate personnel; blowing up of embassies; and seeking revenge on the Hindu government.<sup>192</sup> As well, the fact that the threats were tied to religious fervour increased Kobzey's sense of urgency. He told the Inquiry that:

The possibility of a person being so upset at sacrilege or alleged sacrilege which took place against the holy site or shrine and would cause them to commit acts of violence, was something that I was attuned to and aware of.<sup>193</sup>

Kobzey also commented on the history of the Sikhs and how they not only prided themselves on their involvement in the military, but that they were also "...valorous in the way they conducted themselves in battle."<sup>194</sup>

188 Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3744.

189 Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3745.

190 Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3741-3760.

191 Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3743-3744.

192 Exhibit P-101 CAB0144, pp. 3-4.

193 Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3753.

194 Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3753.

Parmar's allegedly close association with Bhindranwale suggested that he would have access to weapons and explosives and to persons who were skilled in their use. Kobzey inferred from the association of these two men that Parmar might have connections to members of the Sikh community who had the technical expertise to develop explosive devices, and, potentially, to blow up embassies. Kobzey therefore considered it critical to obtain a warrant quickly to learn as much as possible about Parmar, his associates, his contacts worldwide, any involvement in the movement of money, and whether he was looking for arms, munitions, and so on.<sup>195</sup>

The warrant application also addressed rumours within the community that Parmar was an agent of Indian Intelligence. His 13-month incarceration in a West German jail was seen by some community members as a ploy to give him credibility with the Canadian Sikh community. Kobzey saw some merit in the argument that Parmar had something to hide – perhaps training in the field of intelligence work.<sup>196</sup>

Kobzey stressed the relevance of these concerns to the warrant application. On the one hand, Parmar espoused terrorist actions or acts of violence for a political objective. On the other, if he were an intelligence officer, he would also be a security threat to Canada through the creation of problems and unrest within the émigré community as a result of portraying himself as a terrorist.<sup>197</sup>

Kobzey was further concerned that, if Parmar was an agent of the Indian Intelligence Service, he would inspire others to commit acts of violence. He noted that the warrant was essential to enable the agency to determine whether Parmar was in fact a terrorist threat, and what his motives were. A major concern was that Parmar portrayed himself as a fundamentalist Sikh, although some intelligence suggested that he was not. The goal was to deploy appropriate resources to determine exactly what Canada was facing.<sup>198</sup>

A five-month process ensued until the warrant was granted.<sup>199</sup> Kobzey had continued to investigate Sikh extremism in Vancouver, albeit with great difficulty due to the lack of a warrant and no human source coverage. Meanwhile, tensions in Vancouver continued to escalate in response to actions in India.

### ***The Assassination of Indira Gandhi and Reaction in Canada***

On October 31, 1984, the assassination of Prime Minister Indira Gandhi by her Sikh bodyguards added fuel to the escalating tension between Sikhs and India worldwide:

---

<sup>195</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3754-3755.

<sup>196</sup> Exhibit P-101 CAB0144, pp. 5-6.

<sup>197</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3756-3757.

<sup>198</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3758-3759.

<sup>199</sup> See Section 1.3 (Pre-bombing), Parmar Warrant.

That evening, full-scale anti-Sikh rioting broke out across India, except in the Punjab. In New Delhi, gangs of Hindus roamed the streets beating, killing, and setting fire to Sikhs. The government acknowledged that 2717 Sikhs were killed in riots, with 2150 in Delhi alone. 50,000 Sikhs fled from the capital to the Punjab and another 50,000 escaped to government-run refugee camps.<sup>200</sup>

In Canada, many Sikhs celebrated the death of Indira Gandhi.<sup>201</sup> Kobzey had strong concerns because of the manner in which the assassination was planned and carried out. After killing the Prime Minister in the presence of army staff, the bodyguards laid down their weapons and said that they had done what they needed to do. Kobzey noted that this indicated a religion-based motivation beyond the norm. The inference was that there could be similar conviction within the Babbar Khalsa group, or by Parmar, to carry out such actions in Canada. It was incumbent upon CSIS to get the warrant in place to learn more and advise the Government of Canada on how to proceed. Kobzey wrote to HQ about the delay regarding his urgent application for a warrant for Parmar.<sup>202</sup>

In the meantime, events in Vancouver continued to be of concern. There were conflicts over control of the gurdwaras, which were a huge source of money, as Sikhs would give generously to them. Parmar was visiting gurdwaras and soliciting funds, which deeply disturbed Kobzey and those whom he interviewed in the community.<sup>203</sup>

In conducting his inquiries, Kobzey was in contact with the VPD's Indo-Canadian Liaison Team. They too were concerned by what they saw. Kobzey stated that, in the intelligence community, Sikh extremism was an issue of great concern that needed to be addressed.<sup>204</sup>

### ***Warrant Approval for Parmar Finally Obtained***

On March 14, 1985, the Parmar warrant was approved by the Federal Court and deemed valid for a year.<sup>205</sup> BC Region was notified on March 18, 1985.<sup>206</sup> On March 28<sup>th</sup>, the BC Region Chief of CI&W informed the DG CI&W that the intercept on Parmar had been installed on March 25, 1985, over five months after BC Region submitted its urgent application for a warrant.<sup>207</sup>

### ***Delays in Finding a Translator***

BC Region employed a transcriber, Betty Doak, to report on any information spoken in English as well as to record when calls were made, to whom, and

<sup>200</sup> Exhibit P-101 CAA1087, pp. 11-12.

<sup>201</sup> Exhibit P-101 CAA1087, p. 13.

<sup>202</sup> See Exhibit P-101 CAB0166.

<sup>203</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3764.

<sup>204</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3765.

<sup>205</sup> Exhibit P-101 CAD0024, p. 2.

<sup>206</sup> Exhibit P-101 CAA0133, p. 1.

<sup>207</sup> Exhibit P-101 CAB0206, p. 1.

at what telephone number. She also was to have a coordinating role with the translator. At the time, however, BC Region did not have a Punjabi-speaking translator.

On May 16, 1985, BC Region sent out an urgent request to all regions for recruitment of Punjabi translators.<sup>208</sup> In the meantime, BC Region arranged for the Parmar warrant product to be shipped to Ottawa for translation. This resulted in two major problems. First, Kobzey and Ayre did not have contact with the translator to discuss the intercept product. Normally, they would have had daily access to the translator to discuss any concerns or questions and to keep the translator updated on the progress of the investigation. The second problem was that the delay in mailing the tapes meant a delay in translation; and this delay ballooned into an extensive backlog of tapes.<sup>209</sup>

Despite instructions from HQ, the urgency of the situation and the priority of the threat, nothing changed in terms of the translation of the Parmar product until June 7, 1985 when a security-cleared translator was found for BC Region after the passage of several months.<sup>210</sup>

The next day, Kobzey took his annual leave and did not return until the evening of June 22<sup>nd</sup>. The last thing Kobzey did before he took his leave was to "...brief up the translator ... [on] what we were looking at with respect to the line ...."<sup>211</sup> There was no time to develop a relationship with the translator, to go over the transcript and answer questions, or for the translator to become familiar with the target, Parmar.

### ***Physical Surveillance Coverage***

In April 1985, soon after obtaining the Parmar warrant, Kobzey and Ayre submitted a request for physical surveillance (PSU) coverage of Parmar. The purpose was to complement the intercept warrant, especially in anticipation of the upcoming one-year anniversary of the storming of the Golden Temple, and Indian PM Rajiv Gandhi's June visit to the United States.<sup>212</sup>

Kobzey conducted briefings for the PSU surveillants to guide them on what information the investigators needed from surveillance. The surveillants were tasked with locating Parmar, and were provided a priority list of individuals associated with Parmar to cover. Kobzey would update the surveillants' folders if new information came in from other regions.<sup>213</sup>

Kobzey advised them that the target they were following was "...a person who was involved in activities that were extremely ... dangerous." He testified that the surveillants "...knew what they had to do. And they knew the importance of it."<sup>214</sup>

<sup>208</sup> Exhibit P-101 CAB0234, p. 1.

<sup>209</sup> For an in-depth description of the tape problems, see Section 4.3.1 (Post-bombing), Tape Erasure.

<sup>210</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3814.

<sup>211</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3811-3814.

<sup>212</sup> See Exhibit P-101 CAB0209 and Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3793-3794.

<sup>213</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3827-3828.

<sup>214</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3828.

However, coverage was neither ongoing nor immediate. Coverage of Parmar was sporadic during April and May, and ongoing daily coverage of Parmar did not begin until June 1, 1985.<sup>215</sup>

Kobzey had to lobby the DDG ops, Kenneth Osborne, to get any PSU coverage at all, due to the lack of resources and the priorities of other targets in BC Region. Kobzey indicated that he was able to obtain surveillance more regularly as the profile of Sikh extremism rose.<sup>216</sup>

### ***Further Evidence of Growing Tension***

On May 28, 1985, BC Region received an important telex from the DG CT, Deschenes, warning of the heightened tensions created by the upcoming anniversary of the storming of the Golden Temple and the concurrent visit of PM Rajiv Gandhi to the US. Kobzey testified that, based in part on the Deschenes document, Sikh extremism was now considered a threat that matched the priority level of CI. Kobzey testified that information from this document, the attempted murder of an Indian government minister in New Orleans, and arrests made in the US earlier that year, all highlighted the significance of potential violence against Gandhi, or other Indian ministers, and HQ was advising all the regions and districts to be extra vigilant with respect to the issues of Sikh extremism.<sup>217</sup>

The Deschenes memorandum also called for increased scrutiny of wiretap information. This expedited process meant that information from the intercepts was urgent, and that the investigators involved had immediate access, so they or HQ could do whatever was required with that information quickly.<sup>218</sup>

On June 4, 1985, the Duncan Blast occurred. On that day, two CSIS agents witnessed Parmar, Reyat and an unidentified third person enter a wooded area near Duncan, BC.<sup>219</sup> The surveillants heard a loud bang which was interpreted by the senior agent as a gunshot. These events resulted in uninterrupted mobile surveillance of Parmar until June 17, 1985, an unprecedented amount of coverage for a CT target at the time.

### ***Incomplete Information***

When Kobzey took his leave on June 8, 1985, the belief in BC Region appeared to be that the elevated threat situation had passed, though tensions would remain high. However, in his testimony at the Inquiry, Kobzey expressed his view that BC Region was not in possession of all the relevant information that could have aided in a more accurate assessment of the continuing threat, and would have resulted in him delaying taking leave.<sup>220</sup>

---

<sup>215</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3795-3796, 3828.

<sup>216</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3774.

<sup>217</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3790.

<sup>218</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3791-3792.

<sup>219</sup> See Section 1.5 (Pre-bombing), Mr. X.

<sup>220</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3805.

First, CSIS had not received the June 1<sup>st</sup> Telex sent from Air India in Bombay to airports around the world. It stated that vigilance should be maintained for the entire month of June and warned of time-delayed devices being placed in aircraft.<sup>221</sup> Kobzey believes this document would have given him the "... opportunity to ask for extended surveillance for the entire month."<sup>222</sup>

Second, the information gathered regarding the Duncan Blast had been misinterpreted as a gunshot.<sup>223</sup> Kobzey testified that, had the information from the surveillants been described differently – for example, if they had suspected dynamite in the blast – he would have acted much differently.<sup>224</sup>

Third, CSIS BC Region did not benefit from the experience being developed in the Windsor area, where another Sikh extremism wiretap had been set up prior to the bombing. This intercept related to a US operation in May 1985. A young CSIS investigator, Charlie Coghlin, had been reviewing the intercept product and had developed an ear for the code words used by Sikh extremists.<sup>225</sup>

Because of incomplete information, Kobzey believed he could take vacation leave. He was facing burnout due to long hours on the investigation with little institutional support. He went sailing and was not reachable during his leave. This was the pre-cellphone era, and he had no radio communication on board his vessel.<sup>226</sup>

Ayre was left in charge of the Sikh extremism investigation in BC Region, in consultation with other members. During that time, Osborne decided to terminate surveillance on Parmar, after a rather lengthy continuous period. That decision was taken prior to Kobzey's return from vacation.

During Kobzey's absence he had not been made aware that surveillance had been called off against Parmar, nor of the Khurana information and the alleged "wait two weeks" comment.<sup>227</sup> Code words used by the subjects of the Windsor investigation had not been shared with BC Region, and so the use of the same code words in the Parmar intercept material was not caught. Kobzey testified about returning home and learning of the bombing. His first reaction was:

"That expletive Parmar, he did it, they did it"; and that was my gut instinct ....<sup>228</sup>

### ***The June 17, 1985 Situation Report***

Despite Kobzey's absence, the BC Region continued to assess the threat from Sikh extremists as high. BC Region submitted its daily situation report to assist

<sup>221</sup> Exhibit P-101 CAA0174; See also Section 1.2 (Pre-bombing), June 1<sup>st</sup> Telex.

<sup>222</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3811.

<sup>223</sup> See Section 1.4 (Pre-bombing), Duncan Blast.

<sup>224</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3805.

<sup>225</sup> Exhibit P-101 CAA0308, CAA0309(i).

<sup>226</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3813, 3838.

<sup>227</sup> CSIS BC Region was aware of the Khurana information.

<sup>228</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3812.

CSIS HQ in drafting the June 18, 1985 TA requested by the RCMP. The report noted that although no incidents had occurred, the threat potential from the Sikh community continued to be high. BC Region warned about the particular nature of the threat, describing it as political, with religious fanaticism being used as the driving force to achieve its goals.

Ultimately, they warned that "...time is of no consequence to the Sikh extremist element in reaching their objectives" and "...we can expect the overall problem to remain constant for some time to come."<sup>229</sup> BC Region appeared to understand that the Sikh extremist threat was real and serious, but remained unable to provide sufficient insight to prevent the bombing of Air India Flight 182.

### **Windsor District Investigation**

In 1985, the secure CSIS communication system was not employed in all districts. The Toronto office, responsible for the entire Southwestern Ontario Region, had various district offices reporting to it. One of those was the Windsor District, an office with three staff in 1985. Toronto had access to NSR, but the district office did not. This meant that messages for Windsor would be sent through the Toronto office. Similarly, Windsor had to report to HQ through the Toronto office, where the manager would sign off on reports before they were entered into NSR.<sup>230</sup>

Early in 1985, Windsor District observed activity related to Sikh extremism. In fact, HQ sent out a request on February 21, 1985 for further information, specifically in response to material received from Windsor District.<sup>231</sup> An escalation of this activity over the ensuing months led to a cross-border police investigation, with the RCMP taking the lead in Canada. CSIS gathered intelligence from the early stages and throughout the police investigation.

### **New Orleans Plot**

Events in the US in early May 1985 (the "New Orleans Plot") led to greater CSIS attention to the activities of Windsor-area Sikhs. The New Orleans Plot involved an attempted assassination in the US. A group of Sikhs in the New York area initially plotted to assassinate Prime Minister Rajiv Gandhi, but turned their attention to a softer target, an Indian cabinet minister who was convalescing in a New Orleans hospital.<sup>232</sup> The US Federal Bureau of Investigation (FBI) was aware of the plot, and a number of the individuals involved were arrested. The assassination attempt was foiled, but two fugitives from the FBI, Lal and Ammand Singh, were not caught and it was believed they escaped to Canada.<sup>233</sup> Days after the bombing of Air India Flight 182, these two individuals were named in Canadian newspapers as potential suspects.

<sup>229</sup> Exhibit P-101 CAA0219.

<sup>230</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3424-3425.

<sup>231</sup> Exhibit P-101 CAF0111; Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3424-3425.

<sup>232</sup> Exhibit P-101 CAA1086, p. 3, CAA1099, p. 2.

<sup>233</sup> Testimony of Jim Cunningham, vol. 52, September 25, 2007, pp. 6391-6392.



The FBI soon found links between the Sikhs from the New Orleans Plot and Canadian Sikhs. An RCMP threat assessment dated June 14, 1985 reports that:

A current FBI and Secret Service investigation has implicated Vancouver, Toronto and Windsor Sikhs with the conspirators arrested in New Orleans in the foiled Gandhi assassination plot.<sup>234</sup>

On May 13, 1985, Russell Upton wrote a memo addressed to the CSIS representative in Washington and the CSIS Director General of Foreign Liaison, Toronto Region and Windsor District, regarding his concerns following the discovery that the New Orleans Plot had potential Canadian connections. In it he stated:

It would appear that the ... Babbar Khalsa group, in Windsor and area has [established] an important relationship with US activists. This Canada/USA relationship in an area of Sikh terrorism is of special interest and concern to us at this time.<sup>235</sup>

Around the same time, the Sikh Desk at HQ gained another analyst, Bill Dexter. He took over the analysis of reports from the regions to free up Burgoyne to concentrate on the developments in Windsor:

[B]ack in early June, I was involved with an operation down in Windsor, Ontario, where we had a group of Sikhs that were trying to smuggle Uzi machine guns into Canada, and a lot of my time was devoted to that operation.<sup>236</sup>

Over the next few weeks, Burgoyne, considered the CSIS Sikh expert at HQ, became focused entirely on the Windsor situation, writing warrant applications and overseeing the results of the investigation. It was believed at the time that Sikhs in the Windsor area were attempting to gather weapons to send to India. However, Inspector Lloyd Hickman from RCMP Protective Services proposed an alternate scenario in a May 28, 1985 memo:

The only area of concern from the Protective Policing area was the fact that these Sikh extremists in the Windsor/Detroit area who are buying weapons may not be targeting the upcoming Gandhi visit, but may in fact be targeting Indian interests in Canada of which we have a protective responsibility.<sup>237</sup>

---

<sup>234</sup> Exhibit P-101 CAC0438.

<sup>235</sup> Exhibit P-101 CAF0826, p. 3.

<sup>236</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3432-3434.

<sup>237</sup> Exhibit P-101 CAC0356.

Hickman had no further involvement in the Windsor investigation.<sup>238</sup>

On June 11, 1985, the RCMP Windsor Detachment executed search warrants on the homes of Avtar Singh Kooner and Surjit Singh Agimal. The police were looking for weapons allegedly imported from the US. Kooner was known to have travelled to New Orleans in early May, but there was no further evidence to link him to the New Orleans Plot. After the searches, the RCMP launched an interview program involving Windsor NCIS and they were aided by CSIS's Coghlin.<sup>239</sup>

As well, the RCMP reported that they were continuing to work "...shoulder to shoulder with representatives from the Federal Bureau of Investigation and the US Secret Service from Detroit and have had an excellent working relationship in this regard."<sup>240</sup> That "excellent" relationship did not extend to CSIS, perhaps foreshadowing some of the difficulties to be experienced later in the Air India investigation.

On June 17, 1985, CSIS Windsor District sent a damning telex through Toronto Region to HQ. The CSIS investigator commented that CSIS found out about the RCMP searches only by accident, and had not been made aware through the usual liaison channels:

Not wishing to stir up any hornet's nests, the writer, nonetheless feels obliged to state that I personally felt the searches conducted by the RCMP in Windsor were premature and proved ineffectual.... The searches came up negative because neither Agimal nor Kooner are stupid enough to keep such weapons in their homes. In the final analysis, the RCMP came up with one handgun and some passport falsification equipment .... During questioning, Kooner as much as told their interrogators to either charge him, if there was any evidence, or release him. He was released.<sup>241</sup>

Additional comments in the telex show that similar strains on the RCMP-CSIS relationship were being felt in Toronto.<sup>242</sup>

### ***Effect on Other Investigations***

The Windsor investigation did not result in any intelligence that could have prevented the bombing, but it certainly had an effect on the subsequent investigation. A CSIS wiretap was in place during the Windsor investigation.

---

<sup>238</sup> Testimony of Lloyd Hickman, vol. 34, May 28, 2007, p. 3978.

<sup>239</sup> Exhibit P-101 CAB0304, p. 3.

<sup>240</sup> Exhibit P-101 CAB0304, p. 4.

<sup>241</sup> Exhibit P-101 CAB0311, pp. 2-3.

<sup>242</sup> Exhibit P-101 CAB0311, p. 5.

While reviewing the intercept material, Coghlin became aware of certain common code words and phrases. It was not realized until months after the bombing that similar code words were used in the Parmar intercepts.<sup>243</sup> At that time, Coghlin had been transferred to HQ to help with the analysis and was given access to the translators and transcriber logs for the Parmar intercept.

HQ Sikh Desk, however, had access to both reports on Windsor intercepts and those Parmar intercepts that had been translated prior to the bombing. The work was split, with Burgoyne working on the Windsor investigation and Dexter working on the Vancouver investigation. The “need-to-know” principle may have affected the information that flowed between them. Two additional complications may also have played a role in the lack of understanding of the code words before the bombing. First, the Parmar intercept product was subject to a severe backlog. Second, the Windsor reports would also have been delayed to some extent by the routing process that required such reports to go first to Toronto and then to HQ.

Finally, the Windsor investigation may have had one severe consequence: it seems to have provided further evidence that Sikhs were interested in arms acquisition and trading, rather than anything to do with bombs, therefore reinforcing the very narrow view regarding the means of threat (assassination as opposed to sabotage) posed by Sikh extremists that seems to have pervaded CSIS at the time.

### ***The June 17, 1985 Situation Report***

Windsor District also submitted a situation report to assist CSIS HQ in drafting the June 18, 1985 threat assessment. It noted that the RCMP’s raids on the residences of Kooner and Agimal were ineffectual and served only to bolster the Sikh extremists’ status in the Sikh community.

Windsor District warned that the threat against Indian interests remained high. They expressed their view that “...the BK will simply ride out the RCMP campaign, re-group after the force loses interest and attempt to strike at some less high profile target, once the heat is off.”<sup>244</sup> As in the BC Region, Windsor investigators appeared to understand the seriousness of the Sikh extremist threat, but could provide little insight into the specific nature of that threat.

## **3.3 CSIS’s Threat Assessment Failures**

### **What Went Wrong?**

In the year prior to the bombing, CSIS had increasingly dedicated resources to investigate the growing threat of Sikh extremism in Canada. CSIS issued 70

---

<sup>243</sup> Exhibit P-101 CAA0308, CAA0309(i).

<sup>244</sup> Exhibit P-101 CAB0312, p. 2.

threat assessments concerning Sikh extremism and aviation security, including 13 that related specifically to Air India.<sup>245</sup> It is clear that CSIS was investigating this growing threat and disseminating information to advise other agencies about it. What then, went wrong?

Effective intelligence assessment requires successful efforts at every stage of the intelligence cycle: timely, relevant setting of intelligence priorities; comprehensive intelligence collection; analytical tools to effectively process information; and information channels to disseminate and discuss the intelligence.

The Commission's review of the CSIS investigation into Sikh extremism prior to the bombing uncovered deficiencies in each component of the intelligence cycle. The primary reasons for the deficiencies in the CSIS threat assessment process are:

- CSIS was in its infancy when the Air India bombing occurred. As such, already scarce investigative resources were diverted to dealing with transition issues and to developing operational policies and a clearer understanding of its new mandate.
- CSIS failed to adjust its intelligence priorities in a timely manner. The agency failed to recognize the changing threat paradigm in the early-to-mid 1980s from counter-intelligence to counterterrorism and failed to recognize the threat of Sikh extremism in particular.
- CSIS collection and analysis efforts with respect to the threat of Sikh extremism were clearly hindered by a lack of resources and expertise.
- CSIS intelligence analysis capacity was hampered by "tunnel vision" about the expected nature of threats to Indian interests in Canada.
- Information sharing within and outside the agency was not free-flowing, resulting in threat assessments and responses that were not fully informed.
- There was a lack of coordination in the Government's assessment and response to the threat of Sikh extremism, which impeded communications channels for feedback that could have improved or challenged CSIS TAs. This prevented CSIS from producing meaningful TAs that were relevant to the RCMP response operations.

The effects of each of these intelligence failures are discussed below.

---

<sup>245</sup> Exhibit P-101 CAB0902: Security Intelligence Review committee, "CSIS Activities in Regard to the Destruction of Air India Flight 182 on June 23, 1985", November 16, 1992 [1992 SIRC report].

### 3.3.1 The Infancy of CSIS

It would be tempting, but wrong, to conclude that the Air India tragedy simply came at a bad time. CSIS had been created less than one year earlier, and the national security community was still dealing with the difficulties of adjusting to the new structure recommended by the McDonald Commission and implemented by the Security Intelligence Transition (SIT) Group. The fact that CSIS was operating when it was incapable of doing so efficiently is not an acceptable excuse.

Jim Warren, who reviewed the CSIS Air India file in 1986 during his term as DG CT, admitted that CSIS was not "...up and running at full speed" when it was created on July 16, 1984.<sup>246</sup> CSIS itself opened its submission to the Honourable Bob Rae with the statement that, at the time of the Air India bombing, it was an organization in its infancy that had not yet had the opportunity to fully resolve a number of policy and infrastructure issues. It was operating new administration, accommodation, communications and computer systems. CSIS had yet to develop a methodology to deal with a new system of extensive external review.<sup>247</sup>

The Inquiry evidence shows that the *CSIS Act* was passed with virtually no attempt to identify the effect of civilianization on day-to-day operations. The new agency was under-resourced, and no attempt was made to infuse the agency with any coherent identity, all of which made the transition chaotic. The operations of the new civilian service suffered, as all personnel experienced a steep "learning curve" in understanding the effect of their new identity on their pre-existing duties. The evidence leaves the distinct impression that CSIS was created with little thought to the practicalities of running a national civilian intelligence agency.

This lack of preparation affected CSIS operations. Important investigative initiatives were delayed or not initiated. Approval for the "urgent" warrant to intercept the communications of Parmar was delayed for five months due to the "priority" need to convert old RCMP SS warrants to new CSIS warrants.<sup>248</sup> This delay led to an important lost opportunity for CSIS to obtain intelligence and potential evidence that would be subsequently needed by the RCMP.

The Commission has considered the influence of the infancy of CSIS on the agency's ability to assess the threat of Sikh extremism, and asked whether the problems that occurred were inevitable or avoidable.

#### ***Gaps in Policies and Procedures***

The focus of the drafters of the *CSIS Act* was on passing the legislation, and little priority was placed on developing the policies and practices necessary for the

<sup>246</sup> Testimony of James Warren, vol. 48, September 19, 2007, p. 5942.

<sup>247</sup> Exhibit P-101 CAA1086, p. 1.

<sup>248</sup> The full story can be found in Section 1.3 (Pre-bombing), Parmar Warrant.

new Service's day-to-day operations. CSIS management was left to fill these gaps in policy and procedure, a task that proved to be significant, cumbersome and unsupported by adequate resources.

### ***The Focus on Legislation***

It is important to understand the political climate under which the *CSIS Act* was passed. While the Government began transition discussions in 1982, the focus remained on the drafting of the legislation itself. The first legislative attempt, Bill C-157, was studied extensively over the summer of 1983 by a special committee of the Senate (the "Pitfield Committee"). Following the Pitfield report, issued in November 1983, the Bill was allowed to die on the order paper. The second legislative attempt, Bill C-9, which incorporated virtually all the recommendations of the Pitfield Committee, was still in progress at the beginning of 1984. At that time the creation of the new Service was still not a certainty.<sup>249</sup>

Realizing that a general election was forthcoming in September 1984, the Liberal Government became increasingly preoccupied with "...getting the legislation through and getting on with the creation of the new organization" before the Parliamentary session closed for the summer.<sup>250</sup> During this chaotic political period, the *CSIS Act* was the last piece of legislation passed by the Liberal Government, just two days before Parliament recessed and two weeks before the newly-appointed Prime Minister, John Turner, called the election.<sup>251</sup> The Act was proclaimed in force just two weeks later, on July 16, 1984. The rush to pass and proclaim the legislation left little time for the development of the policies and procedures needed to guide the new agency.<sup>252</sup> A further complication was that, as a result of the September election, a new government was formed by the Progressive Conservative Party, which had little familiarity with the intricacies of the transition process and the new CSIS mandate.<sup>253</sup>

Jacques Jodoin, the Director General of Communications Intelligence and Warrants at CSIS HQ, commented on his impression of the work atmosphere in CSIS at the time:

You had to – like they say – jump off the truck and keep running; so we did. And it caused some problem, it caused some shortcomings and yes, that was the situation.<sup>254</sup>

When the *CSIS Act* passed and the SIT Group dissolved, all CSIS personnel were asked to "jump off the truck" that had been pushing them towards civilianization and to "keep running," with little guidance down the path envisioned by the

<sup>249</sup> Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6206.

<sup>250</sup> Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6206.

<sup>251</sup> Testimony of Geoffrey O'Brian, vol. 16, March 5, 2007, p. 1532.

<sup>252</sup> Testimony of Geoffrey O'Brian, vol. 17, March 6, 2007, pp. 1559-1560; Testimony of Jacques Jodoin, vol. 23, May 4, 2007, p. 2246; Testimony of Raymond Kobzey, vol. 33, May 24, 2007, p. 3819.

<sup>253</sup> Testimony of Geoffrey O'Brian, vol. 17, March 6, 2007, p. 1560.

<sup>254</sup> Testimony of Jacques Jodoin, vol. 23, May 4, 2007, p. 2246.

transition group. CSIS, in its first incarnation, was under-resourced, and faced with the daunting tasks of establishing its new civilian identity and developing the policies and procedures that conformed to its new mandate, while at the same time furthering its ongoing investigational priorities.

### ***Failure to Adequately Resource the New Service***

CSIS was not provided with adequate resources to carry out its operations,<sup>255</sup> and was stretched for personnel for years after its creation. There were many vacant positions, even in the first organization charts.<sup>256</sup> There were no new recruits for some months, while CSIS set up its own training academy at Camp Borden. The Camp Borden training program took six months, after which the recruits had to complete training in the field.<sup>257</sup> In this time of transition, CSIS managers were forced to allocate their scarce resources in the best possible manner to meet CSIS intelligence requirements.<sup>258</sup> Russell Upton, who was in charge of allocating resources within a large CT section that included Sikh extremism, noted that, while he fully recognized the seriousness of the Sikh extremist threat, due to this overall lack of resources, he was unable to spare any to augment the admittedly under-resourced HQ Sikh Desk.<sup>259</sup>

### ***Failure to Establish a Separate Civilian Identity***

An independent advisory team, headed by the Hon. Gordon F. Osbaldeston, was given a three-month term by the Solicitor General to produce recommendations regarding the CSIS framework of operational policies, the design of personnel management policies and any possible requirement for further studies.<sup>260</sup> The October 1987 Report, "People and Processes in Transition" (known as the "Osbaldeston Report"), found that CSIS's operations were hampered by its failure to separate from its police background and to make the transition to its new civilian identity.

...there must be more capital expenditure for accommodation and administrative needs. CSIS still shares many operational and administrative facilities with the RCMP. A large percentage of CSIS employees still go to work in the morning at RCMP headquarters, making it rather difficult to generate and maintain the esprit de corps that is so important.<sup>261</sup>

For months after the separation, most lower-level CSIS personnel continued to work in the same building as the RCMP, while CSIS management were housed in

<sup>255</sup> Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6204.

<sup>256</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6122.

<sup>257</sup> Testimony of Raymond Kobzey, vol. 33, May 24, 2007, p. 3818.

<sup>258</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6183.

<sup>259</sup> See Section 3.3.3 (Pre-bombing), Failure to Allocate Resources for a detailed description of the effect of the lack of resources on CSIS pre-bombing investigation.

<sup>260</sup> Exhibit P-101 CAA0569, Appendix A: "Terms of Reference".

<sup>261</sup> Exhibit P-101 CAA0569, p. 29.



a separate building.<sup>262</sup> CSIS personnel still used RCMP stationery and were not issued business cards identifying their status as employees of the new civilian Service.

The separation process created turmoil in the relationships within the ranks of both the RCMP and CSIS. Some viewed the separation positively: there were those within the RCMP who were glad that the “barn-burning troublemakers” in the RCMP SS were gone,<sup>263</sup> and some within the RCMP SS that felt the separation was simply a formal recognition of long-standing conditions.<sup>264</sup> Others noted the negative consequences of the separation. The “brotherhood” that developed during the common training at the RCMP Depot was lost.<sup>265</sup> The ability of members of the Service and the RCMP to chat informally, as had been the case prior to separation, was impeded.<sup>266</sup> The respected RCMP identity was taken away and the new civilian Service had yet to establish any identity of its own.<sup>267</sup>

At the same time, in order to bolster the ranks, CSIS allowed for “direct entry”, which meant that police officers could join CSIS directly, bypass the requirement to attend Camp Borden and assume a higher rank than the civilian recruits who were required to attend training.<sup>268</sup> This procedure created tension within CSIS as testified to by Geoffrey O’Brian, a member of the SIT Group, who went on to hold numerous senior positions in CSIS:

...if you were a young person who joined CSIS, and started off at training, and suddenly here was someone else who’d just become a member of CSIS but had a police background and they jumped two levels on you; ... there was I suppose the inevitable tension.<sup>269</sup>

The “direct entry” procedure also did not help CSIS move away from its police roots towards greater civilianization, a complaint that was echoed by both SIRC and the Osbaldeston Report.

### ***Recognized Need for Wide-scale Policy Revisions***

The need for a review and rewrite of all CSIS policies became apparent early on. Archie Barr admitted that the SIT Group did not have the time to write many policies for the new Service during the transition process. Even basic policies relating to new staffing, pay and administration were yet to be developed.<sup>270</sup>

<sup>262</sup> Testimony of James Warren, vol. 48, September 19, 2007, p. 5941.

<sup>263</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, p. 1561; Exhibit P-437: Statement of Archie Barr, p. 4.

<sup>264</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, p. 1561.

<sup>265</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, p. 1561.

<sup>266</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3573.

<sup>267</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, p. 1562.

<sup>268</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, pp. 1563-1564.

<sup>269</sup> Testimony of Geoffrey O’Brian, vol. 17, March 6, 2007, pp. 1563-1564.

<sup>270</sup> Exhibit P-437: Statement of Archie Barr, p. 9.

The few policies that were issued tended to focus more on what CSIS was not to do, rather than what it was to do and how it was to do it. CSIS was no longer in the evidence-collection business.<sup>271</sup> CSIS collected only information that was “strictly necessary” to carry out its mandate. CSIS would protect its methods, the identities of sources and third party information.<sup>272</sup> It would be a more transparent agency, subject to political control and independent reviews. These policies made clear that CSIS was not to make the same mistakes as the RCMP SS. However, they did not make clear just how CSIS was to achieve that result.

On August 28, 1984, the Solicitor General, the Honourable Robert Kaplan, issued a ministerial directive,<sup>273</sup> declaring that all ministerial policy direction provided to the RCMP SS would remain in effect for the new civilian Service to the extent that it was not inconsistent with the *CSIS Act*. Kaplan acknowledged that:

There is undoubtedly a need to review all existing directions to identify those which require revision or updating and I understand that such a review is already being planned. I welcome this undertaking and look forward to being kept advised of the progress being made.<sup>274</sup>

While Kaplan understood the need to review and revise all policies for compliance with the *CSIS Act*, no policy task force was formed to carry out this daunting undertaking. Instead, CSIS personnel were expected to rewrite policy while dealing with ongoing operational imperatives. Some even felt that the policy-writing process should be postponed until CSIS had operated for some time in order to discover the practical changes that the new mandate would require.<sup>275</sup> It was understood that specific guidelines and policies would be developed as the agency matured. This approach, however, overloaded CSIS management with work and left personnel to operate with little guidance.<sup>276</sup>

### ***New Legalistic Policies and Procedures***

The policy-writing task itself was complicated and time-consuming. The Act imposed unprecedented legal oversight on CSIS activities<sup>277</sup> and, as no jurisprudence existed, nobody really knew what to expect.<sup>278</sup> Unlike in the days

<sup>271</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6124. See, for example, Exhibit P-101 CAA0040: Archie Barr issued a memorandum stating that “...as the *CSIS Act* contains no requirement for collection by CSIS of information for evidentiary purposes, no such capacity will be provided for within CSIS facilities.” The effect of this policy direction on CSIS operations is discussed in Section 4.3.1 (Post-bombing), Tape Erasure.

<sup>272</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6124.

<sup>273</sup> Exhibit P-101 CAA0091.

<sup>274</sup> Exhibit P-101 CAA0091.

<sup>275</sup> Exhibit P-437: Statement of Archie Barr, pp. 8-9.

<sup>276</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3572.

<sup>277</sup> For example, section 21 of the *CSIS Act* required Federal Court approval for all CSIS warrants. The *Official Secrets Act* under which the RCMP SS operated had required only the signature of the Solicitor General for warrant applications.

<sup>278</sup> Testimony of Jacques Jodoin, vol. 23, May 4, 2007, p. 2245; Exhibit P-437: Statement of Archie Barr, pp. 8-9.

of the RCMP SS, legal services became a major part of the CSIS operational decision-making<sup>279</sup> – a legalistic, bureaucratic, cumbersome, but necessary, process.<sup>280</sup>

Chris Scowen, *de facto* Deputy DG CT at the time of the bombing, told the Commission that they were “...walking on eggshells for the first months and the first couple of years” because there was uncertainty about which activities were affected by the Act and how. CSIS management relied heavily on the two lawyers in the Legal Branch for interpretations and explanation as to how the Act would apply.<sup>281</sup>

CSIS management faced the overwhelming tasks of revising administrative and operational policies to conform to the new legalistic requirements, while simultaneously furthering existing investigations and initiating new ones. Each of these tasks could have required management’s full attention.

The Director, Ted Finn, and his five Deputy Directors were responsible for the rewriting of policies to conform to the new CSIS mandate. They held weekly meetings to develop the necessary operational and administrative policies and procedures. However, as time passed, CSIS experienced increasing administrative difficulties, and the greater part of the meetings was spent discussing administrative, staffing and financial problems, rather than operations.<sup>282</sup> Ultimately, the need to revise basic administrative policies and practices proved so overwhelming that the development of operational policies and the furtherance of CSIS investigations suffered.

### ***Lack of Clear Procedures for Policy Development***

Even when CSIS did attempt to write policy, there appeared to be no established procedure for doing so. The confusion over the proper procedure to establish policy, along with unclear roles within CSIS management, resulted in policies of disputed validity. In addition, early attempts often resulted in bureaucratic, overly-cautious procedures that ultimately unjustifiably impeded CSIS investigations.

In April 1984, just prior to the creation of CSIS, Archie Barr wrote a memorandum to revise the tape retention policy to accord with the new non-evidentiary mandate of CSIS. The memorandum established that CSIS would no longer maintain facilities for the retention of tapes for evidentiary purposes.<sup>283</sup> The Barr memorandum was intended to modify a 1980 Ministerial Directive<sup>284</sup> that set out procedures for retention of evidentiary tapes by the RCMP SS, a practice no longer allowed under the new CSIS mandate. This memorandum

<sup>279</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6121.

<sup>280</sup> Testimony of Jacques Jodoin, vol. 23, May 4, 2007, p. 2245.

<sup>281</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6121.

<sup>282</sup> Exhibit P-437, Statement of Archie Barr, p. 5.

<sup>283</sup> Exhibit P-101 CAA0404.

<sup>284</sup> Exhibit P-101 CAA0010.

became a matter of controversy; as it was relied on to justify the subsequent erasures of Parmar intercepts after the bombing. At the time of its issuance, the memorandum was accepted as policy across CSIS. However in 1988, Solicitor General officials questioned the validity of this policy, particularly whether a ministerial direction could be modified or reversed by a decision of the SIT Group.<sup>285</sup> They noted that, although CSIS had indicated that it wanted the Ministerial Directive modified, no new modified policy was ever agreed upon for ministerial approval. This confusion caused concern during the Reyat trial, because the Solicitor General's staff concluded that the Barr memorandum could not be relied upon as established policy, as the proper procedure to change policy had not been followed, and thus, the Barr memorandum could not be used to justify the contentious erasure of the Parmar tapes.

In February 1985, Jacques Jodoin issued a memorandum<sup>286</sup> further revising the tape retention policy, based on his review of the warrant renewal process. He advised all regions and districts to make verbatim transcripts of any vague or incriminating passages, and to retain the underlying tape for one year or until the warrant renewal date. Jodoin's policy was intended to improve the CSIS warrant renewal process. However, Jodoin's memorandum was followed by some regions and ignored by others, including the BC Region. Justifications for why this policy was ignored included the fact that Jodoin, as an HQ manager of technical services, did not have the authority to impose policy on the operational units in the CSIS regions. Within the CSIS regions, the regional directors general had operational autonomy and, therefore, made the ultimate decision on whether to follow technical policy issued from HQ. However, had BC Region implemented the policy, the erasure of the Parmar intercepts could most likely have been avoided.

Ultimately, there was a recognized need to fill the gaps in policies and procedures to meet the new more legalistic requirements of the *CSIS Act*. However, CSIS management was given few resources, and little direction on just how to do this.

### ***Effect of Policy Gaps on Operations***

In general, at the operational level, RCMP SS policies carried over to CSIS unchanged. Personnel utilized the same vehicles, stationery, computer systems and methodology<sup>287</sup> with little modification for basic investigative operations like physical surveillance, transcriptions, translations and source recruitment.<sup>288</sup> Until sometime after CSIS was created, the only notable change with operational implications was that the intelligence officers had lost their peace officer status.<sup>289</sup>

---

<sup>285</sup> Exhibit P-101 CAF0260.

<sup>286</sup> Exhibit P-101 CAA0126.

<sup>287</sup> Testimony of Raymond Kobzey, vol. 33, May 24, 2007, p. 3818.

<sup>288</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6184; Testimony of Neil Eshleman, vol. 75, November 14, 2007, pp. 9440-9441.

<sup>289</sup> Testimony of Raymond Kobzey, vol. 33, May 24, 2007, p. 3818.

CSIS personnel were forced to take the time to learn about their new mandate and adjust their practices with respect to their new role. Because available personnel were scarce at the time, this requirement further taxed individuals who already had significant investigative responsibilities to meet. Inevitably, CSIS investigations suffered as personnel learned about the new mandate, followed more cumbersome processes, and re-established relationships, both within and outside of CSIS.

### ***Investigations “On Hold”***

Some CSIS operations were effectively put “on hold” as new policies and procedures were developed. The need to convert all necessary warrants to accord with the new Federal Court requirements mandated by the *CSIS Act* was a daunting task which took five months to complete. The day-to-day needs of ongoing investigations were set aside, unless shown to be urgent, in order to complete this conversion process. For the Sikh extremism investigation, this meant that BC investigator, Ray Kobzey, who was well aware of the serious threat presented by individuals such as Parmar, Bagri and Gill, was forced to pursue a warrant on Parmar only<sup>290</sup> – and the approval of the Parmar warrant itself was delayed until after the conversion process was completed.

In effect, because of the primacy of the conversion process, Kobzey was unable to apply for warrants on targets he considered to be serious threats, even if he normally had enough information to obtain the warrant.

### ***The Learning Curve***

All CSIS personnel experienced a learning curve, as they became familiar with the new mandate and its effect on operations.<sup>291</sup> Russell Upton spoke about the steepness of that learning curve and the need for everyone to learn about the changes and all the new legal and regulatory requirements.<sup>292</sup>

It was not only CSIS personnel who experienced a learning curve with the new mandate, but also agencies with which CSIS worked closely. One of the first tasks that Randy Claxton, Director General of BC Region, took on after CSIS was created was to conduct briefings for their police partners about the new CSIS mandate.

As a result of CSIS being a new organization on the block it was imperative that I go to all the RCMP subdivisions and city police organizations and conduct briefings primarily to demystify what happened and explain that we are a legislated organization under the *CSIS Act*.<sup>293</sup>

---

<sup>290</sup> Testimony of Raymond Kobzey, vol. 33, May 24, 2007, pp. 3821, 3824-3825.

<sup>291</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6184.

<sup>292</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3573-3574.

<sup>293</sup> Exhibit P-101 CAF0816, p. 22.

### ***Educating the Public***

The new organization was unknown to the community. Reaching out to the public was a high priority but complicated due to lack of resources and policy. Jack Hooper testified that on the day CSIS was created, he was sworn in, returned to his desk, completed the RCMP SS report he had been drafting and sat down to type out three business cards.<sup>294</sup> Bill Turner told the Commission that there was even confusion caused by the lack of policy on whether their cards should be bilingual, have a crest or even identify CSIS. Turner stated that since there was no policy, employees did various things until Headquarters informed them otherwise.<sup>295</sup> Hooper knew immediately that CSIS investigators would have to be creative in establishing CSIS's identity in order to build trust in the community.<sup>296</sup>

Ultimately the lack of identity hindered CSIS operations, as investigators spent time "educating the community" about the new Service.

### ***Dealing with Cumbersome New Processes***

The requirements of the *CSIS Act* created increasingly cumbersome and legalistic processes to replace the previously straightforward processes of the RCMP SS and their affected operations. CSIS management was busy dealing with the many administrative and resource problems, and failed to provide timely operational direction. Personnel in the field were left to make their best guess as to what was required.

Kobzey told the Commission that the process was new and there were no templates in place. In attempting to obtain a warrant to intercept Parmar's activities, he drafted a document labelled "An affidavit pursuant to a judicial warrant" which was signed off by his Director General and submitted. Kobzey's information was repackaged to feed into the actual affidavit, drafted by Bob Burgoyne and signed off by Barr, and went to the Federal Court. Kobzey had no precedent to guide him in the creation of his memo. He tried to include information he felt to be germane to the issue of threats to the security of Canada. The role of the Sikh Desk, also struggling with the lack of guidance for the new warrant requirement, was then to "fine tune" the information and tailor it for presentation in court. Kobzey stated that the transition team, assigned to get CSIS up and running, produced no warrant guidelines and did not have time to address the warrant issue properly.<sup>297</sup>

The procedures that were developed were often overly cautious, as personnel were careful to adhere to the spirit of the McDonald Commission recommendations. In addition to the inexplicably complex warrant process developed for warrant approvals (as described in the Parmar warrant narrative),

---

<sup>294</sup> Testimony of Jack Hooper, vol. 50, September 21, 2007, pp. 6204-6205.

<sup>295</sup> Testimony of Bill Turner, vol. 66, October 25, 2007, p. 8279.

<sup>296</sup> Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6205.

<sup>297</sup> Testimony of Raymond Kobzey, vol. 32, May 23, 2007, p. 3748.

the first warrant applications were signed by, and brought to the Federal Court by, Archie Barr, the second-in-command in CSIS. The misallocation of resources implicit in this arrangement was eventually recognized, and this duty eventually moved down to a much lower level.<sup>298</sup> The increased level of political oversight over CSIS was an impediment; for example, the Parmar warrant was held up for months because of concerns from the Solicitor General's office, concerns which eventually proved to be of no relevance.<sup>299</sup>

### ***Tensions in Relationships Within and Outside of CSIS***

Tensions persisted within and outside of the new civilian Service. Ex-RCMP SS members were given the option to bridge back to the RCMP within two years of the CSIS creation,<sup>300</sup> raising questions with CSIS employees about the wisdom of becoming part of the new agency.<sup>301</sup> Restructuring was going on all over CSIS, forcing many CSIS members to establish new working relationships.<sup>302</sup>

CSIS personnel also testified about the change in relations with some RCMP officers that occurred after its creation. Kobzey noted that it was very difficult, in some cases, to convince old RCMP colleagues that, although CSIS personnel were now "civilians," they were the same people, doing the same job. He testified that, as an RCMP SS member, he had been able to effectively obtain information from the RCMP "...being that we're a member of the RCMP." After the transition, his access to RCMP material changed.<sup>303</sup>

### ***Loss of Basic Investigative Tools***

CSIS investigators lost some of the basic informational tools that they had relied upon to conduct investigations as members of the RCMP SS. After the transition, CSIS lost the ability to perform timely criminal records checks and basic biodata references, as they lost access to the Canadian Police Information Centre (CPIC) database.<sup>304</sup> Kobzey, when asked why he believed these capabilities were withheld from CSIS, replied:

**MR. KOBZEY:** We were no longer a police agency, sir.

**THE COMMISSIONER:** No, but you were serving an important function. I'm not putting the responsibility on CSIS, but wouldn't it have made sense for the government to enlarge the ability of CSIS to obtain that kind of information?

---

298 Testimony of Bill Turner, vol. 66, October 25, 2007, p. 8283.

299 See Section 1.3 (Pre-bombing), Parmar Warrant, for full details.

300 Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3574.

301 Exhibit P-101 CAA1086, p. 5.

302 Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3575.

303 Testimony of Raymond Kobzey, vol. 32, May 23, 2007, p. 3727 and Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3818.

304 Testimony of Jack Hooper, vol. 50, September 21, 2007, p. 6207.



**MR. KOBZEY:** From an investigator's point of view, yes, sir, and I think that was part of the initial transition and some of those issues had yet to be resolved and arranged.<sup>305</sup>

The sudden loss of these basic investigative tools was part of the post-transition reaction to "de-police" the new Service. It is clear that the basic biodata available on CPIC would have been of use to CSIS during their pre-bombing investigation. The procedure put in place after the transition was cumbersome, requiring CSIS personnel to transmit CPIC requests through the RCMP. This procedure forced CSIS to wait for RCMP responses to their requests and exposed their investigations to the RCMP. This inevitably affected the breadth and timeliness of CSIS intelligence collection, and began a long-standing dispute between the agencies, which was not resolved until 1990, when CSIS gained full access to CPIC.<sup>306</sup> These limits on CSIS investigations lacked rational explanations.

### Conclusion

The period after the creation of CSIS was one of confusion, inefficiency and adjustment. Operations were held up by the need to learn about the new mandate and the resulting cumbersome processes that were considered necessary to meet the recommendations of the McDonald Commission.

The responsibility for the failures of CSIS during the period does not rest with the individual members of that organization. It was clear from the evidence that, collectively, they tried to perform their duties as they understood them, under the umbrella of inadequate legislation and resources.

The early difficulty with CSIS rests solely with the government of the day who, in a rush to adopt the McDonald Commission recommendations, produced woefully inadequate implementation legislation. The legislation lacked clarity and direction and did not address resource issues; this resulted in CSIS commencing operations lacking office space, technology and clear legislative direction. The members should be commended for attempting to fulfil their duties in what were, initially, impossible circumstances.

Bill Turner refrained from calling the situation "chaotic," but stated that CSIS personnel were carrying on functions and duties they knew – but without policy.<sup>307</sup> Chris Scowen said: "...we were all very much new boys trying to work out these new regulations in which we operated."<sup>308</sup>

All CSIS personnel had to familiarize themselves with a new, more legalistic mandate and examine how this mandate would affect their daily operations. Resources were known to be inadequate. New people were being brought into CSIS, while existing personnel were considering taking the "bridge back" option

<sup>305</sup> Testimony of Raymond Kobzey, vol. 32, May 23, 2007, pp. 3727-3728.

<sup>306</sup> Testimony of Jean-Paul Brodeur, vol. 18, March 7, 2007, p. 1722.

<sup>307</sup> Testimony of Bill Turner, vol. 66, October 25, 2007, p. 8279.

<sup>308</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6138.

that would allow them to return to the ranks of the RCMP. CSIS personnel were dealing with a new mandate, new policies, new methods and a new chain of command, with minimal guidance from the top ranks.<sup>309</sup>

CSIS's investigations and its ability to cooperate with the RCMP suffered due to the strains caused by transition. At times, it seemed that CSIS was holding its collective breath while transition issues settled out, hoping that tragedy would not strike during this period of confusion. Unfortunately, tragedy did strike.

### 3.3.2 The Changing Threat Paradigm

The diversion of CSIS resources and personnel to deal with transition issues created a situation in which it was especially critical that a resource-starved CSIS properly focus its investigations on the most relevant threats to national security. The intelligence priorities of the RCMP Security Service (SS) in the years prior to the creation of CSIS are outlined in the 1982-1983 Annual Report on the Activities of the RCMP Security Service, issued on May 13, 1983.<sup>310</sup> The report recognized the strain on operations caused by the transition process.

Efforts to create the civilian Canadian Security Intelligence Service [have] progressed in tandem with normal operations. The substantial administrative, research and consultative tasks required of the RCMP Security Service were met through selective reduction of operational coverage on lower priority targets and postponement of less urgent administrative projects.<sup>311</sup>

This Commission investigated whether CSIS adequately adjusted its intelligence priorities during the period preceding the Air India and Narita bombings. The investigation included analysis of whether CSIS adequately recognized the change in the threat paradigm from counter-intelligence (CI) to counterterrorism (CT) and assigned appropriate tasking priority to the emerging threat of Sikh extremism in particular. Or, expressed another way, did CSIS effectively plan for the upcoming war or were they focused on fighting battles of the past?

#### ***The Paradigm Shift from the Cold War to Terrorism***

In the years before separation, Canadian intelligence operated almost exclusively in a Cold War atmosphere. The 1982-1983 RCMP SS Annual Report listed the distribution of effort as 55% counter-intelligence (CI), 17% counter-subversion (CS) and 15% counterterrorism (CT).<sup>312</sup> Within the RCMP SS, CT only had the

<sup>309</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3574-3576.

<sup>310</sup> Exhibit P-101 CAF0017.

<sup>311</sup> Exhibit P-101 CAF0017, p. 4.

<sup>312</sup> Exhibit P-101 CAF0017.

status of a unit within the counter-subversion branch. In the meantime, in the early 1980s, terrorism around the world, and in particular Sikh extremism, was on the rise.<sup>313</sup>

In the early 1980s, the RCMP SS began to bolster its counterterrorism investigations, due to two major terrorist incidents that occurred in Canada. In April 1982, a Turkish commercial counsellor was shot and wounded. Four months later, a Turkish military attaché was shot and killed. Armenian terrorist groups claimed responsibility for both attacks. These terrorists issued bomb threats to various Canadian government departments and attempted to bomb Air Canada premises in Los Angeles. It was clear that Canada was no longer immune to lethal terrorist violence, and the RCMP SS adjusted its priorities to address the Armenian terrorist threat.

The 1982-1983 RCMP SS Annual Report indicated the Service's recognition of the growing threat of terrorism. Counterterrorism investigations were allotted the greatest increase in resources, up 7% from the previous year.<sup>314</sup> However, these resources were mainly assigned to the Armenian CT investigation. As if to confirm this ranking of priorities, in March 1985, the Turkish embassy in Ottawa was stormed by Armenian nationalists. The Annual Report described several other CT investigations, but concluded that these concerns were not considered imminent or high priority. The issue of Sikh extremism did not even merit mention.<sup>315</sup>

Other CT investigations, including Sikh extremism, continued to suffer from a lack of resources due to the focus on counter-intelligence targets and on Armenian terrorist targets. Upon the creation of CSIS in July 1984, CT became a major division, equal to both CI and CS. However, the CT staffing complement did not change. At the time of separation, Geoffrey O'Brian estimated that the operational resources of CSIS were approximately 75% for CI and 25% for all other divisions.<sup>316</sup> Daryl Zelmer testified that counter-intelligence remained the main priority for CSIS in the year leading-up to the bombing. While counterterrorism was a "growing industry," it still was allotted fewer personnel and investigative resources than counter-intelligence,<sup>317</sup> and the resources assigned to CT investigations remained within the Armenian terrorism unit. The following is an excerpt from the testimony of Russell Upton, the Chief of the Europe and Far East Section at CSIS HQ:

**THE COMMISSIONER:** (Off mic) ...other sections were deprived of resources to the same extent you were?

---

<sup>313</sup> International terrorist incidents in the early 1980s included the series of suicide attacks directly against American diplomatic facilities in Beirut, Lebanon and against the US marine barracks at Beirut International Airport in 1983 and, on the same day, against the French paratroops headquarters also in Beirut and against the Israeli Defence Forces command post in Tyre, Lebanon, as well as the 1984 suicide bombings of the US embassy and then the attempt to assassinate the Emir of Kuwait in December, 1984: Testimony of Bruce Hoffman, vol. 19, March 9, 2007, pp. 1786-1787.

<sup>314</sup> Exhibit P-101 CAF0017.

<sup>315</sup> Exhibit P-101 CAF0017.

<sup>316</sup> Testimony of Geoffrey O'Brian, vol. 17, March 6, 2007, p. 1553.

<sup>317</sup> Testimony of Daryl Zelmer, vol. 23, May 4, 2007, p. 2320.

**MR. UPTON:** Not to my knowledge.

**THE COMMISSIONER:** One had more than the other? I mean, you don't know whether [others] had more resources than needed, or...

**MR. UPTON:** I was very well knowledgeable of the Section that was set [up] to handle the Armenian situation after the terrorist act. And it was given a top priority, continued top priority, and it in effect at times hindered me from getting my resources. And it was fully staffed; it had research resource people and everything. And after the bombing, I must say that the CSIS – director transferred some of those resources over to my area and that helped to relieve a lot of pressure. But for me, that was too late. I was already pretty stressed out and I resigned in May of '86.<sup>318</sup>

### ***Lack of Recognition of Sikh Extremism in Early 1980s***

Was the lack of recognition of the Sikh extremist threat reasonable? The early 1980s witnessed the rise of Sikh extremist violence.<sup>319</sup> In Canada, demonstrations against the Indian government grew in size and intensity, Indian diplomatic personnel and personnel were faced with threats, and rumours surfaced of military training within a growing Sikh extremist movement.<sup>320</sup>

During this time, the investigation into Sikh extremism was given relatively low priority. RCMP SS investigators appeared concerned that the unrest in the Punjab could spill over into the Sikh population in Canada, but were given few resources to pursue the concern.<sup>321</sup>

The general belief throughout this period was that the problem of Sikh extremism was foreign, and, at the time, Sikhs in Canada were generally peaceful, with any violence limited to interfactional or religious disputes amongst Sikh groups.<sup>322</sup> Information about the Khalistani movement was obtained primarily from the Government of India itself, as well as from sources developed by other police forces,<sup>323</sup> the media, and a few community contacts. In response to concerns expressed by the Indian Government about Parmar in 1982, Security Service investigators undertook physical surveillance to locate Parmar for an interview, but failed to actually interview him. They did, however, undertake an interview with Surjan Singh Gill, who was a known affiliate of Parmar and the self-

<sup>318</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3604.

<sup>319</sup> See Section 2.2 (Pre-bombing), Failure to Appreciate the Nature and Seriousness of the Threat.

<sup>320</sup> See Section 1.12 (Pre-bombing), A "Crescendo" of Threats.

<sup>321</sup> For a full description of CSIS pre-bombing investigation, see Section 3.2 (Pre-bombing), The CSIS Investigations into Sikh Extremism.

<sup>322</sup> Exhibit P-101 CAB0049.

<sup>323</sup> CSIS relied on the Vancouver Police Department, Indo-Canadian Liaison Team for community intelligence. The VPD dialogued with several members of the Sikh community: See Exhibit P-101 CAB0048.

proclaimed Khalistani “Consular General” in Vancouver.<sup>324</sup> The investigation throughout the pre-bombing period was more reactive than proactive, with CSIS’s efforts focused on substantiating threat warnings received from various sources and on obtaining information about anticipated demonstrations.

### **Focus on Sikh Extremism Increases in 1984**

In early 1984, Sikh extremism did not have its own intelligence requirement (IR), a ranking that prioritized the work and resources of the RCMP SS and, later, CSIS.<sup>325</sup> However, events over the following year revealed the obvious growth of Sikh extremism in Canada, compelling CSIS to begin to bolster its investigation into the threat.<sup>326</sup> The Sikh extremism investigation<sup>327</sup> was given increased priority with the opening of the “Sikh extremism” file on April 7, 1984, with Operational Priorities Review Committee (OPRC) level 2 coverage approved.<sup>328</sup> The higher prioritization was triggered by the increasingly tense situation in the Punjab, as violence escalated and the Indian army surrounded the Golden Temple. In March 1984, the Security Service received information suggesting that this “foreign issue” was about to spill over into Canada in a deadly manner. A source advised that a group of 18 Sikhs from India had sworn a pledge to carry out attacks or to kill moderate Sikh leaders, prominent Hindu leaders and Indian diplomatic personnel in Canada. In fact, the source alleged that some of them had already arrived in Vancouver.<sup>329</sup> Once the Service had opened the Sikh extremist file, all regions were required to provide community assessments of the Indian situation in their areas. The instructions from HQ recognized the inherent link between the events in the Punjab and the possible reaction within the Canadian Sikh community. It warned that if the Indian government was unable to restore calm in the Punjab area, tensions could flare within Canada’s Sikh community.<sup>330</sup>

This happened when the Indian army stormed the Golden Temple on June 6, 1984. The event triggered mass demonstrations across Canada.<sup>331</sup> While the protests were generally non-violent, Security Service threat assessments noted that they were emotionally charged events, in a Sikh community united in grief like never before.<sup>332</sup> The SS believed that the prospect for confrontations and violence in Canada was a certainty. While noting that their recently initiated investigation into Sikh extremism in Canada had not yet yielded any firm conclusions, they did conclude that the threat to Indian missions and personnel was at its highest.<sup>333</sup>

---

324 Exhibit P-101 CAA0018, CAB0031.

325 Testimony of Daryl Zelmer, vol. 23, May 4, 2007, p. 2321.

326 A detailed description of CSIS pre-bombing investigation into Sikh extremism is provided in Section 3.2 (Pre-bombing), The CSIS Investigations into Sikh Extremism.

327 For detailed information about CSIS pre-bombing investigations, see Section 3.2 (Pre-bombing), The CSIS Investigations into Sikh Extremism.

328 Exhibit P-101 CAB0054, CAF0072b.

329 Exhibit P-101 CAB0048.

330 Exhibit P-101 CAB0054.

331 Exhibit P-101 CAB0062.

332 Exhibit P-101 CAB0062, CAB0063.

333 Exhibit P-101 CAB0062.

### ***Investigative Authorization on Sikh Extremism Increased to Highest Level***

In light of the reaction of the Sikh community in Canada to the Golden Temple storming, the Sikh extremism file was given the highest OPRC level 4 investigative authorization, officially approved on June 27, 1984, just three months after the file was opened.<sup>334</sup> This authorization signified the Service's recognition, a year before the Air India and Narita bombings, that the Sikh extremism investigation needed to employ the most intrusive investigative methods to address this serious threat. By the fall of 1984, a "Sikh Desk" had been created at HQ.<sup>335</sup> Over the following year, CSIS identified specific targets within the Sikh extremist community and obtained specific OPRC level 4 authorizations against Parmar (on September 17, 1984),<sup>336</sup> the Babbar Khalsa (on January 30, 1985)<sup>337</sup> and the International Sikh Youth Federation (on May 5, 1985).<sup>338</sup> On May 28, 1985, Mel Deschenes, the DG CT, designated the Sikh extremism file as a top priority investigation with its own IR until at least mid-June.<sup>339</sup> This designation was based on CSIS's concern about the potential for serious incidents in the period leading up to the anniversary of the Golden Temple storming (June 6, 1985) and during the US visit of Prime Minister Rajiv Gandhi, from June 11 to 16, 1985. Investigators were ordered to mobilize and process all available sources on a priority basis, and to submit daily situation reports to HQ.<sup>340</sup> CSIS personnel involved in the Sikh extremism investigation during this period expressed their conviction that prospective violence by Sikh extremists was considered to be a certainty. Kobzey, an Intelligence Officer at BC Region, considered the Sikh extremism file to be urgent, based on the violent rhetoric of Parmar and the religious fervor tied to the threats.<sup>341</sup> Russell Upton testified that the issue of Sikh extremism was clearly evident in 1984; that "...we were getting red flags all over,"<sup>342</sup> and that it was only a matter of time before the terrorist element in the Sikh community was going to "hit us good". Upton agreed with the notion that the bombings were "...a terrorist action that was waiting to happen."<sup>343</sup>

From these designations and comments, it would appear that CSIS was aware of, and assigning appropriate priority to, the investigation of Sikh extremism. However, the Commission's review of the evidence shows that from June 1984, when the Sikh extremism investigation was given OPRC level 4 authorization, to June 1985, when the bombings occurred, CSIS failed to adequately generate useful intelligence on the activities of Sikh extremists in British Columbia. Although the Sikh extremism file had been nominally designated top priority throughout the year leading up to the bombing, investigators were not allotted adequate resources or personnel to effectively carry out the investigation. It

<sup>334</sup> Exhibit P-101 CAF0102, p. 1; Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3520-3521.

<sup>335</sup> Testimony of Daryl Zelmer, vol. 23, May 4, 2007, p. 2321.

<sup>336</sup> Exhibit P-101 CAB0139.

<sup>337</sup> Exhibit P-101 CAF0111.

<sup>338</sup> Exhibit P-101 CAB0117.

<sup>339</sup> Exhibit P-101 CAF0124(i).

<sup>340</sup> Exhibit P-101 CAB0256.

<sup>341</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3753; Exhibit P-101 CAB0144, pp. 3-4.

<sup>342</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3613.

<sup>343</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3609, 3613.

appeared to be a situation in which the investigators on the ground understood the threat, but could not obtain support or guidance from an upper management that was too focused on transition issues and traditional counter-intelligence priorities.

Archie Barr noted that the intelligence landscape was changing quickly at the time.

Although CSIS was newly formed, we brought a well-functioning counterterrorism unit to CSIS from the RCMP, and the need for it grew much larger than we had originally expected, as the threat of terrorism began to spread in the 1980s. Much of the CSIS work in the early days involved counter-intelligence as the Cold War continued, but the intelligence landscape was changing quickly... The shift from counter-intelligence to counterterrorism could have and should have been faster.<sup>344</sup>

Ronald ("Ron") Atkey, the first chairman of the Security Intelligence Review Committee, which had oversight over CSIS, described the three competing intelligence priorities within CSIS prior to the Air India and Narita bombings: counter-intelligence, counter-subversion and counterterrorism. CSIS had begun to disband the counter-subversion branch, in light of its new mandate, which freed up some resources for counterterrorism priorities.

**MR. ATKEY:** But I have to say that the events of June 23<sup>rd</sup>, 1985, did shift the whole mentality of this thing rather quickly... [a]nd the counterterrorism became the focus and resources were directed towards that.

**MR. BOXALL:** I guess, the art to it is attempting to not wait until the event occurs to shift the resources, but for someone to be in a position to predict that?

**MR. ATKEY:** That's correct.<sup>345</sup>

After the bombing, resources were rapidly shifted to the investigation into Sikh extremism. This adjustment in priorities was long overdue and, tragically, too late to assist CSIS investigators in preventing the Air India and Narita bombings.

### ***Failure to Adjust Priorities to the Investigation of Sikh Extremism***

This recognition of the seriousness of the Sikh extremist threat came too late, especially in light of the significant events that were occurring in the year before the bombing. Even the prioritization, long overdue, of the Sikh extremism

<sup>344</sup> Exhibit P-437: Statement of Archie Barr, pp. 5, 7.

<sup>345</sup> Testimony of Ronald Atkey, vol. 49, September 20, 2007, pp. 6007-6010.



investigation that occurred in May 1985 was to be implemented temporarily, “until at least mid 1985 06.”<sup>346</sup> The prioritization appeared to be more a cautious reaction to the highly politicized visit of Rajiv Gandhi to the US, rather than a result of a true understanding of the overall seriousness of the Sikh extremist threat.

This belief that the threat was temporary was shared by the RCMP, who exerted pressure on CSIS to reduce the threat level after Gandhi’s departure. In a June 11<sup>th</sup> TA request, the RCMP informed CSIS that the last CSIS TA had resulted in a deployment of considerable RCMP resources to protect Indian interests, and, should the Gandhi visit take place without serious incident, they “...assumed the threat level ... would diminish.” As such, the RCMP requested an updated TA on June 17<sup>th</sup>, the day of Gandhi’s departure.<sup>347</sup> Despite this pressure, CSIS investigators across the nation cautioned against assuming the problem had passed.<sup>348</sup> The June 17, 1985 TA issued by CSIS assessed the threat as being “... only slightly less serious” and warned that “...extremists/terrorists are no less determined to realize their ambitions and to think that they have abandoned their cause would be somewhat naïve on our part.”<sup>349</sup>

Despite CSIS’s warning that the threat continued, it allowed efforts made to bolster the Sikh extremism investigation in early June to lapse after the departure of the Indian Prime Minister from North America. CSIS HQ ended the requirement for daily situation reports from the regions, several key personnel in both HQ and BC Region were allowed to take leave, and physical surveillance coverage on Parmar was, regrettably, pulled on the day before the bombing.<sup>350</sup> While it was likely that the CSIS personnel involved with investigation were weary after the intense period during the Gandhi visit, this was no excuse for letting the investigative resources lapse without ensuring that suitable replacements were available to maintain CSIS’s ability to assess what was admitted to be a continuing high threat. It is difficult to conceive how CSIS could have warned that the threat continued to be high, while simultaneously reducing its investigative capability.

This lack of appreciation of the breadth and severity of the threat of Sikh extremism on the part of CSIS HQ translated into a failure to prioritize the Sikh

<sup>346</sup> Exhibit P-101 CAF0124, p. 1.

<sup>347</sup> Exhibit P-101 CAB0275.

<sup>348</sup> Exhibit P-101 CAA0219 p. 2 (BC Region wrote, “...we still consider the threat potential from the Sikh community to be high.... It would appear that time is of no consequence to the Sikh extremist element in reaching their objectives therefore we can expect the overall problem to remain constant for some time to come”), CAB0312 (Windsor Region wrote, “...this office feels the threat posed by Sikh extremists against Indian Missions, personnel and interests in this country will remain high ... the BK will simply ride out the RCMP campaign, re-group after the force loses interest and attempt to strike at some less high profile target, once the heat is off”), CAB0316 (Edmonton District wrote, “...it would seem small groups or individuals within Edmonton’s Sikh community have the potential to either support or undertake violence against Indian missions, personnel or interests in Canada or on an international scale in the future long term”) and CAB0315 (Manitoba Region wrote, “...we must not [be] complacent and assume that the Sikh problem has passed. Writer feels that Indian missions and personnel will continue to be a target of the more militant Sikh extremist factions present in this country”).

<sup>349</sup> Exhibit P-101 CAA0220.

<sup>350</sup> See Section 3.3.3 (Pre-bombing), Failure to Allocate Resources.

extremism investigation, and thus into a failure to devote adequate resources and personnel to carry out the investigation effectively. The evidence at the inquiry clearly shows that the BC investigators, Kobzey and David Ayre, had an understanding that there was a serious threat posed by Sikh extremists.<sup>351</sup> What is equally clear is that this view was underappreciated at HQ. In a centralized organization it is difficult for priorities to be adjusted, unless HQ understands and appreciates the need for the adjustment. In the case of the threat posed by Sikh extremism, HQ did not appreciate the risk in a timely manner and, thus, provided inadequate support to the investigators on the ground.

## Conclusion

The Commission's review shows that CSIS was slow to recognize the changing threat paradigm from counter-intelligence to counterterrorism. While CSIS was beginning to bolster its counterterrorism investigations in reaction to two attacks by Armenian terrorists in Ottawa, it failed to adequately recognize other emerging terrorist threats in Canada, such as Sikh extremists. Sikh extremism investigators found themselves in a losing competition for resources with the higher priority counter-intelligence and Armenian terrorist target investigations. In effect, CSIS's targeting priorities were more reactive than proactive: CSIS was busy fighting the threats of the past rather than anticipating emerging threats.

### 3.3.3 Failure to Allocate Resources

#### *The Struggle for Resources*

The failure of CSIS senior management to recognize the threat of Sikh extremism led to an inevitable struggle for resources by the analysts and investigators involved in this investigation. In the year preceding the bombing, CSIS nominally assigned the Sikh extremism investigation increasing levels of priority, but failed to adjust the resources accordingly to allow investigators to actually meet these priorities. Ironically, when Mel Deschenes assigned the Sikh extremism investigation top priority on May 28, 1985, in anticipation of the Golden Temple storming anniversary and the US visit of Rajiv Gandhi, he noted "...any extra resources and attention you can afford this area during the coming weeks shall be appreciated."<sup>352</sup> In fact, this top prioritization did not translate into increased personnel to handle the necessarily increased investigative load. A week later, when Russell Upton tasked the regions to provide daily situation reports, there was similarly no increase in resources to meet the increased requirement.<sup>353</sup> Hard-working investigators were simply asked to work harder.

A number of CSIS intelligence failures with respect to the Sikh extremism investigation in 1984-1985 can be traced, at least in part, to the lack of resources, as noted by Professor Wesley Wark:

---

<sup>351</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3753-3755, 3764-3765; Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3790.

<sup>352</sup> Exhibit P-101 CAF0124(i).

<sup>353</sup> Exhibit P-101 CAB0256.

[I] see two clear kinds of intelligence failure at work in Air India in 1985.... One has to do with intelligence collection, part of the intelligence cycle. Now, it is the case that government agencies were aware of the threat from Sikh terrorism and were targeting that threat, and they were engaged in intelligence collection against it, especially in terms of CSIS efforts. But what we see in the detailed record of the pre-bombing CSIS information collection effort, was an inability to take full advantage, I would say, of that targeting, an inability to sustain physical surveillance on key targets, in particular Mr. Parmar, and the inability to make full use of the wire tap information, the electronic surveillance, again, conducted against Mr. Parmar.... [W]e had the right intelligence instincts at work, but we didn't have a system that could fully deliver on them. Why is that? I think it's very hard for me to reach an assessment about that. There are some things that leap out at one as likely answers, in terms of lack of resources in particular, and lack of capacities to translate intelligence into usable information. But I do see an intelligence failure at work, here.<sup>354</sup>

A review of the Inquiry evidence shows that CSIS's investigation into Sikh extremism was compromised by the failure to move swiftly to engage investigative techniques that might have produced actionable intelligence information, or to devote sufficient personnel to support the investigative techniques that were in fact employed. These deficiencies, along with questionable strategic decisions, affected CSIS's ability at all stages of the intelligence cycle. The units responsible for the collection, analysis and dissemination of relevant and timely intelligence all suffered from a lack of resources and personnel. The lack of intelligence that resulted led to a systemic failure, affecting senior management's ability to appreciate the gravity of the Sikh extremist threat and to adjust tasking priorities to correct the underlying resource and personnel deficiencies.<sup>355</sup>

This section outlines the deficiencies in investigative resources and personnel for the CSIS investigation into Sikh extremism, and the effect of these deficiencies on CSIS's ability to collect, analyze and disseminate intelligence.

### ***Effect on Intelligence Collection***

CSIS's collection of intelligence provides the foundation for all other stages of the intelligence cycle. Effective collection efforts provide context which allows analysts to make informed assessments from which the government can develop appropriate responses and adjust its priorities to meet the changing threat climate.

---

<sup>354</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, pp. 1495-1496.

<sup>355</sup> For a detailed description of the senior management's failure to recognize the changing threat paradigm and sufficiently prioritize the Sikh extremism investigation, see Section 3.3.2 (Pre-bombing), The Changing Threat Paradigm.

With little direction and support from a CSIS senior management that was focused on transition issues and other higher-priority investigations, the furtherance of the Sikh extremism investigation depended on the personal initiative of the on-the-ground investigators. In the aftermath of the Golden Temple storming and the return of Parmar from a German prison in the summer of 1984, CSIS investigators in BC Region and analysts at HQ initiated efforts to gain approval for more investigative resources against Parmar, but were met with constant challenges. Human sources proved difficult to cultivate in a tight-knit, secretive group, and the Sikh community was often unwilling to speak due to threats of intimidation from extremists. The Parmar intercept application was delayed at HQ for five months. There was a lack of security-cleared translators available to process the Parmar tapes, once recorded. The BC Region Physical Surveillance Unit (PSU) coverage was focused on other targets considered to be higher-priority, and covered Parmar or other Sikh extremists only when resources were available. Even staffing levels were inadequate, as few investigators were involved in the Sikh extremist investigation, and those involved were overworked.

### ***Human Sources***

The greatest problem in CSIS's investigation into Sikh extremism was its inability to recruit trustworthy and reliable human sources.<sup>356</sup> Chris Scowen testified that the most important intelligence resource any intelligence service can have is a human source:

You can have all the technical sources you want, they would supply enormous amounts of information but the human source is the only kind of source that can be directed, can use their own intelligence, can use their own imagination in the furtherance of an operation.<sup>357</sup>

Kobzey testified about his efforts to recruit human sources within the Sikh community in British Columbia. He noted that, in 1982, the Sikh extremism investigation was assigned a low level of investigative authority, which was sufficient for him to develop relationships with Sikh community members who could inform CSIS about issues of concerns to them. Kobzey developed these casual relationships with the hope that he would find a person who could become a CSIS source at a later date, when the level of investigative authority was increased. In particular, he was looking for someone who had access to the plans of Sikh extremists like Parmar, Bagri, Gill and their associates.

However, Kobzey testified that this task proved difficult. Members of the Sikh community were very reluctant to be seen to be working with the authorities, for fear of retribution, beatings, and violence, either to themselves or to family members in Canada and overseas. The Sikh extremists themselves were a

---

<sup>356</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3603.

<sup>357</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6155.

close-knit, family-like unit that did not trust anyone outside of their immediate circle.<sup>358</sup> Kobzey considered the introduction of a human source into such a group to be virtually impossible.<sup>359</sup> Ultimately, no human sources had been recruited, prior to the bombing, to support the BC investigation of Parmar and his associates.<sup>360</sup>

CSIS, as a newly-formed and highly secretive agency with little public reputation, lacked vital tools to gain trust in face of the distrust of government present in the Sikh community.

A human source could have provided critical context within which to understand the movements and intercepted conversations of Parmar, who often acted and conversed in a security-conscious manner.<sup>361</sup> Instead, CSIS investigators were forced to turn to inferior investigative methods, including technical intercepts and physical surveillance. Without the insight of a human source, investigators could only make their best guess about the actions and conversations of a group of Sikh extremists with which they had little cultural and operational familiarity.

#### ***Technical Sources: Parmar Warrant***

In light of the difficulty in recruiting human sources, CSIS had to rely on technical sources to obtain insight into the dealings of Parmar and his tight-knit group.<sup>362</sup> Kobzey recognized the importance of gaining comprehensive insight into this group immediately after Operation Bluestar in June 1984, and Parmar's return to Canada in July 1984.

I felt that the action against Bluestar would be so inflammatory that we had to be in a position to deal with this by means of a warrant soonest, to start getting information which would enable us to gather clear insight into this individual, his associates, his contacts worldwide, people who he was dealing with ....<sup>363</sup>

Kobzey drafted an urgent warrant application during August 1984 to intercept the communications of Parmar, and submitted it to CSIS HQ in September 1984. The application warned that "...in view of our limited source coverage, we are in a very poor position to provide timely intelligence with respect to any planned acts of violence."<sup>364</sup> In spite of this warning, the approval and subsequent processing of the Parmar intercept were handled in a non-urgent manner, rife

<sup>358</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3820-3821.

<sup>359</sup> Exhibit P-101 CAB0144, p. 7.

<sup>360</sup> Exhibit P-101 CAB0902: 1992 SIRC Report, p. 40.

<sup>361</sup> Exhibit P-101 CAD0154, p. 10. See also Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3603.

<sup>362</sup> The circumstances surrounding the Parmar warrant are described in detail in Section 1.3 (Pre-bombing), Parmar Warrant.

<sup>363</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3754-3755.

<sup>364</sup> Exhibit P-101 CAB0144, p. 7.

with significant delays, and causing potential losses of critical, contextual and, possibly incriminating, information.

It is important to put this issue in context. There is no certainty that information would have been obtained that would have prevented the terrorist attacks. However, in assessing the steps that were taken during the investigation, it is surprising that the warrant took five months to obtain, considering CSIS's urgent need for insight into the Sikh extremist movement in Canada, and CSIS's view that Parmar was the leader of that movement and had been employing inflammatory rhetoric in public. Kobzey admitted that the unexpected delay hampered his attempts to gain in-depth knowledge about Parmar.<sup>365</sup>

In comparison, shortly after the bombing, with the creation of the CSIS task force in BC Region and a three-person warrant drafting section, CSIS HQ was able to obtain approval by the Federal Court for several additional warrants in a much shorter period of time.<sup>366</sup> This illustrates that CSIS HQ had the ability to process warrants in an expeditious manner once they were considered sufficiently urgent.

The lengthy Parmar warrant process prior to the bombing meant that CSIS investigators lost potentially valuable information not only in relation to Parmar but also to other Sikh extremists.<sup>367</sup> The failure to obtain the Parmar warrant in a timely manner resulted in an inability to apply for additional warrants for other Sikh extremist targets prior to the bombing. This meant that there were no warrants for Ajaib Singh Bagri and Surjan Singh Gill, even though they were known to CSIS and were considered potentially as dangerous as Parmar.

### ***Punjabi Translators***

At the time that CSIS officials in BC Region had determined that they needed to intercept Parmar's communications, it was apparent that there was another problem: the lack of qualified and security-cleared Punjabi translators. Despite knowledge of that deficiency, little, if anything, was done to remedy the problem over the five months that it took to process the warrant application. Even after the warrant was granted, and Parmar's communications were being intercepted, the issue of an acute lack of translators remained unresolved. By way of illustration, two days before the Air India bombing, approximately 100 audio surveillance tapes of Parmar remained untranslated.<sup>368</sup>

The responsibility for ensuring that there were adequate resources for the translation and transcription of wiretaps fell to Jacques Jodoin, the Director General, Communications Intelligence and Warrants (CI&W) at CSIS HQ.<sup>369</sup> BC

---

<sup>365</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3822.

<sup>366</sup> Testimony of John Stevenson, vol. 62, October 16, 2007, p. 7652.

<sup>367</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3775-3777.

<sup>368</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, p. 1510.

<sup>369</sup> Testimony of Jacques Jodoin, vol. 23, May 4, 2007, p. 2278.



Region began searching for a Punjabi translator before the Parmar warrant was installed on March 25, 1985, but was unsuccessful. On May 16, 1985, it sent out an urgent request to all regions for recruitment of Punjabi translators.<sup>370</sup> Despite this nationwide search, CSIS continued to have difficulty in hiring a security-cleared Punjabi translator. Jodoin arranged for the Parmar tapes to be translated through a drawn-out and inefficient process. Tapes were sent to Ottawa to be translated and the translation would then be sent back to BC Region.

This process not only resulted in extensive delays, but also restricted the ability of BC Region investigators to interact daily with the translator. This made it difficult to coordinate investigative efforts with what the translators were uncovering.

One reason offered for the extreme difficulty in recruiting translators was the requirement that they be Top Secret cleared. During the hearings, Jodoin testified that for this clearance one had to have been in the country for at least 20 years. In his view, there were few Punjabi-speaking persons who could meet this requirement in 1985. Additionally, members of the community were unwilling to cooperate because they did not want CSIS investigators asking questions within their own community.<sup>371</sup>

### ***Physical Surveillance Units***

BC Region investigators faced challenges in obtaining PSU coverage for Sikh extremist targets. PSU resources in BC Region were scarce, with units available to cover one target for up to 16 hours any day of the week.<sup>372</sup> All BC Region investigations competed fiercely for coverage.<sup>373</sup> With little new information collected through other investigative means, BC Region Sikh extremism investigators rarely had fresh justification for the commitment of PSU coverage, and often found their investigations second in priority to those of their counter-intelligence (CI) colleagues.<sup>374</sup> Ultimately, surveillance on Sikh extremist targets was intermittent at best.

Kobzey submitted a request for PSU coverage on Parmar on April 4, 1985,<sup>375</sup> at a time when counterterrorism (CT) targets were given low priority in comparison to ongoing CI targets.<sup>376</sup> When coverage was denied, Kobzey would occasionally undertake surveillance on his own, despite not having training. This diverted his efforts away from other important investigative steps more suitable to the role for which he was trained.

Even the critical Duncan Blast surveillance was obtained by a stroke of luck. At the time, PSU coverage on Parmar was granted intermittently and on an ad hoc basis. With the anniversary of the Golden Temple storming and the US

---

<sup>370</sup> Exhibit P-101 CAB0234, p. 1.

<sup>371</sup> Testimony of Jacques Jodoin, vol. 23, May 4, 2007, pp. 2278-2280.

<sup>372</sup> Exhibit P-101 CAD0131, p. 8.

<sup>373</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3838.

<sup>374</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3773-3774.

<sup>375</sup> See surveillance request by Kobzey and Ayre dated April 4, 1985: Exhibit P-101 CAB0209.

<sup>376</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3794-3795.



visit of Rajiv Gandhi approaching, Kobzey took the initiative to make a personal request, insisting coverage was necessary in light of these important events. His request was met with resistance at senior levels, but ultimately PSU coverage was provided for a few days in early June including the day of the Duncan Blast incident.<sup>377</sup>

The events of that day resulted in continued uninterrupted mobile surveillance of Parmar until June 17, 1985. This was an unprecedented amount of coverage for a CT target at the time. It is ironic that intelligence obtained by the PSU itself enabled this coverage. One can only imagine what information CSIS would have obtained had it had timely information from human or technical sources that could have justified even further coverage. Unfortunately, PSU coverage on Parmar was pulled days before the attack, leaving the whereabouts of Parmar and his associates on the day the bombs were planted uncertain to this day. Kobzey was away on vacation at the time and unable to advocate for the continuance of PSU coverage.

The Commission's evidence shows that the quality of PSU coverage provided suffered due to the insufficient resourcing of PSU teams. Inexplicably, members of the PSU mobile surveillance team following Parmar, who witnessed the Duncan Blast, were not provided with cameras.<sup>378</sup> The lack of photos taken on that critical day has contributed to the inability to identify the third person who attended with Parmar and Reyat, known only as Mr. X.<sup>379</sup> If they had had a camera, the PSU might have determined his identity long ago.

### ***BC Region Investigators***

Even if CSIS had been able to obtain more human and technical sources in support of its investigation into Sikh extremism, it did not have the human resources available to efficiently and effectively process the information that they could have provided. While BC Region was generally well staffed overall, with 165 employees including 40 intelligence officers (IOs), there was little effort to adjust staffing priorities to meet the emerging threat posed by Sikh extremists.<sup>380</sup>

Despite Sikh extremism being the number one CT priority for CSIS and despite the fact that the hotbed of Sikh extremism in Canada was in Vancouver, there was a clear shortfall in personnel dedicated to monitoring this threat. In fact, prior to the bombing, only two investigators were working directly on the Sikh extremism issue – Kobzey and Ayre. They reported to their unit head, Jim Francis, who in turn reported to the Chief of CT, Robert Smith.

Kobzey and Ayre spent much of their limited time confronting serious challenges to obtaining resources to support their investigations. They seemed to be in

<sup>377</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3793-3796.

<sup>378</sup> Testimony of Lynne Jarrett, vol. 22, May 3, 2007, p. 2208.

<sup>379</sup> A detailed description can be found in Section 1.5 (Pre-bombing), Mr. X.

<sup>380</sup> Testimony of Jack Hooper, vol. 50, September 21, 2007, pp. 6208-6209.

a constant fight for basic investigative resources, which detracted from their ability to carry out their own important investigative duties.

Even with their limited capacity, the BC investigators were able to appreciate the seriousness of the Sikh extremist threat in BC, as shown by their “urgent” warrant application to intercept the communications of Parmar, submitted to CSIS HQ in October 1984.<sup>381</sup> Once again, BC Sikh extremism investigators met with opposition at the higher levels of CSIS, where the warrant process was delayed in light of the “higher priority” issue of dealing with warrant conversions which had been necessitated by the creation of CSIS.<sup>382</sup>

With their time taken up in a constant battle for resources, with little support from senior management at CSIS HQ, and no human sources, it is not surprising that the BC investigators were unable to further their understanding of the key Air India conspirators, despite their appreciation of the seriousness of the threat. The lack of resources at the investigative level impaired every stage of the intelligence cycle: the ability to define informed intelligence priorities, to analyze the threat information available and to properly advise other agencies of the “reality” of the Sikh extremism threat.

Immediately following the bombing, 14 BC Region CSIS investigators were assigned to the Sikh extremism investigation. This much-needed shift of resources was too late.

### ***Effect on Intelligence Analysis***

The HQ Sikh Desk, the analytical centre for all investigations into Sikh extremism across the country, was severely understaffed in the year leading up to the bombing. Although three analyst positions were allotted to the investigation, only one position was filled for most of the year prior to the bombing.

Russell Upton was the Chief of the CT operations dealing with Europe and the Pacific Rim, including the Sikh Desk. He managed an area of operations far larger than simply the Sikh Desk, including the other CT hot spots in Western Europe, Yugoslavia, South America and the Caribbean.<sup>383</sup> The Sikh Desk, itself, was originally the Western Europe and Far East Desk and dealt with other areas of interest as well. Although Upton had the ability to reassign staff within his section, his entire section was operating with insufficient resources. Staffing was at half its intended complement; only seven of 14 allotted positions were filled.<sup>384</sup> This was at a time when there were constantly-increasing intelligence flows, not only in relation to Sikh extremism but also for other areas within his responsibility.<sup>385</sup> This information had to be interpreted, analyzed and integrated into CSIS’s existing understanding of various terrorist groups. As such, Upton had no “extra resources” to divert to the Sikh Desk.

---

<sup>381</sup> See Section 1.3 (Pre-bombing), Parmar Warrant.

<sup>382</sup> See Section 1.3 (Pre-bombing), Parmar Warrant.

<sup>383</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3568-3569.

<sup>384</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3571-3572.

<sup>385</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3601-3602.

The Sikh Desk therefore remained short-staffed. Glen Gartshore was the head of the desk, and Burgoyne filled one of the three allotted Sikh Desk analyst positions at the time of the storming of the Golden Temple, one year prior to the Air India bombing.<sup>386</sup> Burgoyne was a novice analyst with no background or formal training in Sikh extremism issues. A second analyst position was filled by Bill Dexter, who was away on French language training until March 1985. Dan Godbout filled the final position three weeks prior to the Air India and Narita bombings, but his work did not involve Sikh extremism issues.<sup>387</sup> Even if all the analyst positions had been filled with individuals, working full-time and with expertise on Sikh extremist issues, three analysts would have been insufficient to cover what was designated as the number one CT threat by May 1985.

Despite the diligence of Gartshore and Burgoyne on the Sikh Desk, it is clear that they were overworked and under-resourced. The fact that CSIS had nominally allotted three Sikh Desk analyst positions demonstrates a theoretical awareness of the increasing threat of Sikh extremism. Nevertheless, CSIS failed to actually fill all these critical analyst positions and to provide some training or personnel with experience in Sikh extremism issues. Upton testified:

In so far as Sikh extremism was concerned, the lack of resources starved the investigation at times and resulted in a systemic inability to appreciate the threat so as to affect CSIS's priorities and investigative deployments.<sup>388</sup>

Upton said that the Sikh Desk analysts performed "...admirably under the circumstances," in light of the limited analytical resources at their disposal, especially as they were dealing with an extremely tragic and high-profile terrorist matter.<sup>389</sup> Unfortunately, even admirable performance under the circumstances was inadequate to deal with potentially lethal terrorist threats to the security of Canadians.

Personnel at HQ were rapidly transferred to the Sikh extremism investigation after the bombing, to newly-created analyst positions. Much like the post-bombing shift in resources at BC Region, this after-the-fact prioritization at CSIS HQ was too late to assist the overburdened analysts, who had been working to "connect the dots" to prevent the bombing of Air India Flight 182.

### ***Effect on Intelligence Dissemination***

The scarcity of personnel in the HQ Threat Assessment Unit (TAU) limited its ability to add value to CSIS's threat assessments from the regions, or to ensure that the finished product met the requirements of the requesting agency. John Henry was the Head of the TAU, which consisted of two persons who

<sup>386</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3569.

<sup>387</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3570-3571.

<sup>388</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3604-3606.

<sup>389</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3604.

produced 952 time-sensitive threat assessments in the year preceding the Air India bombing.<sup>390</sup> The TAU handled the dissemination of threat assessments for all CSIS investigations, not just the Sikh Desk. As such, the TAU only had the capacity to focus on liaison duties, relying almost entirely on the operational desks for the analysis and assessment of threats.<sup>391</sup>

Once a desk responded with a draft threat assessment, the TAU would review the assessment to ensure "...it conformed with all the rules ... at the time and that it said nothing to infringe upon the duties of other units ...." The TAU could edit the assessment to remove any information not deemed suitable for dissemination outside of CSIS, and was responsible for adding caveats restricting the use of the information contained in the assessment. The TAU might also substitute vocabulary more familiar to the police. The TAU would occasionally challenge the desk on the material "from an outsider's perspective." Any changes or alterations were made in conjunction with the desks. However, most of the time, the TAU would not make any changes to the assessments provided by the desks, basically issuing a verbatim copy to the appropriate agencies.<sup>392</sup>

In effect, the TAU was resourced to act as a threat assessment post office, receiving threat requests and sending back threat assessments, while contributing little analytical input to improve the quality of the product. In the Commission's view, by limiting the TAU to this role, CSIS likely missed an opportunity to take a more client-centred approach to the TA process. The TAU, with no particular expertise in the issues dealt with in CSIS-wide TAs, would not have been expected to contribute to the substantive portions of the TA. However, they had the best opportunity, as the link between the analytical desks and the RCMP, to obtain an understanding of the RCMP's requirements, and to ensure that the format and content of the TAs met these requirements in a meaningful way. Instead, Henry testified that, although he felt he had a good liaison relationship with RCMP VIP Security Branch, he was not familiar with the operations of the RCMP Airport Policing Branch or even the CSIS Sikh Desk.<sup>393</sup> Notably, the liaison between Airport Policing and the Sikh Desk was relevant in relation to threats to Air India.

### ***The Week of the Bombing: Failure to Maintain Minimal Personnel and Resources***

The general lack of resources for the Sikh extremism investigation was exacerbated by the fact that, during the week prior to the bombing, a number of important staff members were permitted to be absent, and investigative resources were diverted to other matters.

In the BC Region, Kobzey went on vacation on June 8<sup>th</sup> and returned the night of June 22<sup>nd</sup>. He was not on hand to advocate for continued surveillance of Parmar,

---

<sup>390</sup> Testimony of Daryl Zelmer, vol. 23, May 4, 2007, pp. 2313-2314.

<sup>391</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2545-2546.

<sup>392</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2508, 2511.

<sup>393</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2511-2512, 2542-2543.

to guide the transcribers and translators of the Parmar tapes, or to assess the significance of the “two weeks” comment made during the Khurana meeting before the bombing.

Betty Doak, the key transcriber for the Parmar intercepts, who also undertook responsibility for liaising with the translators, was away from just before the bombing until a week after. In her absence, the Punjabi translator alone processed the intercepted communications. This led to crucial gaps in the transcription, as the translator failed to record the subscriber information, a task normally carried out by the transcriber. As a result, although Parmar called Bagri on the day of the bombing, the telephone number where Bagri received the call was never recorded. This would have provided critical information about Bagri’s location on the weekend of the bombing. Instead, Bagri’s location that weekend was never determined.<sup>394</sup>

At HQ, there were similar absences. Upton took leave for five weeks starting June 21<sup>st</sup>. Deschenes, his direct superior, was away in Los Angeles for the week preceding the bombing, on another case.

All these people were key links for the Sikh extremism investigation. None had adequate replacements with in-depth knowledge of the investigation.

Valuable investigative resources were also pulled just prior to the bombing. CSIS had requested daily situation reports from all regions during the period leading up to, and including, the US visit of Rajiv Gandhi. This requirement was withdrawn as soon as Prime Minister Gandhi left the US.

One of the most unfortunate decisions made in CSIS’s pre-bombing investigation was the decision to withdraw surveillance from the stationary observation post (OP) near Parmar’s residence on the day of the bombing. Notably, mobile surveillance coverage had been removed days before, on June 17<sup>th</sup>. Although unprecedented mobile surveillance coverage for a CT target had been afforded to Parmar in June 1985, the removal of both the mobile and stationary surveillance resulted in CSIS having no record of Parmar’s movements on that day. Kobzey testified that surveillance priorities were determined with the chiefs of the various units, in consultation with the Chief of the PSU and the Deputy Director General Operations (DDG Ops).<sup>395</sup> Kenneth Osborne was the DDG Ops at the BC Region at the time. In a June 1992 interview with the Security Intelligence Review Committee (SIRC), Osborne was asked why the stationary observation post was unmanned on the day of the bombings. Osborne indicated that he would not have been consulted on this.<sup>396</sup> CSIS has been unable to locate specific documentation regarding the reasons why the OP was vacated on June 22, 1985.<sup>397</sup> The persistent lack of explanation for this critical decision is troubling, as it is impossible to assess the adequacy of the decision made. Was

---

<sup>394</sup> Exhibit P-101 CAA0557.

<sup>395</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, p. 3827.

<sup>396</sup> Exhibit P-101 CAB0883, p. 2.

<sup>397</sup> Exhibit P-101 CAA1086, p. 4.

surveillance pulled because BC Region failed to appreciate the significance of the threat from Parmar and his associates? Or, if it was cognizant of the threat, but allowed surveillance to be pulled due to a belief that some other investigation had a more compelling call on the scarce resources available, why did they not substitute another method to monitor Parmar's location in its place?

The reasons for this cutback in resources and personnel may have been a perceived easing of the threat, with the end of Prime Minister Rajiv Gandhi's state visit to the United States, as well as a need to relieve overworked personnel.<sup>398</sup> Despite the fact that the threat from Sikh extremists was still considered high, many key persons may have taken the "uneventful" end of the Gandhi visit and the passing of the anniversary of the Golden Temple storming as assurance that they could now take leave, and their superiors apparently agreed.

### ***Lack of Training and Development of Expertise***

The sufficiency of the training provided to the CSIS investigators and analysts is a matter which was canvassed during the Inquiry. The sudden transition from the RCMP Security Service to CSIS was not accompanied by opportunities to retrain or to provide enhanced training geared towards a civilian intelligence agency. Training in the first few years continued much as it had in the past under the Security Service which, as a practical matter, meant continuing with an emphasis on on-the-job learning.

Within the first year of CSIS, a new training academy was set up at Camp Borden. The purpose, however, was to train new civilian recruits rather than those already part of CSIS. At the same time, in order to bolster the ranks, CSIS allowed for "direct entry", which meant that police officers could join CSIS directly, bypass the requirement to attend Camp Borden, and assume a higher rank than the civilian recruits who were required to attend training. Geoffrey O'Brien testified that this procedure created inevitable tension within CSIS.<sup>399</sup>

The direct entry procedure also did not help CSIS move away from its police roots towards greater civilianization, a complaint that was echoed by both SIRC and the Osbladeston Report.

### ***HQ Analyst Training***

The members of the Sikh Desk testified about the training they were provided. Training was primarily on-the-job, and specific Sikh extremism expertise was developed on one's own time.<sup>400</sup>

Some basic training courses were offered. For example, Burgoyne took a basic training course for new employees (when he was a member of the RCMP SS). The

---

<sup>398</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, pp. 3572, 3620.

<sup>399</sup> Testimony of Geoffrey O'Brien, vol. 17, March 6, 2007, pp. 1560, 1563-1564.

<sup>400</sup> Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3576.

two-week course was for both desk analysts and field investigators. The course only covered the basic structure of the RCMP SS, and provided background on what the different units offered. They also had external speakers and instructors lecture on the global political climate. As well, liaison officers from the British and Australian security services spoke in relation to their operations. The courses did not specialize in any way, but only provided a general overview of the RCMP SS.<sup>401</sup>

Burgoyne testified that he was not given any particular training in relation to Sikh extremism:

No. I think the attitude at Headquarters was that as long as you understood operational policy, whether you're working the Armenians or the Sikhs or the Palestinians, – the issues, that's up to you to learn ... and quickly because one day you may be working one area, the next day another area. So you know, the issues dealing with Sikhism or the problems in the Punjab, you had to do your own reading and usually night-time reading.<sup>402</sup>

No time off was given to read up on relevant topics, such as the history of the Sikhs or the history of conflicts in India, issues which could have provided needed context to the Sikh struggle in 1985. No resource library existed at HQ. The only resource was the general conditions file on the countries. That file was generally made up of open source information provided to HQ by security liaison officers (SLOs) abroad. In fact the information provided by SLOs on a continuing basis was perhaps the greatest source of information available to CSIS.<sup>403</sup>

Gartshore's testimony was relatively similar:

**MR. FREIMAN:** Did you get any specific training in Western European terrorism?

**MR. GARTSHORE:** No.

**MR. FREIMAN:** Did you get any specific training in Pacific Rim terrorism?

**MR. GARTSHORE:** No.

**MR. FREIMAN:** Did you get any training in Sikh terrorism, or Sikh extremism?

**MR. GARTSHORE:** No.

---

<sup>401</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3402-3403.

<sup>402</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3403.

<sup>403</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3403-3404.



**MR. FREIMAN:** What was the theory – how were you to get yourself up to speed?

**MR. GARTSHORE:** Whatever I could read. Essentially we were conducting investigations. It was just like doing police work. Accept it.<sup>404</sup>

Gartshore testified that he too relied on any information he could gather on his own. Other material included reading material sent to CSIS by the Government of India, reports from discussions with community members in Canada and material from CSIS investigations. He also stated that most of the leads received by CSIS were from the Government of India.<sup>405</sup>

Upton confirmed that analysts were trained on the job. They were expected to learn from others and to learn by doing.<sup>406</sup> One obvious problem in the context of the Sikh Desk was that, at the outset, Burgoyne was the sole analyst and therefore the opportunity to learn from others was correspondingly attenuated.

Finally, the RCMP had offered some members of the Security Service the opportunity to upgrade their education with tuition paid to attend Carleton University and other universities.<sup>407</sup> Burgoyne was turned down when he made his request and was told he could complete his final year part-time.<sup>408</sup>

Burgoyne was transferred to the Sikh Desk (then the Western Europe and the Pacific Rim Desk) when the only analyst, Bill Dexter, was sent away for French Language training. Dexter did not return until May 1985. Though the effort to improve the bilingualism of the employees was commendable, the Commission notes that the timing was poor, given that enhanced French language skills would not have been useful for investigating Sikh extremism.

### ***Regional Intelligence Officer Training***

Intelligence Officers (IOs) in the regions received similar training. All of them had been RCMP officers prior to joining the RCMP SS and had therefore gone through regular officer training. On joining the RCMP SS, some received additional training, such as source development and source handling.<sup>409</sup> However, when it came to specific issues, such as Sikh extremism, the BK and the ISYF, the investigators relied on their internal files, which were put together through open source material and from their own investigation.<sup>410</sup>

---

404 Testimony of Glen Gartshore, vol. 31, May 22, 2007, p. 3516.

405 Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3549-3550.

406 Testimony of Russell Upton, vol. 31, May 22, 2007, p. 3576.

407 Testimony of John Henry, vol. 25, May 8, 2007, pp. 2544-2545.

408 Testimony of Bob Burgoyne, vol. 30, May 17, 2007, p. 3404.

409 Testimony of William Laurie, vol. 61, October 15, 2007, pp. 7394-7395; Testimony of Neil Eshleman, vol. 75, November 14, 2007, pp. 9440-9441.

410 Testimony of William Laurie, vol. 61, October 15, 2007, pp. 7394-7395.

Of particular note, the IOs did not receive training on specific policies, such as retaining notes. William Dean (“Willie”) Laurie, a CSIS IO who became involved in the investigation after the bombing, testified about this training:

**MR. BOXALL:** And you had received no training and policies of keeping a separate notebook or maintaining your records – the original records of information obtained from the witness?

**MR. LAURIE:** You know, earlier today such a policy was put before me and we didn’t see it and I know of no member actually using it....

**MR. BOXALL:** Was there any training with respect to officers as to what to do in that situation when they were overlapped? ...

**MR. LAURIE:** I was never given any guidance to do that.<sup>411</sup>

As with the Sikh Desk, none of the IOs in BC Region were given specific training on Sikh extremism. They learned about the issues through the documents they received through NSR, through community interviews and by reading in their spare time.

Despite the lack of resources, the IOs managed to develop an expertise in Sikh extremism that outweighed that of the RCMP. Soon after the bombing, CSIS investigators in both Toronto and Vancouver were asked to give talks to the RCMP in order to bring them up to speed on Sikh extremism issues.

### ***Physical Surveillance Training***

Physical surveillance personnel received regular officer training when they first joined the RCMP. Once they joined the RCMP SS PSU, they received on-the-job training. There was no formalized training course on physical surveillance, and there was no training in relation to Sikh extremism or any other issue which might relate to the targets they were following. The PSU members gained most of the knowledge they needed from the IOs, who briefed them at the start of the day. In effect, since the IOs themselves had very little opportunity for issue-specific training, such as on Sikh extremism, the PSU was equally disadvantaged.

Most training in surveillance skills was done on the job, with junior members of the team relying heavily on the expertise of senior members, as was the case with Lynne Jarrett and Larry Lowe, the surveillants at the Duncan Blast. Jarrett was very new to surveillance and was the most junior person in the unit. Lowe was not only the team leader, but an agent with 25 years on-the-job experience.<sup>412</sup>

---

<sup>411</sup> Testimony of William Laurie, vol. 61, October 15, 2007, pp. 7536-7538.

<sup>412</sup> Testimony of Lynne Jarrett, vol. 22, May 3, 2007, pp. 2194-2196.

The PSU personnel were given limited training with regard to weapons. This type of training would have been useful in connection with the Duncan Blast to help identify the sound that was heard. Jarrett testified that, although she had had some exposure to weapons during her training, it had been in a controlled environment, wearing ear protectors. In fact, Jarrett testified that, prior to the Duncan Blast, she had never heard rifle shots in the open without ear protection.<sup>413</sup>

Training in cultural differences might have aided the PSU in avoiding some of the errors they made. PSU members experienced great difficulty in differentiating Sikh males and relied heavily on the colour of their turbans. There are numerous incidents of misidentification throughout the Air India narrative, most notably in the case of Mr. X.<sup>414</sup> Further, they were seemingly unaware that all Sikh males included “Singh” in their name (either middle or last name), an issue which led to the misidentification of the telephone number Parmar dialed on the ferry on June 4, 1985.<sup>415</sup> While the PSU personnel were not expected to be experts in the field of Sikh extremism, they were lacking certain basic information which would have aided them in identifying persons who came into contact with Parmar. There was no evidence presented to suggest that any of the above issues were addressed in the PSU.

### ***Threat Assessment Training***

The Threat Assessment Unit had equally poor training. It is acknowledged that the TAU was not expected to be expert in any one field, in marked contrast to the members of the Sikh Desk. However, training on the basics of threat assessments, their role, to whom they were to be given, and how to best craft them, was lacking. John Henry testified that, when he was placed in charge of the TAU in 1980, he had had no experience in writing TAs. Instead, he had to rely on his second-in-command, who did have experience, to “show him the ropes”. Once again, training was done on the job, in this case with the junior officer teaching the officer in charge.<sup>416</sup> Such a situation was hardly acceptable, let alone ideal.

Henry told the Commission that, while part of the RCMP SS, he was sent to the RCMP training division to take a course entitled “Intelligence Analysis”. Henry testified that it did deal with TAs to some degree but it was not very helpful. The course dealt more with bootlegging and bookmaking operations and contained no specific training on writing threat assessments.<sup>417</sup>

As is clear from testimony from all sections of CSIS, training, especially focused training on Sikh extremism, was woefully inadequate. While many members of CSIS invested their own time in developing expertise, that necessity was an

---

<sup>413</sup> Testimony of Lynne Jarrett, vol. 22, May 3, 2007, p. 2186.

<sup>414</sup> See Section 1.5 (Pre-bombing), Mr. X.

<sup>415</sup> See Section 1.4 (Pre-bombing), Duncan Blast.

<sup>416</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2534-2535.

<sup>417</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2544-2545.

institutional failure on the part of CSIS. While learning on one's own time should not be discouraged, the fact that no institutional training was offered meant that those who did not invest their own time in expanding their knowledge may have been working with grossly inadequate knowledge and skill. Intelligence employees should have been given the resources to make sure their basic knowledge was developed, at least to a certain satisfactory level.

### ***Lack of Resources Continues after the Bombing***

These deficiencies continued to affect CSIS's investigations for years after the bombing, contributing to failures to prevent further terrorist attacks. CSIS's failure to prevent the attempted assassination of an Indian Minister in BC by Sikh extremists in March 1986 was partly attributed to a lack of resources. Due to resource limitations, the region had generally-accepted standards that allowed for time lags between communication interception, transcription and translation. Consequently, although CSIS possessed intercepts that warned of the attack, these tapes were not processed until after the attack.<sup>418</sup>

Warren recalled that, in the post-bombing period, the government granted approximately \$3.1 million specifically for augmentation of the counterterrorism program. He noted that the money was spent quickly. In October 1987, the Osbaldeston Report commented on the lack of resources and personnel in CSIS's CT investigations that had persisted since CSIS was created.

Throughout our review we were continually aware that CSIS has had serious resource problems. On the one hand, CSIS was established without due regard for the real costs of many "housekeeping" matters. On the other hand, we have observed that CSIS applies too many operational resources against some types of targets, and that the allocation of these resources needs further review.

We can state without further study that there must be more capital expenditure for accommodation and administrative needs. [CSIS] still shares many operational and administrative facilities with the RCMP. A large percentage of CSIS employees still go to work in the morning at RCMP headquarters, making it rather difficult to generate and maintain the esprit de corps that is so important.<sup>419</sup>

Not until after the release of the Osbaldeston Report in 1987 did CSIS finally receive adequate funds to deal with the gaps in their counterterrorism program that had persisted since the beginning of CSIS.<sup>420</sup>

---

<sup>418</sup> Exhibit P-101 CAB0647.

<sup>419</sup> Exhibit P-101 CAA0569, p. 29.

<sup>420</sup> Testimony of James Warren, vol. 48, September 19, 2007, pp. 5941-5943.

## Conclusion

CSIS's failure to allocate sufficient resources and personnel to the Sikh extremism investigation hampered its performance at all stages of the intelligence cycle. This deficiency was perhaps most pronounced in CSIS's intelligence collection efforts.

Each failure to obtain an investigative resource compounded CSIS's inability to build its base of knowledge and to justify the approval of further resources, eventually creating large gaps in the domestic intelligence environment. With little intelligence on Sikh extremism collected by CSIS, analysts were forced to rely on information from other sources, often foreign, of unknown reliability, which the organization was continually unable to corroborate or contradict. The outcome was a failure to understand the changing nature of the terrorist threat. That failure, in turn, materially harmed CSIS's ability to assess the Sikh extremist threat in advance of the June 1985 terrorist attacks.

### 3.3.4 CSIS Failures in Assessing the Threat

#### *Inability to Imagine a New Threat Paradigm*

CSIS threat assessments suffered from a set of uncritical assumptions about the nature and targets of Sikh terrorism. The Government of Canada was unprepared for a tragedy like Air India – a lethal, coordinated attack on Canadian targets. The emergence of Sikh terrorism represented a new threat paradigm, one motivated by political objectives but justified by religious imperatives. CSIS analysts treated information about the new threat paradigm with skepticism, expecting threats to conform to those of the past, rather than looking ahead to the changing threat environment. Admittedly, it is very difficult to successfully predict the next emergent threat, as experienced personnel will differ on the true nature of the “next war”. However, there must be institutional flexibility and creativity to recognize emergent threats, and an ability to focus on understanding the goals of those who threaten national security, in order to think through the modalities by which they might seek to achieve these goals.

The lack of imagination on the part of CSIS analysts about the nature and targets of Sikh terrorism was attributable to inexperience in the emerging field of terrorism, compounded by inadequate intelligence collection efforts. Wesley Wark described CSIS's failure to develop sufficiently the capability and expertise to properly assess threats to national security:

CSIS ... [were] doing threat assessments with the same tools and the same people that the RCMP Security Service were doing them with; the same people and tools that were heavily criticized by the McDonald Commission after all, for their failure to be sufficiently sophisticated about the nature of international security threats.<sup>421</sup>

---

<sup>421</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, p. 1497.

The Sikh Desk acted as the analysis centre for Sikh extremist threats, but its analysts were not provided the basic tools: experience, information and resources that would have enabled them to recognize the nature of the emerging threat of lethal violence in Canada. Proper analysis would have required training on emerging terrorism trends, comprehensive domestic intelligence collection by CSIS investigators, and adequate resources and personnel to process the mass of available information. Sikh Desk analysts were provided with none of these.

### ***Dependence on Foreign Intelligence***

The Sikh Desk's main supplier of intelligence regarding the Khalistani movement in India and Canada was the Government of India (GOI) and the rhetoric of Sikh extremists themselves.<sup>422</sup> Often, CSIS first became aware of many of the key figures and groups in the Sikh extremist movement in Canada through the GOI. As early as April 1982, the GOI identified Parmar as a Khalistani terrorist leader, responsible for several crimes, including the murder of two policemen in India. In July 1982, the GOI further identified Parmar as a specific threat to Prime Minister Indira Gandhi during her upcoming visit to New York City.<sup>423</sup> In November 1983, the GOI first sent information about the emergence of the Babbar Khalsa (BK) in Canada.<sup>424</sup>

CSIS did not have a long-established intelligence-sharing relationship with the Government of India. While CSIS commonly accepted the reliability assessments of its allied intelligence partners, it felt unable to rely upon the assessments by the Indian government. The Sikh Desk was cautious about accepting the *bona fides* of the voluminous threat information provided by the Indian government and the threats issued by Sikh extremists. The Desk sought specific corroboration of all information passed on by the Indian government,<sup>425</sup> which was rarely found, due, in part, to CSIS's own limited intelligence collection capabilities in its Sikh extremist investigation.

### ***CSIS Skepticism about the Sikh Extremist Threat***

In the year preceding the bombing, CSIS was generally skeptical about information on the Sikh extremist threat in Canada. CSIS understood the importance of the credibility of its assessments and placed great importance on its ability to separate the wheat from the chaff, and to calibrate the reliability of threat information received. CSIS thus generally adopted a cautious stance, remaining skeptical about threat information until it was able to substantiate the information with reliable intelligence, collected by itself or its established partners.

This approach was fueled by the sentiments held by members of the Canadian Sikh community in relation to the Sikh extremist threat and its causes.<sup>426</sup> CSIS

<sup>422</sup> Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3549-3550.

<sup>423</sup> Exhibit P-101 CAB0031.

<sup>424</sup> Exhibit P-101 CAB0042.

<sup>425</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, pp. 3476-3477.

<sup>426</sup> See, for example, Exhibit P-101 CAB0176: Article by Tara Singh Hayer alleging that any confrontation would be due to GOI provocation.

was aware that members of the Sikh community felt that the Indian government was issuing the multitude of threat warnings in a simple attempt to discredit Sikh nationalism in Canada.<sup>427</sup> Sikh extremist leaders were claiming that the Indian government had sent spies to Canada to portray Sikhs as being violent and extremist.<sup>428</sup> In one instance, the Sikh Desk noted that moderate leaders within the Sikh community had discounted the rumoured existence of a “hit list” of targets in Canada, and that they felt that the “hit list” was simply “...an idea being used by a small militant group to increase the climate of tension in the Sikh community and to induce moderates to adopt a more extreme stance.”<sup>429</sup>

CSIS’s skepticism about the seriousness of Sikh threats was also partly attributable to fatigue over the seemingly constant threat. The large volume of information provided by the GOI and the suspicion of bias on the part of the GOI combined to create a view at CSIS that much of the information could be discounted as nothing more than “crying wolf.”

The seriousness of the threat posed by Sikh extremists continued to be discounted, even after the terrorist bombing of Flight 182. In March 1986, an Indian government official was shot while visiting Vancouver Island for personal reasons. CSIS had intercepted communications prior to the attack, but the investigators in BC Region did not feel the information was credible enough to alert the responding agencies, as unsubstantiated threats were commonly issued by Sikh extremists.

[T]he fact that the taped communications contained threats of harassing Sidhu was not seen as unusual; threats against others that are rarely carried out were said to be common in communications between CSIS Sikh targets.<sup>430</sup>

Archie Barr noted that the threat information received by the BC Region prior to the attack should have been assessed as significant, and investigators should have passed the information to HQ rather than discounting it as another “cry wolf” remark.

Clear information about the pending attempt on his life was received the Friday before it happened, but it wasn’t passed on until Monday following the attack. This was a case of negligence, if not ineptitude.... Some action could have been taken, and it should have been taken. It was poorly handled and there was no excuse for not contacting Headquarters.<sup>431</sup>

---

427 Exhibit P-101 CAB0124, p. 2.

428 Exhibit P-101 CAB0129, p. 2.

429 Exhibit P-101 CAB0105.

430 Exhibit P-101 CAB0647, p. 13.

431 Exhibit P-437: Statement of Archie Barr, pp. 14-15.



While it was important that CSIS attempted to assess the validity of all threat information, a review of the Inquiry evidence indicates that Desk analysts relied too heavily on the notion that the Sikh extremist threat would adhere to conventional conceptions about terrorism.

### ***Conventional Conceptions about Terrorism***

Bruce Hoffman testified that the Air India and Narita bombings differed from conventional acts of terrorism at the time.<sup>432</sup> The lethal and simultaneous nature of the attacks was quite exceptional. The common belief was that "...terrorists wanted a lot of people watching and not a lot of people dead." Any violence was expected to be directed at "symbolic" targets such as diplomats and consular properties. Hoffman testified that this led to a fatally false sense of security, based on the belief that terrorist violence would be kept within acceptable boundaries, and that terrorists thought that indiscriminate murder would alienate the very people they wished to recruit and influence. It was believed that terrorists wanted to preserve an image of legitimacy, notwithstanding their threats and occasional resort to violent attacks, and thus would tailor their actions in ways designed to not offend the international community and to avoid triggering harsh repressive measures from their enemy. Experts at the time noted that terrorist actions were often limited to simply issuing a manifesto and threats to gain publicity for their cause.

### ***The Rise of Religious Terrorism***

However, by the early-to-mid 1980s, terrorists became convinced that more spectacular, daring and bloody acts were necessary to obtain the degree of attention that more constrained acts might have garnered in the past. Justifications for violence began to emerge in terrorist circles. There was a new inclination to resort to violence as revenge for oppression. Religious-based terrorism emerged, justifying violence on religious precepts. Violence became a divine duty or a sacramental act, and, by implication, refusing to engage in violence would mean disobedience to a religious obligation. Religious-based terrorists arose, who felt that they had no choice but to take up arms to fight perceived victimization and persecution.<sup>433</sup>

Hoffman noted that the actions of the radical Sikh movement in the early 1980s conformed to the patterns and characteristics of religious terrorism.<sup>434</sup> The "martyrdom" of Bhindranwale in the Golden Temple storming created an ideal basis for support of religious terrorism by Sikh extremists. At the time of the bombing, CSIS investigators on the ground appeared to understand the religious motivations behind the movement. The BC Region situation report on June 17, 1985 noted that "...basically what we are dealing with is a problem involving a political issue with religious fanaticism being used as the driving

---

<sup>432</sup> Testimony of Bruce Hoffman, vol. 19, March 9, 2007, pp. 1779-1785.

<sup>433</sup> Testimony of Bruce Hoffman, vol. 19, March 9, 2007, pp. 1787-1789, 1793.

<sup>434</sup> Testimony of Bruce Hoffman, vol. 19, March 9, 2007, p. 1796.

force to achieve the goal in question.”<sup>435</sup> Meanwhile, Sikh Desk analysts appeared to recognize the new phenomenon of religious terrorism, but did not expect it to emerge as quickly and lethally as it did. While the Sikh Desk worked diligently to understand the Sikh extremist movement, it failed to give credibility to the rapid increase in the potential for large-scale violence after the Golden Temple storming, justified by the religious basis of the movement. Burgoyne testified that:

My personal feeling is that no one saw the Sikh issue – rising so quickly in prominence and I think that was as a result of the raid on the Sikh Golden Temple and maybe it was our lack of understanding of Sikhs and how very emotional – and how this single issue is what propelled us into what was a very tumultuous year.<sup>436</sup>

The Sikh Desk analysts appeared to adopt the conventional wisdom about terrorism, including the belief that terrorists wanted publicity, not violence. The Air India bombings did not conform to this conventional understanding. They were acts of indiscriminate mass murder, conceived in Canada and targeted against Canadians. CSIS analysts were ill-equipped to conceive of such acts at the time, and CSIS and the agencies it advised remained unprepared for them.

### ***Breaking Conceptions about Terrorism***

To have fully appreciated the emerging Sikh extremist threat, CSIS would have had to break out of the conventional conceptions about terrorism. The Commission investigated CSIS’s attitude towards the flood of threats prior to the bombings, in an attempt to determine whether CSIS’s assessments were justified on an unbiased review of the facts, or instead hampered by tunnel vision.

In CSIS’s constant search for corroboration and for “specific” threats, it failed to step back to consider the significance of the growing amount of information indicating the changing nature of the Sikh extremist threat. CSIS analysts remained wed to the ideas that the Sikh extremist threat was mainly a foreign-influenced issue; that the potential for violence in the Sikh extremist community was remote; and that terrorist attacks, if they were to occur, would be focused on obvious symbolic targets such as Indian missions and personnel.

### ***Sikh Extremism: A Foreign Threat***

Initially, the Sikh Desk appeared to subscribe to the notion that terrorist violence was a foreign-influenced issue, not a domestic one. The Sikh extremism investigation was opened to investigate the possible eruption in Canada of Sikh

---

<sup>435</sup> Exhibit P-101 CAA0219, p. 2.

<sup>436</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3488.

community violence, brought about by related developments from India.<sup>437</sup> Early CSIS investigations were unable to uncover definite evidence of terrorist conspiracies by Canadian Sikh extremist groups. However, their ability to do so was hampered by their overall lack of investigative capacity in this area.

Early assessments generally described the unrest occurring in the Punjab region, focusing on the events at the Golden Temple rather than the situation in Canada. CSIS took the view that the Sikh community in Canada was generally peaceful, but that foreign Sikh extremists might come to North America to commit terrorist acts.<sup>438</sup> After the Golden Temple storming, CSIS admitted that there was a possibility that extremist elements within the Canadian Sikh community could pose a threat to Indian interests.<sup>439</sup> In mid-June 1984, when Air India warned of suicide attacks, CSIS called for further investigation, but, on the basis of its limited knowledge, expressed skepticism that violence by Sikh extremists would occur in Canada.

It is unclear whether this attack is planned for Canada or any vulnerable Air India office worldwide.... Air India in Canada has never been the target of attack by extremists. The hijacking of Air India aircraft by Sikh terrorists has been limited to flights in India and Pakistan.<sup>440</sup>

The GOI issued a White Paper on the Punjab Agitation on July 10, 1984,<sup>441</sup> outlining an international Sikh extremist threat. The White Paper clearly described a major Canadian connection to the Sikh extremist movement. It indicated that Parmar had set up the BK in Canada and was the head of the overseas unit of the BK. Parmar had allegedly claimed that the BK was responsible for several murders and acts of sabotage in India. The White Paper also mentioned Surjan Singh Gill and his February 1984 letter to Sikh leaders in the Punjab, which asked them to continue the fight for Khalistan, urging them to consider employing suicide squads. Indian authorities claimed Parmar was "...the most dangerous Sikh terrorist presently at large", but CSIS viewed the Indian assessment as being biased.<sup>442</sup>

Canada had the second largest concentration of Sikhs outside India, after Britain.<sup>443</sup> In addition to the information received from the GOI, CSIS was aware of the violent extremist rhetoric espoused by three Canadian Sikhs, Parmar, Bagri and Gill – rhetoric that included calls for 50,000 Hindus to be killed as revenge for the Sikhs killed in the Golden Temple storming, and threats that all Hindus

---

437 Exhibit P-101 CAB0054.

438 Exhibit P-101 CAB0055, CAB0057.

439 Exhibit P-101 CAB0111.

440 Testimony of Bob Burgoyne, vol. 31, May 22, 2007, pp. 3458-3459; Exhibit P-101 CAB0076, p. 2.

441 Exhibit P-101 CAB0104, p. 6.

442 Exhibit P-101 CAB0114.

443 Exhibit P-101 CAB0100, p. 5.

living in North America after August 1<sup>st</sup> would be killed.<sup>444</sup> Upon his return to Canada from the West German prison, Parmar stated: "I want to warn the Indian government they'll pay the price for attacking the Temple."<sup>445</sup>

By October 1984, CSIS had focused its investigation on Parmar, Bagri and Gill. CSIS recognized the threat potential posed by Parmar, warning that he was the most radical and potentially dangerous Sikh in the country, with a close circle of like-minded associates who posed a serious threat. However, CSIS noted that his support in Canada appeared to be minimal at the time.<sup>446</sup>

In the following months, CSIS began to realize the threat potential of Sikh extremist groups in Canada, noting in several TAs that the threat to Indian interests from these groups was high. However, CSIS continued to underestimate the potential for a coordinated conspiracy to undertake violent action in Canada, despite the fact that several major Sikh extremist figures were present in the country and espousing violent rhetoric.

### ***Underestimating Potential for Violence of Sikh Extremists***

CSIS considered early incidents of violence in the Sikh community to be emotional outbursts in reaction to events in India, or to interfactional temple rivalries (and thus, not related to threats to national security). This rationalization allowed CSIS analysts to maintain the belief that violence would be minimal, sporadic and contained within the Sikh community.

The Sikh Desk understood that the majority of Sikhs were peaceful, desiring communal harmony, and that the threat of violence came from a very small group of radicals. In the year preceding the bombings, the Desk acknowledged the growing threat potential from this radical group but did not adequately assess the potential for coordinated, large-scale conspiracies. Any violence was expected to be due to "uncontrolled outbursts" by persons overtaken by emotion.<sup>447</sup> CSIS cited the shooting at the Toronto Consulate in 1982,<sup>448</sup> and the Winnipeg attack on the Acting Indian High Commissioner Fabian, as examples of "emotional" outbursts by Sikhs.<sup>449</sup> In August 1984, the Sikh Desk began to warn of increasing possibilities of violence. It reported on a protest at which young Sikhs chanted angrily and threw eggs. The TA recognized the volatile nature of the youths involved, and warned that it could lead to more serious incidents, with the eggs being replaced by something more harmful.<sup>450</sup> By September 1984, CSIS noted the growing polarization between the moderates and extremists within the Sikh community and warned that "...the real threat comes from the radical groups who ... might take precipitous actions not

444 Exhibit P-101 CAB0143.

445 *The Province* (Vancouver) (July 9, 1984).

446 Exhibit P-101 CAA0104.

447 Exhibit P-101 CAB0120.

448 Exhibit P-101 CAB0035 (November 16, 1982), CAB0112 (July 25, 1984), CAB0124 (August 13, 1984).

449 Exhibit P-101 CAB0148.

450 Exhibit P-101 CAB0130.

sanctioned by ... the moderate leadership<sup>451</sup> This view persisted within CSIS ranks and was noted in the May 24, 1985 TA issued in anticipation of the Gandhi visit to the US. The TA notes that Sikh extremist groups were attempting to "... flame the emotions of younger Sikhs who may be susceptible to irrational and spontaneous acts of violence."<sup>452</sup>

The threat assessments in 1984-1985 regarding Indian interests exhibited CSIS's lack of knowledge about key Sikh extremist groups in Canada.<sup>453</sup> After the Indian government alerted CSIS in 1983 about Parmar's group, the Babbar Khalsa (BK), CSIS had difficulty confirming its existence in Canada. In June 1984, the BC Region offered the opinion that the BK might be a "...group of malcontents and frustrated separatists who utilized threats in order to get attention from a small minority of local Sikhs."<sup>454</sup> In assessing the BK's threat potential, CSIS remained unable to confirm the BK's existence in Canada, but concluded that the threat that the BK would kidnap or kill Indian diplomats in Vancouver could not be entirely discounted.<sup>455</sup> By October 1984, CSIS noted the recent emergence of groups in Canada using names of Sikh extremist groups that were known internationally, including the BK. At the time, CSIS believed that these named groups were being used in Canada by a small number of advocates of Sikh separatism to attract attention to their cause and to broaden their appeal within the Sikh community.<sup>456</sup> Nearly a year later, CSIS appeared to have little new knowledge about the activities of the BK in Canada. In April 1985, CSIS noted that whether the BK was actually planning an action in Canada or abroad was a matter of conjecture, and that it had no information that would support such speculation.<sup>457</sup> CSIS provided the RCMP with an overview of the BK on April 24, 1985, consisting of a brief listing of the threats issued by the BK in 1984 and a mention that Parmar was considered to pose the greatest threat in Canada to Indian interests. CSIS reported that it believed the organization consisted of approximately 20 members.<sup>458</sup> Other than the increased membership, it appears that CSIS had not collected any independent intelligence about the BK to better understand its activities throughout this period.

CSIS TAs often offered the view that the threats made by Sikh extremists were exaggerated, issued more for tactical reasons than as an expression of an actual willingness to carry out violent acts.<sup>459</sup> While this may generally have been true in terms of past Canadian experience, relying on the continued validity of this conventional notion of terrorism prevented CSIS from adequately investigating the possibility of planned violent actions by Sikh extremist groups. CSIS generally dismissed threats to Indian missions and Air India flights made by phone or

451 Exhibit P-101 CAB0136, CAB0137.

452 Exhibit P-101 CAB0236, p. 3.

453 Exhibit P-101 CAB0105. CSIS reported difficulty in confirming the existence of a known Sikh terrorist group, the Dashmesh Regiment, in Canada.

454 Exhibit P-101 CAB0061, CAB0064, CAB0085.

455 Exhibit P-101 CAB0058, CAB0061.

456 Exhibit P-101 CAA0104.

457 Exhibit P-101 CAB0223.

458 Exhibit P-101 CAB0221.

459 Exhibit P-101 CAB0105.

letters. An October 22, 1984 TA warned against the emotional characteristics of Sikhs, but stated that CSIS was still inclined to believe that Sikhs in Canada would continue to concentrate their efforts here without resorting to tactics such as aircraft hijackings.<sup>460</sup> One CSIS TA noted that telephone bomb threats had been made to Air India offices in Toronto in the summer of 1984 "...as part of the antagonistic campaign against Indian interests."<sup>461</sup> Threatening letters sent to the Toronto Consulate in February 15, 1985, were dismissed as a ploy by Sikh fanatics to keep the Khalistan issue alive.<sup>462</sup> CSIS assessed a threat reported against the incoming Air India flight on April 13, 1985 as unlikely to result in actual violence:

We believed then as we believe now that threats of this nature are probably generally communicated by mail or telephone to continue to cause problems and perpetuate terrorist threats in hopes of causing unrest/retaliatory measures by the Indian Government so as to keep Khalistan alive in the minds of all Sikhs.<sup>463</sup>

The TAs in the following months regularly cited a general "high" threat potential from Sikh extremists in Canada, but added that CSIS had no specific information about this "high" threat.<sup>464</sup> In the months before the Air India bombing, CSIS appears to have recognized the growing threat potential of Sikh extremists, but remained unable to gather information about the specific plans of these groups. On March 20, 1985, CSIS warned that Sikh extremist activity in Canada had not receded and that the threat of violent actions against Indian interests remained high.<sup>465</sup> On May 24, 1985, CSIS described the BK and ISYF as Sikh extremist groups with "clear violence potential." However, the TA concluded that although both groups were planning demonstrations in relation to the Gandhi visit in early June, CSIS had no information to indicate that violence was being planned. CSIS warned, however, that the situation could change rapidly based on events in the Punjab.<sup>466</sup> It appeared resigned to its inability to predict the actions of Sikh extremist groups and, on June 5, 1985, cautioned that should the radical elements plan any action, there was a good possibility that it would not have any foreknowledge.<sup>467</sup>

The misconception that Sikh extremist groups would not likely resort to violence in Canada resulted in an abdication of responsibility on the part of CSIS to take the threats seriously enough to consider when and how these threats might come to fruition. The underlying logic was that, if an act of violence were to occur, CSIS would not have had advance notice, as the actions of Sikh extremists were assumed to be spontaneous and emotional responses to events in the Punjab.

---

<sup>460</sup> Exhibit P-101 CAB0148.

<sup>461</sup> Exhibit P-101 CAB0218.

<sup>462</sup> Exhibit P-101 CAB0192.

<sup>463</sup> Exhibit P-101 CAB0218.

<sup>464</sup> Exhibit P-101 CAB0173 (December 7, 1984), CAB0182 (January 9, 1985), CAB0192 (February 15, 1985).

<sup>465</sup> Exhibit P-101 CAB0203.

<sup>466</sup> Exhibit P-101 CAB0236(i).

<sup>467</sup> Exhibit P-101 CAB0249.



### ***Attitude towards Threats to Air India***

The TAs issued by the Sikh Desk tended to focus on threats to Indian missions and personnel, with much less attention and credibility given to possible threats to other Indian interests such as Air India or to the general public. This may have been due to the fact that the RCMP VIP Protection Unit, whose specific mandate was to protect GOI missions and personnel, was the main client for CSIS TAs.

CSIS TAs were generally classified as dealing with threats to “Indian Missions and Personnel.” John Henry, the Head of the Threat Assessment Unit (TAU), testified that the term “Indian interests” was intended to include Air India. However, it is not clear that the agencies receiving the CSIS TA product were fully aware of this fact. The June 7, 1984 TA, in response to the Golden Temple storming, warned of demonstrations at Indian missions “...and possibly other Indian interests.”<sup>468</sup> No effort was made to explicitly list these Indian interests.

Even when threats to Air India were received and noted in CSIS TAs, CSIS often expressed skepticism that the threat would apply to Air India flights in Canada<sup>469</sup> despite the fact that, throughout the year preceding the bombings, it had received a flood of information from a range of sources linking threats to Air India to Canada. In June 1984, the Air India General Manager at Mirabel passed on a warning that 20 Sikhs were preparing to launch a suicide attack against Air India.<sup>470</sup> Later that month, an Air India sales agent in Toronto received a call from a person using the name “Grewal,” stating that “...one of the Air Indian aircraft one of these days is likely to be sabotaged.”<sup>471</sup> A few days later, the Air India Toronto office received a call warning of a bomb threat on an Air India flight.<sup>472</sup> On August 7, 1984, the Vancouver Police Department (VPD) Indo-Canadian Liaison Team informed CSIS that two audio cassette tapes warning that a plane would be hijacked had been dropped into an Air Canada mail slot. The voice on the tape was suspected to be that of a Sikh.<sup>473</sup> In September 1984, the Desk was notified of a threat of three terrorists hijacking an Air India flight “...originating from Canada and North America.”<sup>474</sup> In October 1984, the GOI warned that Bagri was known to be part of a plot to hijack Air India aircraft from any port of origin and destination in North America.<sup>475</sup> A separate police source warned that a plot was underway to sabotage an Air India flight from Montreal. The GOI continued to send threat warnings predicting the hijacking of Air India flights to and from Canada. In January 1985, the GOI warned of Sikh extremist plans to stage some spectacular actions threatening civil aviation, including hijacking an Air India flight from Montreal or Toronto.<sup>476</sup> The GOI passed on an unconfirmed report that

---

<sup>468</sup> Exhibit P-101 CAB0101.

<sup>469</sup> Exhibit P-101 CAB0076; Testimony of Bob Burgoyne, vol. 31, May 22, 2007, pp. 3458-3459.

<sup>470</sup> Exhibit P-101 CAB0076.

<sup>471</sup> Exhibit P-101 CAB0079.

<sup>472</sup> Exhibit P-101 CAB0088.

<sup>473</sup> Exhibit P-101 CAF0818.

<sup>474</sup> Exhibit P-101 CAB0140, p. 4.

<sup>475</sup> Exhibit P-101 CAA0103.

<sup>476</sup> Exhibit P-101 CAB0185.



an Air India flight to Toronto would be hijacked, specifically on April 13, 1985.<sup>477</sup> On May 16, 1985, the RCMP informed CSIS that the London Metropolitan Police had arrested five Sikhs in the UK who were buying remote-controlled devices. An Air Canada flight schedule was found amongst the documents of the five Sikhs.<sup>478</sup> All these threats were directed at Canadian flights and almost all were specifically directed to Air India flights in Canada. With only one flight arriving and departing Canada weekly, it is difficult to imagine not considering that any threat to Air India would apply to Flight 182 from Canada.

Even when CSIS considered threats to Air India in Canada, it generally concluded that the possibility of an actual attack was remote. In October 1984, CSIS responded to a threat to Air India passed by the GOI, and advised that Sikhs in Canada were not expected to resort to tactics such as aircraft hijackings. CSIS did not however rule out the possibility entirely, due to the “emotional characteristics” of the Sikhs.<sup>479</sup> Days later, CSIS received some corroboration from the Vancouver Police Department of a threat to Air India, and appropriately concluded that the “...potential for Sikh Extremists damaging an Air India aeroplane is real.”<sup>480</sup> While CSIS changed its assessment on the basis of the new information from the VPD, its ongoing assessment efforts were hampered by its general inability to find corroboration through its own investigations. Even after this, CSIS continued to generally discount subsequent threats to Air India in Canada. One reason for discounting these threats might have been the “cry wolf” syndrome. The fact that repeated threats to Air India failed to come to fruition appears to have created a threat fatigue within CSIS. John Henry expressed his doubts about the seemingly constant threat to Air India in the year prior to the bombing. Regarding the threat to the incoming Air India flight to Toronto on April 13, 1985, he stated:

We didn't really think there was any substance to it. An example here is your Air India flight 181. It was going to be hijacked coming in to Toronto. It seems to me none of them were ever hijacked.<sup>481</sup>

When the RCMP received the June 1<sup>st</sup> Telex, it failed to pass the threat on to CSIS,<sup>482</sup> but did ask for an updated assessment of threats to Air India. CSIS's response was brief and vague, providing no specifics. It did, however, contain one of the only clarifications on record that assessments relating to threats to Indian missions were intended to include Air India.

---

<sup>477</sup> Exhibit P-101 CAB0215.

<sup>478</sup> Exhibit P-101 CAB0233.

<sup>479</sup> Exhibit P-101 CAB0148.

<sup>480</sup> Exhibit P-101 CAB0154.

<sup>481</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2552.

<sup>482</sup> See Section 1.2 (Pre-bombing), June 1<sup>st</sup> Telex.

Currently CSIS assess [*sic*] the threat potential to all India missions in Canada as high. This is also intended to include Air India. CSIS, however, is not aware of any specific threat to the airline. Should we learn of any specific threat relating to Air India, you will be advised immediately.<sup>483</sup>

It is unknown how CSIS's assessment would have changed had it seen the June 1<sup>st</sup> Telex. However, it is clear that, up to this point, CSIS was aware of a flood of threats to Air India, and, less than three weeks before the bombing, offered no more detail about the potential target, perpetrators or timing of the threat than to conclude that the threat potential to Air India was "high."

### **Conclusion**

CSIS underestimated the ability and will of Sikh extremists to channel their emotions into coordinated, lethal attacks in Canada – attacks that might have been predicted and prevented by more thorough intelligence investigations into these small extremist groups.

Admittedly, CSIS's ability to further the Sikh extremism investigation was limited by the fact that the extremists operated in close-knit groups and were often secretive about their activities. However, as noted in the previous sections, CSIS failed to properly prioritize and resource the investigation into Sikh extremism, and this resulted in a situation where analysts had little information that might motivate them to look beyond the then-current notions about terrorism. Accordingly, they continued to assume that terrorist violence would likely be confined to the Punjab, and that these acts would, in any event, be unplanned and spontaneous, embodying emotional responses to events in the Punjab, and would not likely be directed against large-scale civilian targets such as Air India. The inability of CSIS analysts to comprehend the possibility of a different orientation for potential Sikh extremist acts of terrorism left CSIS, and the agencies it advised, unprepared for the events of June 22-23, 1985.

### **3.3.5 Failures in Internal Information Sharing**

Because of the lack of resources assigned to the intelligence collection effort in the Sikh extremism investigation, good communication and coordination were critical between the few investigators and analysts who were involved. This would allow CSIS to make the most of the limited information collected.

CSIS was a centralized organization, with Headquarters (HQ) assigned the responsibility for coordinating the investigations undertaken by regional offices across the country. HQ was the information gatekeeper, acting as a depository for all related information received from the various regions, as well as from other government departments and foreign partners. HQ was responsible for ensuring that regional investigators gained access to information obtained from other sources that was relevant to the regional investigation.

---

<sup>483</sup> Exhibit P-101 CAC0416.

A free flow of information within CSIS was critical, not only because of the lack of resources, but also in recognition of the fact that terrorism was rarely a localized phenomenon, but rather one with national and international dimensions. The Commission analyzed the adequacy of CSIS policies and practices regarding information sharing within the agency, and asked whether there were any deficiencies that affected the CSIS investigation into the Sikh extremist threat before the bombings. A number of deficiencies were found.

### ***Practices and Policies***

Information collected by CSIS was stored in a centralized computerized database, the Narrative Storage and Retrieval (NSR) system. All HQ analysts and regional Intelligence Officers (IOs) across the country had access to the NSR system. Information was searchable by keyword. Regional IOs entered information collected from their investigations into NSR, where it could be accessed by CSIS personnel at HQ and other regions. HQ analysts entered information received from external sources, including other government departments and foreign agencies. Kobzey testified that all CSIS investigators had daily access to the NSR system, allowing them to obtain information provided by other investigations across the country and to receive orders from HQ.

Kobzey testified that he would normally check the system daily, upon his arrival at the office, to see if any new data had been uploaded in the form of intelligence, surveillance or search reports, etc., by investigators from headquarters and the regions. He was interested in threat assessments or assignments from HQ for investigation. Anything urgent would be downloaded, printed and placed on his desk for him to take the necessary action. This could involve conducting field inquiries, requesting PSU coverage, conducting his own surveillance, or whatever was necessary.<sup>484</sup>

The IOs were responsible for diligently inputting information obtained from their investigations in a form that allowed others to benefit from their insight. Each NSR report would contain an “Investigator’s Comments” section, where the IOs would provide context to the information reported. They would also outline the significance of the information to HQ orders or investigations by other regions.

[T]here would be a block with the title “The Investigator’s Comments.” That would be where I would try to put into context, for the benefit of the other regions and my Headquarters counterpart, the significance of the information in relation to the investigation we were conducting in BC or, if it was a follow-up inquiry for HQ tasking or if it pertained to messages that were coming to us from the other regions regarding activities taking place in their locations and

---

<sup>484</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3734-3735.

any information that we had that was pertinent to those investigations, we would cross-reference their message and make notes in the comments about the significance of what we had done.<sup>485</sup>

A good example of the utility of the NSR system was the Subject Evaluation Report prepared on Parmar for the OPRC (Operational Priorities Review Committee) level 4 investigative authority application.<sup>486</sup> Kobzey prepared an initial report on Parmar, based on the information available on the NSR system and his personal knowledge of the subject. The initial report was passed to HQ analysts, who added relevant information from other government departments and foreign partners that Kobzey could not access.<sup>487</sup> Ultimately, the report included information gathered by CSIS investigators in BC Region and by other CSIS regions, as well as information about Parmar's activities in India and his arrest in West Germany.<sup>488</sup> As an example, Parmar was in Calgary when he made one of his most infamous statements, in which he "...strongly urged Sikhs to unite, fight and kill in order to revenge the attack on the Golden Temple in the Punjab."<sup>489</sup> That information was entered into NSR by CSIS personnel in Calgary, and was therefore available for Kobzey when he prepared his initial report on Parmar. The information was included in both Kobzey's report and in the subsequent HQ application.<sup>490</sup>

The NSR database provided a system that theoretically allowed CSIS personnel to obtain a comprehensive understanding of any CSIS investigation. The success of the NSR system depended on the thoroughness of the information in the database and the ease with which information could be accessed.

The Commission assessed the adequacy of the system for sharing of information within CSIS. The NSR system was ahead of its time in its ability to offer a centralized database of information, linking investigations across the country. With some hindsight, and allowing for the state of technology then and now, the Commission undertook a critical review of the NSR limitations. The Commission found failures in internal sharing that hindered CSIS's ability to "connect the dots" in their assessment of the threat of Sikh extremism in the period leading up to the bombing. These failures were the result of weaknesses in both operations and policies within CSIS. First, the utility of the NSR system suffered from technical limitations. Second, compartmentalization was apparent among all CSIS units, as information sharing was restricted on a "need-to-know" basis.

### ***Deficiencies in the NSR System***

The NSR was designed to provide a useful system for archiving and accessing the large quantity of intelligence collected by CSIS. While it often achieved this

---

485 Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3736.

486 Exhibit P-101 CAB0139.

487 Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3739-3743.

488 Testimony of Ray Kobzey, vol. 32, May 23, 2007, pp. 3739-3740.

489 Exhibit P-101 CAB0139, p. 3.

490 Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3741.

objective, its utility was limited by the fact that the database was not necessarily easily searched, nor was it accessible to all CSIS offices.

Kobzey called the NSR system cumbersome, and admitted that proper use of the system required taking a course to understand how to retrieve information using basic Boolean searches.

It was a program, bearing in mind we are talking 1981 onwards. It was an older style of computer database, and it was a cumbersome database. It required basically Boolean search ... equations, to retrieve the information that you were looking for. And you had to take a course in it, a storage and retrieval course ... and be certified before you could go on the system.<sup>491</sup>

John Henry admitted that CSIS was "...in [its] infancy when it came to computerization at the time." He noted that, although all the documents were placed in the database system, there did not exist a foolproof way to ensure that the information was properly correlated and easily accessible.<sup>492</sup>

In 1985, the NSR system was not employed in every district. The Toronto office was responsible for the entire South West Ontario Region, and as such, district offices in certain areas reported to the Toronto office. This included Windsor District, which was staffed by three agents at the time. While Toronto had access to NSR, the districts did not. This meant that messages for Windsor would be sent to Toronto first, and Toronto would disseminate them to Windsor. Likewise, when Windsor needed to report to HQ, it would send its report to Toronto, where the manager would sign off on the report before it would be entered into the NSR system.<sup>493</sup>

The concept behind the NSR system was sound: to provide a centralized database of information collected by CSIS from related investigations across Canada. While this system provided a potentially useful means for assessing all security intelligence gathered by CSIS's own investigations, its ultimate utility was limited, perhaps by the cumbersome technology of the day.

### **Compartmentalization**

Internal communications within CSIS were stifled by compartmentalization and secrecy. While CSIS collected a large quantity of information, communication was not free-flowing among investigators, analysts and senior management. This prevented CSIS from taking full advantage of the wealth of intelligence collected.

---

<sup>491</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3738.

<sup>492</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2529.

<sup>493</sup> Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3424-3425.

Compartmentalization existed between senior management and on-the-ground investigators, as well as among investigations across the country and even within a single investigation. This compartmentalization meant that one CSIS investigator might not necessarily know what another was working on. John Stevenson noted this point when comparing the differences between CSIS and the RCMP:

I'm coming from CSIS; I'm coming from a security intelligence background where the "need-to-know" principle is rigidly applied; where documents are stored properly; where investigators, work in fairly – close proximity to each other, [and] may not know what the other investigator is working on  
....<sup>494</sup>

This meant that access to intelligence was restricted, both within CT (Counterterrorism) and between CI (Counter-Intelligence) and CT investigations. This segregation within CSIS led to the possibility that CSIS would miss the opportunity to make relevant connections. The importance of open information sharing within CSIS is illustrated by the fact that key breakthroughs after the bombing were made by investigators outside of the BC Region. For example, the Windsor investigation did not result in any intelligence that could have prevented the bombing, but it had an effect on the subsequent investigation. There was a CSIS wiretap in place during the Windsor investigation. While reviewing the intercept material, Charlie Coghlin became aware of certain words and phrases that were commonly used as code. The realization that the same code words were being used in the Parmar intercepts was not made until months after the bombing, when Coghlin had been transferred to HQ to help with the analysis and was given access to the translators and transcriber logs for the Parmar intercept.<sup>495</sup>

The failure of CSIS HQ to appreciate the importance of Coghlin's finding, and to pass it on to investigations of Sikh extremist targets in other regions, resulted in a missed opportunity to share critical insight that might have enabled Kobzey to advance his investigation on Parmar.

This compartmentalization was the result of CSIS's adherence to the ill-considered and strict "need-to-know" principle and the fact that CSIS personnel operated within their own silos of responsibility.

### ***"Need-to-know" Principle***

Compartmentalization, based on the "need-to-know" principle, appears to have been widely and uncritically accepted within CSIS. In an interview with the BC Crown prior to the Reyat trial, Ayre stated:

---

<sup>494</sup> Testimony of John Stevenson, vol. 62, October 16, 2007, p. 7674.

<sup>495</sup> Exhibit P-101 CAA0308, CAA0309.

I think that it comes down to the fact that we are all very compartmentalized. We operate on a need to know basis [sic] and there are a lot of areas that are being talked about that were need to know and I didn't need to know about them.<sup>496</sup>

The “need-to-know” principle was cited as a key principle upon which the intelligence community operated.<sup>497</sup> It was a prevailing principle for the RCMP Security Service (SS), and subsequently CSIS, not only in dealing with outside agencies, but also within its own establishment.

In relation to sharing between HQ and the regions, HQ always claimed that it had the requisite need to know, in terms of what the regions were seeing and collecting (with the possible exception of the names of human sources), but the reverse was not always true. HQ did not always share information with the regions. Its decision on what to share, and what not to share, was based on its assessment of whether the investigator in the region had a need to know. A clear difficulty, not only with this asymmetrical relationship, but with the very concept of “need-to-know”, is the fact that it will almost always certainly lead to an inadequate information flow: because it is impossible to know completely what you need to know, if you are not deemed to have the “need-to-know” status that would allow you to evaluate the information in the first place.

Information within the NSR system was available to investigators, but if the information was considered sensitive it would trigger an alert to a user conducting a search that the information existed, but was accessible on a “need-to-know” basis only. To gain access, the IO could contact whoever had responsibility for the file to explain the need to access the information.<sup>498</sup>

This compartmentalization was one of the major deficiencies of the centralized, top-down organization at CSIS: investigators on the ground were denied access to CSIS information that was relevant to their investigations. Restrictions due to the “need-to-know” principle were often placed on information from foreign sources, including information collected by the Communications Security Establishment (CSE). HQ acted as the gatekeeper for foreign intelligence, reviewing all material, but not necessarily entering it into NSR, due to third party or secrecy concerns.<sup>499</sup> In its attempt to respect such concerns, HQ could withhold information from the regions.

Investigators, including Kobzey, appeared to accept the notion that HQ should be able to withhold information that could be relevant to their local investigations. Kobzey stated in testimony that he may not have had the necessary clearance level for information of a highly sensitive nature (such as that from CSE). He accepted that having “Top Secret” clearance would not automatically give him

<sup>496</sup> Exhibit P-101 CAD0183, p. 12.

<sup>497</sup> Testimony of Robert Chesney, vol. 83, November 26, 2007, p. 10729.

<sup>498</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3854-3855.

<sup>499</sup> Testimony of Chris Scowen, vol. 50, September 21, 2007, p. 6127.



access to everything; HQ would make a determination regarding whether he had the requisite need to know and, if not, HQ officials would assess the veracity of the information themselves, without the benefit of Kobzey's insight into the investigation.<sup>500</sup>

It is not clear, however, that HQ was best qualified to determine what information would be relevant to a given regional investigation, particularly in comparison to the judgment of the investigators themselves. HQ received summary reports from the regions that contained the intelligence that investigators found to be of obvious significance. Intelligence withheld by HQ might have provided a new context to trigger a different interpretation of an event originally perceived to be insignificant. This restriction on the sharing of information eliminated opportunities to make important connections, since information stayed within silos.

Secrecy and third party concerns could conceivably be relevant in terms of sharing information with other agencies, where these agencies might be subject to different requirements and mandates. However, it is difficult to understand why these concerns would exist within CSIS itself. Why did HQ feel that it could not share certain types of sensitive information with regional investigators working on the same file? All investigators were Top Secret cleared and the restriction of access to relevant information appears difficult to justify. The process was unduly restrictive and, as a result, generally ineffective in a service dedicated to acquiring and, in theory, sharing it. The "need-to-know" principle, as developed by CSIS, was a demonstrable mistake.

### ***Silos of Responsibility and Filtering of Information***

In 1984-1985, CSIS appeared to be an agency that was aware of the recommendations of the McDonald Commission to respect individual privacy rights. It was not accustomed to either the public spotlight or close political scrutiny. CSIS personnel attempted to perform their duties, but often without knowledge of all the information in CSIS's possession that was relevant to their investigations. The Osbaldeston report noted:

Within CSIS, we have observed a formal, hierarchical decision-making process that has tended to isolate the Director .... The compartmentalized CSIS management committee structure inhibits the accommodation of new or different points of view, does little to encourage effective communication within the Service, and does not provide a corporate level perspective to program priorities and resources. The Director must chair important internal management committees for his leadership to be manifest.<sup>501</sup>

---

<sup>500</sup> Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3854-3855.

<sup>501</sup> Exhibit P-101 CAA0569, p. 17.

This isolation of roles and the filtering of information began at the lower levels of the organization. Investigators briefed Physical Surveillance Units (PSU), translators and transcribers only on the key points of an investigation. However, the PSU, the translators and the transcribers were ultimately responsible for making relevant observations, while investigators reviewed reports and summaries of the information collected.

An example of problems with this approach can be seen around the Duncan Blast incident.<sup>502</sup> The PSU surveillant noted the phone number dialed by Parmar during the ferry ride to Nanaimo, and understood he was calling a “Singh.” The Unit looked in the Duncan phone book and noted the one “Singh” listed there, despite the fact that his number did not match what the surveillant believed she saw Parmar dial while on the ferry. The PSU personnel seemingly were unaware that all Sikh males had the middle or last name Singh. The BC investigator received the PSU report, and drafted a report to be distributed to CSIS HQ and the RCMP. This summary report contained only the phone book number of “Singh,” but not the number observed by the PSU surveillant on the ferry. After the bombing, the RCMP asked to see the underlying PSU report, but CSIS initially denied access on the basis that the summary report would be sufficient. CSIS eventually released the underlying PSU report to the RCMP, at which point it was realized that the number first observed by the PSU surveillant was that of Inderjit Singh Reyat. The lost detail in the investigator’s summary report delayed this important finding for months. In fact, this may have never been discovered had the RCMP not gone back to review the original PSU report.

Another example of harmful filtering of information was the process set up for translating and transcribing intercepts, such as those recorded on Parmar. Investigators received intercept reports that consisted mainly of paraphrased, rather than verbatim, translations, a practice that CSIS senior management noted made these reports of little use as key intelligence information.<sup>503</sup>

### ***Note-Taking Policies and Practices***

The failure to appreciate the importance of reviewing raw information extended to the note-taking practices of the IOs. Kobzey testified that he would often take notes during an interview, if the interviewee permitted him to do so. However, after completing the summary report for submission into the NSR system, he would shred the notes, according to policy.<sup>504</sup> Evaluation of the handwritten notes in comparison with the intelligence report was, of course, made impossible by the destruction of the notes. It is difficult to determine which details might have been omitted or altered, or written with different emphasis.

While, generally, the regional investigators provided briefings to the PSU and intelligence monitors, they failed to appreciate the importance of maintaining

<sup>502</sup> See Section 1.4 (Pre-bombing), Duncan Blast.

<sup>503</sup> Exhibit P-101 CAF0818, p. 2.

<sup>504</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3738.

the raw, initial reports. The importance of these reports became most apparent after the bombing, when the opportunity to review the raw information, especially the intercept tapes, from a new perspective would have been valuable. The destruction of raw information and the lack of communication between CSIS personnel resulted in lost opportunities to connect the dots and to gain maximum benefit from the collected intelligence.

### **3.3.6 Lack of Meaningful Threat Assessments**

#### ***Lack of Coordination: Intelligence for Intelligence's Sake***

A major deficiency in CSIS's analysis efforts was the fact that the Sikh Desk, effectively the "analysis centre" for threats to Indian interests, performed its analysis functions in isolation. Analysts never "brainstormed" with other involved agencies to pool their knowledge on the Sikh extremist threat and to understand the range of available responsive actions. Instead, Sikh Desk TAs (Threat Assessments) were based on the skill of individual analysts with little expertise in Sikh extremist issues and no personal, on-the-ground insight. No mechanism was in place to take advantage of the depth of knowledge and analytical skills across government agencies to enable them to collaborate with the Sikh Desk or challenge its TAs.

The purpose of CSIS TAs was to provide relevant intelligence to allow other government agencies and ministers to determine appropriate operational policies and responses. CSIS was deliberately not given enforcement powers. Thus, CSIS's main role in the government's counterterrorism efforts was to provide timely and relevant advice to the government through its threat assessment product.

After reviewing CSIS's TA process as it stood in 1985, the Commission is left with the impression that intelligence was being produced for intelligence's sake. CSIS's intelligence product was insufficiently tailored to the needs of its client agencies, and it was produced with little input from those clients. Instead CSIS unilaterally determined the scope of tasking, collection, analysis and dissemination of its product. CSIS could determine if information, although relevant, should be left out of the assessment product because of secrecy concerns or for other reasons. This resulted in the production of general assessments that, at times, lacked the precision and detail necessary to allow other agencies to develop an appropriate response.

The 1987 Osbaldeston Report surveyed consumers of CSIS TAs and noted:

The consensus of this group was that CSIS operational intelligence is of high quality, but that there is not enough of it. Some of our interlocutors stated that CSIS did not seem aware of what sorts of operational intelligence might be of interest to its consumers. This was attributed to a lack of understanding

of the needs of the rest of Government on the part of CSIS and many of its analysts. On the other hand, intelligence consumers must tell CSIS what they want.<sup>505</sup>

As noted by the Osbaldeston Report, the failure to ensure meaningful TAs was not attributable solely to CSIS. It appears that the intelligence consumers did not provide direct feedback about the utility of the intelligence product. Admittedly, these consumers were hampered in their ability to assess the intelligence product, as they were often not aware of any underlying information available to CSIS that had not been disclosed in the TA. Rather than addressing deficiencies in the TA product, consumers like the RCMP simply came to expect little utility from the TAs and began to advocate developing intelligence capabilities of their own.<sup>506</sup> Major criticisms of the TAs generally occurred at high levels after the fact. Personnel across government agencies dealing with the Sikh extremism investigation failed to work together to improve the TA product on an informal and daily basis.

CSIS assessments tended to be general, consisting of a description of the general threat environment and a simple designation of the threat level as “high”, “medium” or “low”. Rarely included were details about the nature of the threats, speculative information regarding the range of possible threats, an estimate of the likelihood of harm or any possible consequences.<sup>507</sup> CSIS TAs purposely would not contain suggestions regarding the appropriate response, as this was felt to be a decision within the sole jurisdiction of the RCMP and other protective agencies.<sup>508</sup>

### ***Lack of Meaningful Threat Levels***

As indicated, CSIS TAs classified the threat level according to three broad categories: high, medium and low. Agencies responsible for protective response to threats were expected to set operational responses on the basis of these general threat assessment levels.

The threat level to Indian interests consistently remained “high” for the year prior to the Air India and Narita bombings, beginning with the June 1984 storming of the Golden Temple. Effectively, the RCMP P Directorate was responsible for adjusting its response in the face of a consistently high general threat.<sup>509</sup>

It is unclear whether there was any agreed view of how CSIS threat levels related to a recommended operational response by the RCMP. John Henry, Head of the Threat Assessment Unit (TAU) at CSIS HQ, testified to his understanding of the

<sup>505</sup> Exhibit P-101 CAA0569, p. 19.

<sup>506</sup> Exhibit P-391, document 210 (Public Production # 3343): RCMP response on July 31, 1985 to an early draft of the Seaborn Report, “ICSI Review of Counter-Terrorism Measures Respecting Airport/Airline Security” [RCMP Response to Draft Seaborn Report].

<sup>507</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2543.

<sup>508</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2543-2544.

<sup>509</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2555.

threat levels: when the threat was rated as high, it meant that one should be extra vigilant and prepared for anything.<sup>510</sup> It is difficult to understand how this “be prepared for anything” guidance was helpful to the RCMP in formulating an effective and targeted threat response.

Henry sympathized with the RCMP P Directorate’s frustration about the lack of specificity in the CSIS TAs. He admitted that, in general, all CSIS could provide was an assessment that stated, “[t]he general threat is high, but we have nothing specific.”<sup>511</sup>

CSIS did not undertake to better understand the RCMP’s methodology concerning threat responses or to design its TAs to correspond to the RCMP’s operations. There was a lack of recognition on the part of both the RCMP and CSIS of the need to translate threat levels into something corresponding to a more specific range of operational responses by the RCMP.

This deficiency was noted in a review of the failures in the TA process that allowed Armenian terrorists successfully to seize the Turkish Embassy in March 1985. The Canadian government undertook an interdepartmental review of the incident and concluded that CSIS, in cooperation with other relevant government agencies, should develop standard threat levels for its TA products.<sup>512</sup>

The review has also identified a need, in the preparation of threat assessments, to define in standard and precise terminology various terrorist threat levels or “thresholds” in terms of their seriousness. This would allow a more responsive implementation of precautionary measures by responsible agencies.<sup>513</sup>

This deficiency was not dealt with prior to the attack on Air India Flight 182, nor did the agencies do anything, in light of that conclusion, to try to ameliorate the problem on an informal basis until a broader review could take place.

### ***Lack of Threat Details***

TAs issued by CSIS in the period leading up to the Air India and Narita bombings lacked specifics and failed to probe alternative threat scenarios, especially when it came to the possibility of terrorist bomb attacks against Air India flights.

This deficiency was noted in the 1992 Security Intelligence Review Committee (SIRC) Report:

Many of the assessments contained little more than a statement that the threat level against Indian Government

---

<sup>510</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2543.

<sup>511</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2512.

<sup>512</sup> Exhibit P-101 CAF0063. The report entitled “Review of Federal Counter-Terrorism Arrangements” was prepared with the participation of the Solicitor General’s office, External Affairs, National Defence, the Privy Council Office and the Department of Justice.

<sup>513</sup> Exhibit P-101 CAF0063, p. 4.

interests remained high. We noticed that the assessments which mentioned Air India showed little sign of analysis leading to more detailed assessment of the form any attack might take.<sup>514</sup>

Details regarding the nature of the expected threat could be critical for the RCMP to tailor the appropriate response. It is clear that the appropriate response for a hijacking threat would differ from that for a bombing threat. It is also clear that details about the expected target and potential suspects would allow the RCMP to focus their response to address the areas of highest threat. In spite of this, CSIS often left out details regarding the expected targets, type of threat and possible suspects.

### ***Targets: Threats Related to Air India***

Sikh Desk TAs generally related to “threats to Indian missions and personnel”, a term that was intended to include Air India.<sup>515</sup> However, this inclusion was explicitly clarified for the first time in an early June 1985 TA<sup>516</sup> in response to an RCMP request for a specific TA on Air India. The fact that the RCMP requested a specific TA on Air India indicates that the RCMP did not necessarily consider that any threats to Indian missions might pertain to Air India as well.

This clarification was particularly relevant in light of the fact that the P Directorate consisted of two separate branches: VIP Security and Airport Policing. CSIS sent the TAs to the P Directorate, which was responsible for disseminating the TAs within the RCMP. Threat details were critical to ensure that the P Directorate brought the TAs to the attention of the appropriate RCMP departments.

However, CSIS did not appear to appreciate fully the division of responsibility within the RCMP and the need for threat details to facilitate the P Directorate’s dissemination efforts. Since all threats to Indian missions were meant to include Air India, all TAs related to threats to Indian missions should have clearly indicated the need for them to be passed to the Airport Policing Branch. The TAU within CSIS failed to ensure that this occurred. Henry would generally copy both Airport Policing and VIP Security on TAs dealing with threats to aviation security. However, the TAU often failed to copy Airport Policing on general TAs<sup>517</sup> regarding threats to Indian interests, including those issued in the critical month before the bombing, even though these threats were clearly applicable to Air India.

---

<sup>514</sup> Exhibit P-101 CAB0902: 1992 SIRC Report, p. 27.

<sup>515</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2513-2514.

<sup>516</sup> Exhibit P-101 CAA0194.

<sup>517</sup> See, for example, Exhibit P-101 CAB0218, which is a threat assessment regarding the April 13, 1985 threat to an incoming Air India flight. See also Exhibit P-101 CAB0071, which was copied to both VIP Security and Airport Policing.

***Nature of Threat: Hijacking or Bombing***

CSIS failed to provide details about the expected nature of threats in its TAs. It is clear that the RCMP would need to respond differently to counter hijackings versus bombing threats.

Burgoyne, the key CSIS analyst on the Sikh Desk, testified that the Desk did not differentiate between hijacking and bombing threats in its assessments.<sup>518</sup> Henry's testimony indicated that terminology used in the threat assessment could be ambiguous. He testified that "sabotage" could mean a wide range of things:

I refer to sabotage as damage. Damage could be puncturing the skin of the airplane, like with a truck. I've seen it happen. Slashing the tires so that it'll have difficulty as you crash on landing, a bomb, yes, there's sabotage. Even as the air crew go through the lobby, slipping tranquilizer pills into their say, coffee. The range is as far as your imagination can go.<sup>519</sup>

Henry's comment reflects the attitude that responding agencies should be prepared for anything. The lack of precision in the language of the assessments did not appear to be a major concern for CSIS, as it seemed content to issue general assessments of the expected threat. This overly cautious approach inevitably hampered the RCMP's ability to tailor the most effective response to the threat.

***Suspects: Names of Suspected Sikh Extremists***

TAs would rarely include names of Sikh extremists under investigation by CSIS, even in the face of direct requests from the RCMP for information on certain persons. Burgoyne testified to his understanding of the importance of details regarding suspects during the Inquiry hearings.

I think it's important that we find who's behind the threat, what is that person capable of doing ... what method may that person employ. So whether you are a martyr, a marksman or explosives expert, I think this is the information that we have to try and gather on the person who is behind the threat.<sup>520</sup>

Despite this recognition of the importance of identifying suspected perpetrators, CSIS commonly issued TAs lacking any such detail.

---

<sup>518</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3454.

<sup>519</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2552.

<sup>520</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, pp. 3453-3454.



On June 21, 1984, the RCMP requested a TA and enclosed a list of names of alleged members of the Babbar Khalsa (BK), including Parmar and Gill.<sup>521</sup> At the time, the RCMP Security Service (SS) knew that Indian officials had claimed that Parmar was the leader of a terrorist section of the Khalistan movement and had been the subject of an extradition request by the Indian government for the alleged murder of two policemen in India.<sup>522</sup> The GOI had also specifically identified Parmar as a threat to the safety of Prime Minister Indira Gandhi during her 1982 visit to the US. The RCMP SS knew that Gill had identified himself as the Vancouver Khalistan "Consul General," was a personal acquaintance of leaders of other international Sikh extremist groups, and was present at a 1982 egg-throwing incident staged against the Indian High Commissioner.<sup>523</sup> While the RCMP SS had passed on this information to VIP Security in 1982, it did not include the information in its noticeably vague responding TA on June 21, 1984, which simply stated that:

All of these persons are supporters to varying degrees of greater political autonomy and religious freedom for Sikhs in India. Some are Sikh community and Spiritual leaders in Canada. Others are advocates of an independent Punjab and provide financial and moral support to those professing to represent the Government of Khalistan in exile.<sup>524</sup>

On September 6, 1984, the Sikh Desk issued a TA to provide an updated synopsis of the Sikh situation in Canada.<sup>525</sup> It stated that:

It is the radical groups, often advocates of Khalistan, that constitute the greatest danger and create the largest risk factor for Indian diplomatic premises and personnel. Elements within this group have expressed support for acts of terrorism in India and some may have ties to terrorist groups there.

However, the TA failed to provide any descriptions of the "radical groups," descriptions which would have assisted the RCMP in better focusing its response to the "high" threat.

Meanwhile, about five weeks earlier, on July 31, 1984, the Sikh Desk had reported detailed information about Parmar internally within CSIS.<sup>526</sup> This detailed information on Parmar was finally released to the RCMP on October 26, 1984, along with information about Bagri and Gill. CSIS noted that it "...continues to assess the threat as high as [*sic*] result of the actions of the individuals mentioned."<sup>527</sup>

---

521 Exhibit P-101 CAB0079, pp. 2-3.

522 Exhibit P-101 CAB0042 (May 7, 1982), CAB0031 (July 28, 1982).

523 Exhibit P-101 CAB0031 (July 28, 1982).

524 Exhibit P-101 CAB0085.

525 Exhibit P-101 CAA0093, p. 2.

526 Exhibit P-101 CAB0114.

527 Exhibit P-101 CAA0105.

The hesitancy to pass on specific names was likely due to a perceived need to protect individual privacy and the secrecy of CSIS's own investigations. TAs that contained information about individuals would include a comment to the effect that information which might affect Canadian citizens or permanent residents should be referred to senior level management, who would then manage potential dissemination to Indian authorities.<sup>528</sup> CSIS was acutely aware of the need to protect privacy rights, to the detriment of its information-sharing practices with the RCMP.

### **The RCMP Perspective on CSIS Threat Assessments**

The RCMP expressed dissatisfaction with the general nature of CSIS TAs in the immediate aftermath of the Air India and Narita bombings. In July 1985, the RCMP characterized the information received from CSIS in the year prior to the bombing as mainly providing a general historical and political overview, rather than any "concrete intelligence."

The CSIS did not forewarn us and to this point in time they have not been able to provide any concrete intelligence or information that has assisted our investigation since the mishaps. They have provided a historical and political perspective which the RCMP was cognizant of due to the many protective operations it had to engage in involving Indian diplomats and associated criminal investigations following attacks on them or Indian missions over the course of the past year in Vancouver, Winnipeg and Toronto.<sup>529</sup>

Because of its constant concern about proper resource allocation, the RCMP often requested updated TAs from CSIS to ensure that the level of protection was still required. Even in the critical month of June 1985, the RCMP was eager to reduce the resources assigned to the protection of Indian interests. On June 11, 1985, the RCMP noted that the "high threat levels" in the CSIS TAs had resulted in the deployment of a considerable number of RCMP resources. The RCMP TA request sent on that date stated that if the Gandhi visit occurred without serious incident, it was assumed that the threat level would diminish.<sup>530</sup> The RCMP appears to have been implicitly pressuring CSIS either to provide some evidence of the continuously high threat or to reduce the threat level in its analysis.

The RCMP was not content to rely on CSIS TAs as the main source of security intelligence upon which to design its responses, in part because of its dissatisfaction with the CSIS information and assessments. In July 1985, the RCMP reported that, although it had relied on CSIS to provide valuable details on threats, it felt that the information provided was not adequate to inform its threat responses effectively.

---

<sup>528</sup> Exhibit P-101 CAB0085, p. 2.

<sup>529</sup> Exhibit P-391, document 210 (Public Production # 3343): RCMP Response to Draft Seaborn Report.

<sup>530</sup> Exhibit P-101 CAB0275.

A vacuum has been created following the separation of the Security Service from the RCMP with respect to valuable street-level criminal/dissident/terrorist and law enforcement intelligence because of a lack of essential contacts, sources and informants within the various ethnic communities. The Force has had to rely on CSIS for this kind of information which has not been effective to date in countering terrorist acts.<sup>531</sup>

After the creation of CSIS, the RCMP developed its own parallel TA process.<sup>532</sup>

### ***Interdepartmental Threat Assessments***

The usefulness of CSIS TAs could likely have been improved by an interdepartmental review of the TA product. However, in 1985, CSIS TAs were developed on the basis of CSIS insight alone, despite the fact that various other agencies relied upon the product to make critical operational and policy decisions. CSIS's ability to provide meaningful TAs was impaired by a lack of consultation with its client agencies, particularly the RCMP.

The Sikh Desk, the analysis centre for TAs on Sikh extremist threats, had no direct contact with its major client, the RCMP P Directorate.<sup>533</sup> All TA requests and responding assessments were sent through the CSIS TAU.<sup>534</sup> No mechanism existed for Sikh Desk analysts to engage with the P Directorate for an evaluation of its TAs. Burgoyne testified that he was unaware of how the P Directorate would respond to the TAs, but assumed that it would contact the Sikh Desk for clarifications if necessary.

Well, not having had contact with "P" Directorate if there was a problem with the interpretation – of our assessment, perhaps, they would have asked – can we be a little bit more clearer, or is there anything else that we can provide them with, to better assess. Although, I do think our assessments were quite accurate based on the information we had at the time. So how they would react to this, I really can't say.<sup>535</sup>

At the Inquiry hearings, Burgoyne did not recall any instance where the P Directorate asked for clarification about a threat assessment from the Sikh Desk.<sup>536</sup>

The P Directorate did maintain direct contact with the TAU at CSIS. Henry admitted that the TAU did not follow up to determine whether the consumer

<sup>531</sup> Exhibit P-391, document 210 (Public Production # 3343): RCMP Response to Draft Seaborn Report.

<sup>532</sup> See Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

<sup>533</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3444; Testimony of Glen Gartshore, vol. 31, May 22, 2007, pp. 3549-3550.

<sup>534</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3444.

<sup>535</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3453.

<sup>536</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3453.

agencies found CSIS product to be of any use. The TAU acted purely as a liaison centre and did not develop any capability to provide added value to the TAs. Henry had limited knowledge of the operations of the RCMP units that relied upon the CSIS TAs. He felt he had a good liaison relationship with VIP Security, in that there was often dialogue about the TAs. However, he was not familiar with the operations of the Airport Policing Branch, which was notably the branch responsible for responding to threats to Air India.<sup>537</sup>

Henry was also unaware of the process by which the Sikh Desk drafted the TAs.<sup>538</sup> He testified that he “hoped” that the receiving agencies would take the CSIS TA and draw on its own sources of information to develop an operational plan.

What is striking about the relationship between CSIS and the RCMP is that there was virtually no dialogue between them. Given the general nature of some of the TAs, one would have thought that the RCMP would have followed up with CSIS to get more information. It is as if each agency assumed the other understood the situation at hand when in fact, at times, neither did. Instead, each appeared to have chosen to duplicate efforts, rather than trust the other to carry out its separate role.

#### ***Early Efforts to Create an Interdepartmental Threat Assessment***

The clear need for an interdepartmental system of intelligence assessment was recognized in the review of the March 1985 Turkish Embassy incident. The review report recommended that:

[A]n interdepartmental system be established, with CSIS as the focal point, for the preparation of comprehensive terrorist threat assessments, and for regular consultation between appropriate intelligence and security components – CSIS, DEA, RCMP, CSE and as necessary, CEIC, DOT and DND.<sup>539</sup>

In late May 1985, James Bartleman of External Affairs formed the *ad hoc* Interdepartmental Working Group on Sikh Extremism, in recognition of the need for increased coordination to assess and respond to the “crescendo” of threats to Indian interests at the time. Efforts at international coordination were also initiated, as government officials from DEA, CSIS, RCMP and the Solicitor General’s office attended a tripartite meeting on Sikh extremism in Washington in the week prior to the bombing.<sup>540</sup>

In the month before the bombing, CSIS began distributing TAs related to threats to Indian interests more widely. Rather than forwarding TAs to the P Directorate for further dissemination, CSIS sent its TAs directly to VIP Security, NCIB, Solicitor

<sup>537</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2511-2512, 2543, 2555.

<sup>538</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2542.

<sup>539</sup> Exhibit P-101 CAF0623, p. 2.

<sup>540</sup> Exhibit P-101 CAB0289, p. 3.

General, PCO, DND, DEA, CSE, Transport Canada, Immigration Canada, Customs, and all CSIS regions, districts and liaison officers stationed abroad.<sup>541</sup>

These efforts toward increased interdepartmental coordination of the threat assessment might have helped to produce more meaningful TAs and enhanced interdepartmental cooperation. Unfortunately these efforts were far too late to prevent the Air India and Narita bombings.

### **3.4 Deficiencies in RCMP Threat Assessment Structure and Process**

#### **Introduction**

Prior to the creation of CSIS, the RCMP Security Service collected security intelligence and provided threat assessments to the RCMP units in charge of implementing protective measures. The assessments issued by the Security Service contained relevant information about potential threats as well as an analysis of the level of the threat to assist in determining the appropriate security response. The RCMP did not otherwise carry out threat assessment functions as part of its policing operations, though it did have some units gathering criminal intelligence. When CSIS was created, the new agency took over the duties previously carried out by the Security Service, including the dissemination of threat assessments to Protective Policing. However, the RCMP decided to produce its own threat assessments also, while continuing to receive those from CSIS.<sup>542</sup> Hence, a new threat assessment process was put in place by the RCMP.

Unfortunately, the RCMP threat assessment process was not efficient in gathering and/or analyzing threat information centrally and, at times, interfered with the process in place at CSIS. The RCMP devoted significant resources to gathering and transmitting information that CSIS was already providing to Protective Policing. However, the RCMP was unable to address existing gaps in the threat assessment process by bringing into it the information to which it had unique access or even the information already in its possession. Relevant information was not always recognized or was not reported in a timely manner, and the RCMP often had difficulty appreciating the significance of the information or the seriousness of the threat.

#### **Threat Assessment and the RCMP Mandate**

##### ***Government Policy***

The official Government position in 1984 was that the responsibility for the collection and assessment of intelligence about threats to the security of Canada was assigned to CSIS, while the RCMP would remain responsible for protective policing and enforcement duties in connection with criminal

<sup>541</sup> Exhibit P-101 CAA0187 (June 6, 1985 TA), CAA0220 (June, 17 1985 TA).

<sup>542</sup> Exhibit P-101 CAA0039(i), p. 51, CAC0275, p. 2, CAC0495, p. 4.

offences related to security threats.<sup>543</sup> The same legislation that created CSIS specified a mandate for the RCMP in the area of “security offences”, giving the RCMP primary responsibility to perform peace officer duties in connection with criminal offences arising “...out of conduct constituting a threat to the security of Canada” or targeting “internationally protected person[s].”<sup>544</sup>

In the Government’s attempt to effect a surgical division of mandates between CSIS and the RCMP,<sup>545</sup> it was envisioned that the “security intelligence” mandate and resources would be transferred from the RCMP SS to CSIS, which would then have “...the responsibility and the capability to supply the RCMP with security intelligence it requires to meet its security enforcement and security protection responsibilities.”<sup>546</sup> The RCMP was expected to rely on CSIS for intelligence relevant to protective policing operations and security offences investigations. In terms of threat assessment, this would mean that CSIS would investigate and provide the threat information to the RCMP, which would then be responsible for taking appropriate protective action and which could also use the information to conduct its criminal investigation should a security offence be committed.

A Guideline was approved by the Minister about the appropriate role, policies, administrative arrangements and resource allocation which should guide the RCMP in the discharge of its security-related responsibilities. The Guideline recognized some potential overlap and duplication between “security intelligence” and “security enforcement” investigations, but took a narrow view of the RCMP’s role in collecting information about security offences. The RCMP was expected to take action only in investigating and gathering evidence where it was apparent or likely that a security offence had been or was about to be committed. In cases where there was only a possibility that threats could give rise to security offences, the RCMP was expected to rely on CSIS to provide relevant intelligence information.<sup>547</sup>

Recognizing that the RCMP would likely produce or acquire information related to security threats in the course of carrying out its policing duties, the Guideline instructed the Force to pass this information on to CSIS so that CSIS would be in receipt of all security intelligence relevant to its mandate.<sup>548</sup> The RCMP Commissioner was authorized to establish dedicated units with no investigative or operational mandate for the purpose of liaison with CSIS.<sup>549</sup> The role of these units was to be limited to sharing information with CSIS and consulting on cases requiring enforcement or protective action,<sup>550</sup> while the actual protective

<sup>543</sup> The information in this section comes from Exhibit P-101 CAA0081, pp. 2-15.

<sup>544</sup> Exhibit P-107: *Security Offences Act*, S.C. 1984, c. 21, ss. 57, 61. See also Section 3.0 (Pre-bombing), *The CSIS Act*.

<sup>545</sup> See discussion on the McDonald Commission in Section 2.1 (Pre-bombing), *The Civilianization of Security Services*.

<sup>546</sup> Exhibit P-101 CAA0081, p. 8.

<sup>547</sup> Exhibit P-101 CAA0081, p. 13.

<sup>548</sup> Exhibit P-101 CAA0081, pp. 9-10. See also the recommendation at p. 15, that the RCMP pass to CSIS information relevant to the CSIS mandate.

<sup>549</sup> Exhibit P-101 CAA0081, pp. 3, 16.

<sup>550</sup> Exhibit P-101 CAA0081, p. 16.

and security offences investigations work would continue to be carried out by existing RCMP units.<sup>551</sup> The creation of the new units was said to require only a “small level of resources” immediately.<sup>552</sup>

While not directly addressed in the Guideline, it is clear that the Government contemplated that CSIS would be in charge not only of collecting but also of analyzing all information relevant to national security threats in order to advise other agencies, including the RCMP, of the nature and seriousness of the threats. Hence, the RCMP had to provide the threat information it acquired to CSIS so that it could be centrally analyzed and so that the overall threat could be assessed by CSIS. The role contemplated for the RCMP in the threat assessment process was minimal, at most.

### **Creation of RCMP Threat Assessment Process**

As mentioned, when CSIS was created, the RCMP decided that, since the threat assessment functions previously carried out by its Security Service would now be transferred to CSIS, the Force needed to create its own threat assessment process.<sup>553</sup>

The RCMP never viewed intelligence-gathering activities relating to terrorism or other security-related crimes as being excluded from its mandate, and consequently believed that it needed to maintain an intelligence function, in particular for the gathering of “criminal intelligence.”<sup>554</sup> To the RCMP, intelligence-gathering activities and involvement in threat assessment were part of the Force’s mandate to detect and prevent crime, and were made necessary by the Force’s protective policing duties, as well as by the “expanded” law enforcement responsibilities it was assigned in the *Security Offences Act*.<sup>555</sup>

According to former RCMP Commissioner Robert Simmonds, in order for the RCMP to carry out its crime prevention duties with respect to terrorism, it was necessary for the Force to gather non-offence-specific criminal intelligence. The mandate to intervene where the commission of an offence was anticipated, as opposed to completed, was said to require police, at times, to initiate investigations in advance of criminal conduct.<sup>556</sup> By getting actively involved early on, through “intelligence-led policing,” the RCMP could take steps to prevent breaches of peace, to maintain public order or to stop criminal acts before the fact.<sup>557</sup>

---

<sup>551</sup> Exhibit P-101 CAA0081, pp. 11, 14.

<sup>552</sup> Exhibit P-101 CAA0081, p. 14.

<sup>553</sup> Exhibit P-101 CAC0275, p. 2, CAC0495, p. 4; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5439-5440.

<sup>554</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1665; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5423-5424, 5428-5429.

<sup>555</sup> Exhibit P-101 CAC0283, pp. 4-5, CAC0406, p. 3, CAC0495, p. 5.

<sup>556</sup> Exhibit P-101 CAA0474.

<sup>557</sup> Exhibit P-101 CAA0474, p. 10; Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1659-1660; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5359-5360.



The RCMP believed it could not rely solely on CSIS for relevant threat information and intelligence as it had done previously with the Security Service.<sup>558</sup> CSIS information was described as relevant to threat assessments mostly "...in areas that fall within the CSIS mandate."<sup>559</sup> The RCMP did not believe that the intelligence gathered by CSIS would encompass all the issues that were potentially relevant to its responsibilities.<sup>560</sup> This belief was related to actual or perceived limits on the CSIS mandate and to the RCMP's perception of the choices made by CSIS about the type of intelligence probes it would be conducting. For example, the activities formerly carried out by the Security Service to gather intelligence on domestic groups who could present a security threat<sup>561</sup> were viewed by the RCMP as particularly relevant to its mandate.<sup>562</sup> Deputy Commissioner Henry Jensen testified that the RCMP needed intelligence about dissident groups and organizations ("public order intelligence") in order to conduct its protective policing operations.<sup>563</sup> This was the type of information that CSIS could collect "...if they committed the resources to it and went out to the field" but, according to Jensen, "...they were not doing it", so the RCMP had to "...complet[e] the loop."<sup>564</sup>

Simmonds, for his part, spoke of the "high degree of frustration" experienced by the RCMP in its day-to-day operations because of the "...difficulty we were having in getting meaningful daily information from CSIS."<sup>565</sup> He also expressed concern about the use the RCMP could make of the information CSIS collected.<sup>566</sup> It was felt that by engaging in intelligence-gathering related to terrorism, the Force would be better able to carry out its mandate to acquire the evidence necessary to prove any terrorism offences that did take place.<sup>567</sup>

Though Simmonds noted in testimony before the Inquiry that he personally never doubted CSIS's competence,<sup>568</sup> there may have existed within the RCMP a certain lack of confidence in CSIS's abilities. In April 1985, the Commanding Officer of the RCMP H Division noted that "...in some quarters, the RCMP felt they could not rely on CSIS."<sup>569</sup> In his view, the RCMP would not be able to "...know that CSIS had done their work right" if it did not control the operations.<sup>570</sup> As late as 1987, following a National Security Enforcement conference, an RCMP officer asked the CSIS Nova Scotia Chief how "certain" CSIS could be of its threat assessments.<sup>571</sup>

---

558 Exhibit P-101 CAC0406, p. 3

559 Exhibit P-101 CAC0283, p. 5.

560 See Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5457, indicating that the RCMP concerns mostly related to the "completeness" of the information provided by CSIS.

561 See, generally, Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1630-1633.

562 Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1632-1633.

563 Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5396, 5439-5440; Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1632-1633, 1661.

564 Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5440.

565 Testimony of Robert Simmonds, vol. 74, November 8, 2007, p. 9341.

566 Testimony of Robert Simmonds, vol. 74, November 8, 2007, p. 9347.

567 Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5372. See also Exhibit P-101 CAC0030, p. 4, where Simmonds describes counterterrorism as the area of common interest between CSIS and the RCMP and the one area where information sharing was necessary.

568 Testimony of Robert Simmonds, vol. 74, November 8, 2007, p. 9347.

569 Exhibit P-101 CAA0144, p. 1.

570 Exhibit P-101 CAA0144, p. 1.

571 Exhibit P-101 CAA0531.

For these reasons, a process was put in place at the RCMP for the central collection of threat information in order to advise Protective Policing about the threats. The RCMP undertook not only to collect and transmit to Protective Policing the threat information already in the Force's possession, but also to actively seek out information relevant to its new threat assessment process.<sup>572</sup> The RCMP planned to use every possible avenue to obtain "suspected and known criminal intelligence" about terrorism and extremism in Canada.<sup>573</sup> For this purpose, units were tasked with reviewing open sources of information, like magazines, newspapers and local publications, to look for information about possible law enforcement matters and to identify individuals or organizations with a potential for violence directed at public figures.<sup>574</sup> RCMP Foreign Liaison Officers were asked to obtain national security "criminal information" that might impact on Canada from foreign police forces.<sup>575</sup> The RCMP also decided to conduct follow-up investigations about threat information.<sup>576</sup> A 1985 draft Guideline on National Security Enforcement and Liaison provided that investigations or "preventative action," targeting individuals or groups who advocated violence, supported criminal activity, or indicated an apparent intent to engage in unlawful activity, could be engaged in where a statement, activity, or action would constitute a threat or cause harm to the security of Canada.<sup>577</sup>

### ***RCMP Threat Assessment Structure***

The National Criminal Intelligence Branch (NCIB) was an RCMP Headquarters (HQ) branch which existed within the structure of the RCMP criminal operations side prior to the creation of CSIS, reporting directly to the Director of Criminal Investigations.<sup>578</sup> NCIB was a unit with no operational or investigative capacity, which was responsible for coordinating intelligence-gathering on criminal activities and criminal organizations.<sup>579</sup> Within each Division, a National Criminal Intelligence Section (NCIS) was in charge of gathering intelligence on major criminal activities. The NCIS had investigative capacity and acted as the operational arms of NCIB, though they did not report directly to NCIB. NCIB and the divisional NCISs were created in the 1960s.<sup>580</sup> Their focus at the time was specifically on organized crime<sup>581</sup> but, by the 1980s, NCIS also had responsibilities for gathering intelligence about planned or suspected "criminal extremist/terrorist activities."<sup>582</sup>

After the creation of CSIS, a National Security Enforcement (NSE) Section responsible for intelligence coordination and sharing with CSIS, particularly for information about political terrorism, was added within NCIB.<sup>583</sup> NCIB NSE

<sup>572</sup> Exhibit P-101 CAC0283, p. 5.

<sup>573</sup> Exhibit P-101 CAC0286, p. 2.

<sup>574</sup> Exhibit P-101 CAA0039(i), p. 19, CAC0283, pp. 6-7, CAC0495, pp. 4-5.

<sup>575</sup> Exhibit P-101 CAC0286, p. 2.

<sup>576</sup> Exhibit P-101 CAC0283, p. 6.

<sup>577</sup> Exhibit P-101 CAA0039(i), p. 18.

<sup>578</sup> Exhibit P-110; Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1642-1644.

<sup>579</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2565-2566.

<sup>580</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5358.

<sup>581</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5358.

<sup>582</sup> Exhibit P-101 CAC0495, p. 3.

<sup>583</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1644; Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2560.

members were instructed to review and disseminate RCMP information about extremism and threats to the security of Canada.<sup>584</sup> Their role was essentially to "...monitor the situation across Canada."<sup>585</sup> They were tasked with liaison functions with CSIS and were also responsible for conducting records checks for individuals appointed to various government positions, which consumed a significant amount of their time.<sup>586</sup> NSE units were also added within most divisional NCIS sections.<sup>587</sup> Their main function was to serve as a liaison facility "...for collecting criminal intelligence information relating to national security between the RCMP and CSIS, as well as other Agencies."<sup>588</sup>

In addition to its liaison functions, the NSE Section at NCIB was put in charge of the new RCMP threat assessment functions.<sup>589</sup> According to the process put in place, the RCMP Protective Policing Directorate (P Directorate), which was responsible for VIP Security and Airport Policing, was to request threat assessments from both CSIS and NCIB NSE.<sup>590</sup> NCIB NSE was to pass on requests to divisional NCIS NSE units which would then contact other RCMP units in their division, as well as other agencies such as local police forces, to gather intelligence.<sup>591</sup> The divisional units were also expected to review open sources materials and identify relevant information.<sup>592</sup> The information gathered would then be reported back to NCIB, where a member of the NSE Section would review it, conduct file research and records checks, and then prepare a threat assessment for P Directorate.<sup>593</sup>

The ministerial Guideline continued to govern the scope of the RCMP's "... appropriate role, policies, administrative arrangements and resource allocation" for its security-related responsibilities. The NSE Section at NCIB and the NSE units at NCIS were created pursuant to the Guideline as the dedicated liaison units.<sup>594</sup> The Treasury Board submission applying for funding for the NSE replicated the language of the Guideline, specifically stipulating that the new liaison units would have no investigative or operational mandate.<sup>595</sup> Hence, NSE units at HQ and in the Divisions had no investigative capacity and were not expected to conduct investigations.<sup>596</sup> However, the RCMP provided for a mechanism

584 Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2566.

585 Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2723.

586 Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2560; Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2723.

587 Exhibit P-101 CAC0286, p. 2. In four Divisions, NSE representation was on a part-time basis. In those cases, threat assessment requests were transmitted to the Criminal Investigations Bureau (CIB) Officer in the Division: Exhibit P-101 CAC0283, p. 7.

588 Exhibit P-101 CAC0286, pp. 2-3. See also Exhibit P-101 CAA0039(i), pp. 17, 50.

589 Exhibit P-101 CAC0275, p. 2, CAC0495, p. 4; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5439-5440.

590 Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2568; Exhibit P-101 CAC0283, pp. 5-6, CAC0495, p. 4.

591 Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2569-2570; Exhibit P-101 CAC0278, p. 3, CAC0495, pp. 2-3.

592 Exhibit P-101 CAA0039(i), p. 19, CAC0283, pp. 6-7, CAC0495, pp. 4-5.

593 Exhibit P-101 CAC0283, pp. 5-6; Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2568-2569.

594 Exhibit P-101 CAA0081, pp. 2-16.

595 Exhibit P-101 CAC0017, CAC0021.

596 Exhibit P-101 CAC278, p. 3, CAC0286, p. 2; Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2578.

enabling it to investigate threat information, where it was deemed necessary, by instructing the divisional NSE units to bring matters requiring investigative follow-up to the attention of District Intelligence Officers (DIOs) so that other RCMP units could be tasked with conducting these investigations (whether after-the-fact or preventive).<sup>597</sup>

### ***Impact of the Decision to Create a Parallel RCMP Threat Assessment Process***

The Government's aim in approving the creation of dedicated RCMP liaison units (the NSE units) was to improve coordination of activities between CSIS and the RCMP and, in part, to ensure that CSIS received all threat-related information in the RCMP's possession so that it could be centrally analyzed as part of the global CSIS threat assessment process. In practice, however, CSIS was largely cut out of the picture in the new RCMP threat assessment process. The new NSE units mainly gathered information for the RCMP's own internal use in its new threat assessment process.

Rather than encouraging "...a high degree of coordination between 'intelligence' and 'action'",<sup>598</sup> NSE units were incorporated in a parallel RCMP threat assessment structure operating largely independently from the CSIS threat assessment process. The two agencies often ended up collecting and analyzing their threat information separately, with neither agency being in a position to conduct an overall analysis of all of the information available. P Directorate received advice about threats from both CSIS and NCIB NSE, but had no central threat assessment mandate or capacity of its own.<sup>599</sup>

### ***Deficiencies in the RCMP Threat Assessment Process***

#### ***Failures to Identify, Report and Share Relevant Information***

The new RCMP threat assessment process was meant to ensure that threat information uncovered by the various RCMP units in the course of their policing activities was transmitted to NCIB NSE, where it could be globally assessed so that Protective Policing could be advised of the threat situation. In practice, however, a great deal of potentially relevant threat information that was obtained by the Divisions, or that was accessible to them, was never reported to NCIB. E Division NCIS received information in April 1985 about possible attacks on the Vancouver Consul General and about various Sikh extremist groups. Included in this information was a mention that Parmar's group was the most dangerous, was keeping a low profile, and was working on a highly secret project.<sup>600</sup> None of this information was reported.<sup>601</sup> Kamloops NCIS learned that a group of Sikh

<sup>597</sup> Exhibit P-101 CAC0283, p. 6; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5446.

<sup>598</sup> Exhibit P-101 CAA0081, p. 8.

<sup>599</sup> Testimony of J.B. MacDonald, vol. 27, May 14, 2007, p. 2772; Testimony of R.E. Muir, vol. 28, May 15, 2007, p. 2928.

<sup>600</sup> Exhibit P-101 CAC0290.

<sup>601</sup> The information was transmitted by E Division VIP to P Directorate in HQ and NCIS in Vancouver, but not to NCIB: Exhibit P-101 CAC0290, p. 2.

extremists were planning to kidnap an Indian Consul General. NCIB received this information from CSIS, rather than from the divisional NSE unit that should have been collecting and reporting it.<sup>602</sup> In the same time frame, E Division NCIS was informed that an unknown number of Sikhs from Vancouver and Toronto were planning to travel to New York to attend a meeting on June 9, 1985, to establish policy for the violent resolution of problems.<sup>603</sup> This information also apparently went unreported to NCIB, in spite of the obvious national and international issues it raised.

### ***The Khurana Information***

On June 12, 1985, a Vancouver Police Department (VPD) source, Sarbjit Khurana, allowed the VPD to record a meeting with Sikh extremists who were attempting to intimidate him. During the debriefing immediately after the meeting, he advised that Pushpinder Singh, a suspected terrorist believed to be directing International Sikh Youth Federation (ISYF) operations, had responded to a statement by ISYF spokesperson Manmohan Singh complaining about the lack of attacks against Indian officials, that they should "...wait two weeks to see something being done."<sup>604</sup> This information was available to RCMP E Division NCIS members who worked at the Vancouver Integrated Intelligence Unit (VIU).<sup>605</sup> It was clearly relevant to the threat assessment process, but it was not passed on to NCIB by the NCIS prior to the Air India bombing.<sup>606</sup>

### ***The Duncan Blast Surveillance Information***

On June 4, 1985, CSIS followed Parmar, Reyat and an unknown third person to a wooded area near Duncan. A loud explosion, which the surveillance team initially thought was the discharge of a large calibre handgun, was heard before the men returned to their car and departed.<sup>607</sup> The information provided by CSIS about the Duncan Blast surveillance was not reported to the E Division NSE member or to NCIB. The RCMP has long complained that CSIS had not provided it with sufficient detail to allow an understanding of the potential significance of this event prior to the bombing.<sup>608</sup> In fact, CSIS advised different RCMP members and units of the information in various forms several times prior to the bombing, but the RCMP members who received the information apparently did not understand its significance to the threat assessment process and did not report it through the RCMP system in place.<sup>609</sup>

Even if the RCMP members who received the Duncan Blast information did not know that the noise heard in the woods may not have been a gunshot, the

---

<sup>602</sup> Exhibit P-101 CAB0169.

<sup>603</sup> Exhibit P-101 CAB0269(j); Testimony of Axel Hovbrenner, vol. 33, May 24, 2007, pp. 3893-3894.

<sup>604</sup> Exhibit P-101 CAB0321, p. 3, CAC0487, p. 4; Section 1.6 (Pre-bombing), Khurana Information.

<sup>605</sup> See Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

<sup>606</sup> See Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces and Section 1.6 (Pre-bombing), Khurana Information.

<sup>607</sup> Exhibit P-101 CAA0188.

<sup>608</sup> Testimony of Gary Bass, vol. 87, December 3, 2007, pp. 11241-11243; Exhibit P-101 CAA0335, p. 19, CAF0814, pp. 1-2.

<sup>609</sup> See Section 1.4 (Pre-bombing), Duncan Blast.

information they received was precisely the type of information that divisional units were expected to report for the purposes of the RCMP threat assessment process. The divisional NSE member, Sgt. Michael (“Mike”) Roth, who should have received and transmitted this information within the RCMP threat assessment process, had the proper security clearance to receive this secret CSIS information and was specifically responsible for sanitizing, rewriting, and reproducing classified CSIS information in a form that allowed its dissemination within the RCMP.<sup>610</sup> He testified before the Inquiry that he did not learn about the Duncan Blast until after the bombing of Air India Flight 182 and that this was precisely the type of information he should have received.

Other new and potentially related information was apparently not reported to the divisional NSE unit or to NCIB for threat assessment purposes. According to intelligence received by the Duncan Detachment on June 10, 1985, following a split in the local Sikh temple, extremists started a new temple whose leader, an associate of Reyat, was advocating “...selling homes and property to buy guns and ‘get strong’, *cut off all travel with Air India*, cut off all business with Vancouver, take revenge for any allegations.”<sup>611</sup> Back in September 1984, an RCMP source who provided information about a plot to bomb an Air India plane (Person 1) had also referred to a man in Duncan who could manufacture “nitro” for blowing up an Air India plane.<sup>612</sup> As the information was not reported to NCIB, it was not taken into the RCMP threat assessment process. Had it been, the RCMP would have been in a position to analyze the Duncan Blast surveillance information in light of this information and in light of the information about threats against Air India which was otherwise known to the Force, including the possibility of bombing raised by the June 1<sup>st</sup> Telex.<sup>613</sup>

The Duncan Blast information clearly suggested possible criminal activity at least, and contained many potential national security implications. It certainly was “information of threat assessment value.” It should have been reported through the channels that had been set up within the RCMP precisely for the purpose of gathering “criminal intelligence” and “intelligence related to security offences.” That it was not is an obvious intelligence failure. This conclusion does not excuse CSIS’s own intelligence failures in collecting, following up, or analyzing the Duncan Blast information.<sup>614</sup>

### ***The November 1984 Plot Information***

In September 1984, E Division obtained information from “Person 1” about a plot to bomb an Air India plane.<sup>615</sup> The information was not reported to the divisional NSE unit or to NCIB. Instead, it was communicated by telephone to the

---

<sup>610</sup> Testimony of Michael Roth, vol. 46, September 17, 2007, p. 5604.

<sup>611</sup> Exhibit P-101 CAA0276, p. 2 [Emphasis added], CAA0307, p. 3.

<sup>612</sup> Exhibit P-120(c), p. 6 (entry for March 10, 1986: doc 521-3).

<sup>613</sup> See Section 1.2 (Pre-bombing), June 1<sup>st</sup> Telex.

<sup>614</sup> See Section 1.4 (Pre-bombing), Duncan Blast.

<sup>615</sup> See Section 1.1 (Pre-bombing), November 1984 Plot and Exhibit P-120(c), p. 1 (entry for Sept. 20, 1984: doc 526-3, p.26).



Montreal Drug Coordinator Office.<sup>616</sup> There is no indication that the information was passed on to the local airport policing detachment. Jensen testified that this was precisely the type of information that would have to be reported to HQ “in a very rapid way”;<sup>617</sup> but the Division only transmitted information about this plot to NCIB over a month later,<sup>618</sup> in October 1984, after the VPD transmitted it to CSIS and to the RCMP on the basis of information received from “Person 2.”<sup>619</sup>

On learning of the delay in the transmission of the November Plot information to NCIB by E Division, Jensen directed that the field be instructed to “...use rapid communication which is timely” and that investigators report this type of information as soon as received.<sup>620</sup> Jensen agreed during his testimony before this Inquiry that the divisional investigator’s view – that the Person 1 information was not reliable<sup>621</sup> – should not have excused him from reporting on it.<sup>622</sup> There is no evidence of any additional steps taken to implement Jensen’s instructions about the reporting of threat information.

### ***Failures to Identify and Report Background Intelligence***

Without basic intelligence about extremist groups, it is difficult to grasp the significance of the information reported through the threat assessment process. When Sgt. Warren Sweeney, who was in charge of the terrorist desk at NCIB NSE,<sup>623</sup> learned about the Khurana information from VPD Cst. Don McLean on the day of the bombing, he had not previously been made aware of the role of Manmohan Singh (the ISYF spokesperson who complained about the lack of attacks on Indian officials) or Pushpinder Singh (the suspected terrorist believed to be directing ISYF operations who replied with the “wait two weeks” comment).<sup>624</sup> Having such background information available in the threat assessment system would have been necessary for NCIB to be able to appreciate the full significance of the Khurana information itself.

Without information on the identity of the main participants in the Sikh extremist movement and on the organizations to which they belonged, it was difficult for NCIB to put the information it received in its proper context to assess the seriousness of the threat. The VPD did have extensive knowledge of many of the most important Sikh extremist players and organizations in British Columbia

<sup>616</sup> Exhibit P-120(c), p. 1 (entry for Sept. 20, 1984: doc 526-3, p. 25) and (entry for Nov. 7, 1984: doc 526-3, p. 38).

<sup>617</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5449. See also Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2595, indicating that it was important that this kind of information come to NCIB as it affected the RCMP security offences mandate.

<sup>618</sup> Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 239-3).

<sup>619</sup> Exhibit P-120(c), pp. 1-2 (entry for Oct. 1984: doc 231-3, pp. 2-4) and p. 2 (entry for Oct. 23, 1984: doc 7).

<sup>620</sup> These instructions were issued on November 8, 1984: Exhibit P-120(c), p. 3 (entry for Nov. 8, 1984: doc CivLit1).

<sup>621</sup> See Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4107: Douglas, the divisional investigator, continued to defend his view that he “...very much doubted the information as being provided by P1 and P2, and did not believe it to be “credible.”

<sup>622</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5449.

<sup>623</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2572.

<sup>624</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2641; Exhibit P-101 CAF0035, p. 28.



as well as of the connections among the individuals and groups involved.<sup>625</sup> Although available to E Division NCIS members, this significant intelligence was not reported to NCIB.<sup>626</sup>

### ***NCIB Failure to Share Threat Information***

The divisional units that were expected to investigate threat information and to identify and report relevant information were not kept sufficiently informed of the overall threat situation. RCMP documents convey an expectation that the most useful threat information would be obtained from regular RCMP units and other agencies "...who are well informed on the threat assessment process" and in a position to obtain threat information.<sup>627</sup> There is no evidence that the members of divisional investigative units were provided on a routine basis with threat information gathered by other RCMP units and analyzed at HQ, even where such information was directly relevant to areas specifically being investigated.

As Sweeney confirmed in his testimony, in order to identify the information relevant to the threat assessment process, the Divisions needed to take into account other information about their targets, about the general threat level, about the possible ramifications of any planned action, as well as about the national and international context.<sup>628</sup> There does not, however, appear to have been a meaningful passage of such information to the Divisions. NCIB had access through RCMP central records to the CSIS threat assessments sent to P Directorate,<sup>629</sup> but only began to transmit the assessments routinely to the divisional NSE units in April 1985, when it started to receive its own copies.<sup>630</sup>

There is no record of E Division NCIS having received the information contained in an April 1985 CSIS threat assessment that a member of the Sikh Student Federation had been arrested at Vancouver International Airport with the barrel of an Uzi machine gun along with 100 rounds of ammunition in his luggage.<sup>631</sup> Had NCIS been advised, Sgt. Wayne Douglas, who was investigating Sikh extremism in British Columbia, would have likely gone to the airport and

---

<sup>625</sup> See Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

<sup>626</sup> See Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

<sup>627</sup> Exhibit P-101 CAC0495, p. 2.

<sup>628</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2606, 2613.

<sup>629</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2653-2655; Testimony of Warren Sweeney, vol. 26, May 9, 2007, 2692-2693.

<sup>630</sup> See Exhibit P-101 CAA0147, CAB0207, CAB0851, pp. 3-8 and CAC0291, indicating the time when NCIB began receiving copies of the CSIS TAs. About the usefulness of transmitting this information to the Divisions, see Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2703. For an example of a CSIS TA being sent to the Division by NCIB, see Exhibit P-101 CAA0160. The Commission find no such examples before NCIB began to receive its own copies.

<sup>631</sup> Exhibit P-101 CAB0207.

attempted to interview the individual for intelligence purposes.<sup>632</sup> NCIB's failure to keep the Divisions informed made it difficult for the units to do any follow-up investigations.

In April 1985, the E Division NCIS extremist/terrorist unit reported that very little action had been taken in the November Plot investigation and that "...[t]here has been no further information received from any sources that would indicate this or any bombing of an Air India Plane will occur."<sup>633</sup> NCIB did not take any steps to inform the divisional unit that there was, indeed, information about threats to Air India suggesting the possibilities of hijacking or sabotage and that the threat to Air India was considered high.<sup>634</sup> It was suggested at the Inquiry that this information was not communicated to E Division because the threats related to Air India flights out of Toronto and Montreal and did not originate from Vancouver.<sup>635</sup> This approach to information sharing is inconsistent with the basic premise that those who are to gather threat information need context and background in order to be able to recognize relevant information and to appreciate its significance.

### ***Lack of Training and Clear Instructions***

When the RCMP decided to create its own threat assessment process, it provided no specific training to its members to help them with their new responsibilities.

Sweeney testified that he received no training either before or after he left the Security Service to join the NCIB NSE terrorist desk.<sup>636</sup> Like other NCIB NSE members, he was involved in receiving and transmitting threat information and in following up on divisional investigations, but he never received any training about the new RCMP threat assessment process.<sup>637</sup> He received no training about the role of CSIS before or after its creation, nor was there any briefing about the *CSIS Act* and its effect on RCMP responsibilities. NCIB NSE personnel were given no training about Sikh extremism, even if it was stated to be a counterterrorism priority at the time.<sup>638</sup>

<sup>632</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4057. He would have done similar follow-up in relation to information contained in another CSIS threat assessment (Exhibit P-101 CAB0207), which indicated that a "...self-admitted Sikh terrorist was arrested at the Vancouver International Airport" who "...claimed to be a member of a cell within the Khalistan movement in India, which has received terrorist and commando training sponsored by this movement.": Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4056-4057.

<sup>633</sup> Exhibit P-120(c), p. 3 (entry for April 10, 1985: doc 526-3, p. 45).

<sup>634</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2612-2613. At the time, the amount of threat information transmitted by Air India, though viewed by some as Air India's way to obtain additional security for free, was perceived as very important by Government officials, who went as far as to state that every flight was preceded by a letter reporting a threat: Exhibit P-101 CAC0517, p. 2. While this appears somewhat exaggerated in light of the documentary record before the Commission, it is clear that NCIB perceived that much threat information was being transmitted by Air India and nevertheless did not see fit to inform E Division, which indicated that it had "no information from any sources".

<sup>635</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2613.

<sup>636</sup> Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2722-2723.

<sup>637</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2566. See, generally, the November 1984 Plot Chronology in Exhibit P-120(c), which Sgt. Sweeney followed up on: Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2593-2594.

<sup>638</sup> Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2723-2725.

Sweeney also received no training about protective measures, including airport security that might be applied to respond to the threat information NCIB NSE members were to analyze. He explained in testimony that he was not expected to know what the various airport security levels entailed, or to be aware of the security measures applied by Airport Policing, since he did not work in Airport Policing.<sup>639</sup> An understanding of Protective Policing roles and responsibilities would have been helpful in assessing the relevance of the threat information and for identifying information in need of further investigation. Without such understanding, NCIB NSE threat assessments would be of questionable utility to those members who had to implement security measures in response to the threats.

Members of the divisional NCIS units did not seem to have been provided with any training as to the type of information they were expected to report for the threat assessment process.<sup>640</sup> They received little guidance about the type of information which had to be shared with CSIS.<sup>641</sup> It was suggested in July 1985 that divisional NSE units be "...tasked to undertake a liaison and training program" to explain to members of other units in their Division the need to look for and report threat-related information and to educate them about the RCMP's security offences mandate.<sup>642</sup> This was not undertaken prior to the Air India bombing. In fact, an Extremism/Terrorism course was only developed by the RCMP Training Division years after the tragedy.<sup>643</sup>

HQ provided instructions to the Divisions in an attempt to explain the purpose of the RCMP threat assessment process. These instructions stressed the fact that RCMP members were to focus on "criminal intelligence." The official documentation referred to the need to provide threat assessments regarding "violent and criminal activities" that may be directed against an assortment of targets.<sup>644</sup> The messages instructed members to identify and report all "...suspected and known criminal intelligence information" about terrorism or extremism,<sup>645</sup> all information "...of a criminal threat assessment value,"<sup>646</sup> and all "...criminal extremist/terrorist information that would warrant consideration in the threat assessment process."<sup>647</sup> The documents failed, however, to provide any definition of what "criminal intelligence" was, or any further explanation about what such information might look like.

Further, guidance provided through HQ instructions was often no clearer as to the types of investigations RCMP members were expected to conduct in support

<sup>639</sup> Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2735-2736, 2742.

<sup>640</sup> See Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2581, 2605. Sweeney was not aware of any training being available at the time. No evidence was presented to the Commission and no documents were located, about any training.

<sup>641</sup> See Section 3.5.3 (Pre-bombing), RCMP Failures in Sharing with CSIS.

<sup>642</sup> Exhibit P-101 CAC0495, p. 3.

<sup>643</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2605.

<sup>644</sup> Exhibit P-101 CAC0275, p. 2.

<sup>645</sup> Exhibit P-101 CAC0286, p. 2.

<sup>646</sup> Exhibit P-101 CAC0495, p. 5. See also Exhibit P-101 CAC0406, p. 3, referring to the Divisions being familiar with the NSE role to provide criminal intelligence, and Exhibit P-101 CAC00278, pp. 3-4, discussing the NSE interest for "...areas when violent and/or criminal activity surfaces."

<sup>647</sup> Exhibit P-101 CAC0495, p. 2.

of the threat assessment process. When CSIS was created, the E Division NCIS terrorist/extremist unit in BC received no instructions to adjust its mandate, and "...just plodded along as [they] always had." The unit was originally called the "Dissident Group Squad", but the name was changed because "...headquarters in Ottawa did not like the reference of Dissident Groups." Douglas, the unit's head, testified that he was never comfortable with the new "Terrorist/Extremist" moniker. He explained that the distinction between investigating individuals and groups who could pose threats from a political versus a criminal perspective was "a very fine line."<sup>648</sup>

Because of this confusion, the NCIS unit at times appeared to be engaging in activities consistent with a purely CSIS-type "security intelligence" investigation and at other times failed to investigate what would appear to be clear and important threats of criminal activity. In the course of his duties, Douglas would sometimes go with his camera and "...shoot a couple of rolls of film" of individuals who attended demonstrations, even without any indication of criminal activities being planned or perpetrated.<sup>649</sup> Nevertheless, despite the fact that the RCMP had information that "Talwinder Singh Parmar is the subject of an international warrant issued by the Indian Government for murder and is considered to possess [*sic*] the greatest threat in Canada to Indian diplomatic missions and personnel,"<sup>650</sup> NCIS was not actively investigating Parmar's activities. Douglas told the Commission that the NCIS mandate related strictly to criminal activities, and that there was a "...fine line [that] flows back and forth" between Parmar's political aspirations and possible criminal activities. He noted that CSIS had been monitoring Parmar's activities, and that the view within the RCMP was that there was no point to duplicating effort.<sup>651</sup>

HQ provided the Divisions with explicit and implied warnings that some information should not be pursued. The 1985 draft RCMP Guideline on National Security Enforcement and Liaison instructed members to exercise discretion in the application of the security offences mandate, keeping in mind unspecified "underlying principles of the legislation." The Guideline provided for the conduct of intelligence operations and preventive action to be undertaken where there was "a legitimate law enforcement requirement" based on information indicating that prevention or detection of a criminal act was required. The operations were to be terminated when the investigation was complete or when "...legitimate law enforcement interest justifies their discontinuance." Without specifics, however, the RCMP members were left on their own to exercise "discretion" as to which investigations were consistent with the "...general law enforcement powers, authorities, principles and policies which have evolved with respect to the prevention and detection of criminal conduct."<sup>652</sup>

In response to CSIS's expressed concerns, NCIB NSE sent a telex to the Divisions indicating that assurances had been given that "...random interviews of ethnic

<sup>648</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4027-4028.

<sup>649</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4039.

<sup>650</sup> Exhibit P-101 CAB0221, p. 2.

<sup>651</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4115-4116.

<sup>652</sup> Exhibit P-101 CAA0039(i), pp. 8, 16-17.

communities for purposes of looking for information of a possible national security interest," are not within the RCMP's mandate, and that interviews are "...only conducted in furtherance of the criminal investigation of a criminal situation or the investigation of a person suspected of a criminal offence." It was requested that the Divisions ensure that their personnel understand and conform accordingly. K Division requested clarification, stating that "...surely we can continue to contact our established sources for the purpose of providing accurate/up-to-date threat assessments."<sup>653</sup>

Without clear instructions from the center, there was significant inconsistency in the types of activities and level of investigative initiative undertaken among the NCIS groups, even within the same Division. Whereas the E Division Terrorist/Extremist Unit did not undertake to develop sources,<sup>654</sup> Surrey NCIS worked proactively to develop intelligence by meeting with temple leaders and individuals to find people who would provide information about the "potential players"; and to develop a network of people in the community as a resource for RCMP intelligence.<sup>655</sup>

### ***Limited Investigative Capability***

The information flow for the RCMP threat assessment process envisaged regular investigative units of the Force collecting and investigating national security or threat information which they would report to divisional NSE units. No additional funding was provided for the regular investigative units to perform these new functions.<sup>656</sup> NCIS, which was responsible for collecting intelligence on major criminal activities in the Divisions, including extremist/terrorist activities, was expected to be particularly helpful to NSE in collecting threat information.<sup>657</sup> The reality, however, as it related to Sikh extremism in British Columbia, was quite different. The E Division NCIS and its intelligence unit investigating Sikh extremism were not truly functional and were unable to fulfil the role envisaged for them.

NCIS had limited human resources.<sup>658</sup> Its collection of criminal intelligence on extremism/terrorism was only undertaken on a "spasmodic basis", as the focus was mainly on traditional organized crime.<sup>659</sup> There was very little continuity of terrorist/extremist investigations, which usually lasted only for the time when a problem situation was a high priority – for example, during the visit of a dignitary.<sup>660</sup> This meant that investigators did not have the opportunity to build up significant and necessary expertise in a specific area. When an offence or incident did occur, or there was otherwise a need for relevant information, "...there [was] no reasonably comprehensive up-to-date police data base that [could] readily be referred to."<sup>661</sup>

---

<sup>653</sup> Exhibit P-101 CAF0820, pp. 35, 56, 59.

<sup>654</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4040.

<sup>655</sup> Testimony of Laurie MacDonell, vol. 76, November 15, 2007, pp. 9611-9613.

<sup>656</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5446.

<sup>657</sup> Exhibit P-101 CAC0495, p. 3.

<sup>658</sup> Exhibit P-101 CAF0821, p. 11.

<sup>659</sup> Exhibit P-101 CAF0821, p. 11.

<sup>660</sup> Exhibit P-101 CAF0821, p. 11.

<sup>661</sup> Exhibit P-101 CAF0821, p. 12.

The exception to the pattern of disjointed and intermittent focus was the Vancouver Integrated Intelligence Unit (VIU) in E Division, where one or two NCIS criminal intelligence members had been tasked for a number of years with criminal extremist/terrorist responsibilities.<sup>662</sup> However, NCIS members working at VIU often did not access or report the valuable intelligence gathered by their colleagues from the VPD who also worked at VIU, though it was generally available to them.<sup>663</sup>

During the pre-bombing period, the Criminal Terrorist/Extremist Group headed by Douglas at NCIS E Division was responsible for the entire province of British Columbia. The group's mandate was "...collecting intelligence on groups or individuals that could pose a threat to the community and to Canada at large."<sup>664</sup> The unit received and responded to requests for threat assessments and information from Headquarters as well as from various detachments in the BC region.

A number of factors led to serious deficiencies in the effectiveness of the E Division NCIS Terrorist/Extremist group. First, the unit did not view itself as fundamentally "investigative," or "operational" which, in practical terms, meant that it did not regularly take initiative to actively follow up on threats. Though issues of Sikh extremism formed "...the predominance of the workload" from the time of the Golden Temple, in the pre-bombing era members of the unit never met with Talwinder Singh Parmar, Ajaib Singh Bagri or Surjan Singh Gill<sup>665</sup> despite many indications of the real threat posed by these individuals.<sup>666</sup> In June 1985, NCIS members finally interviewed Parmar and Gill, in cooperation with US authorities, but this was only done as part of a "diffusion interviews" program meant to dissuade Sikh extremists from taking action against Indian PM Rajiv Gandhi during his upcoming visit to the US.<sup>667</sup>

When NCIS received information in April 1985 that Parmar's group was the most dangerous and was currently working on a "highly secret project,"<sup>668</sup> the unit took no steps to investigate further and find out what the project was.<sup>669</sup> Similarly, NCIS did not investigate the Khurana information and the "wait two weeks" comment prior to the bombing.<sup>670</sup> Although it was informed of the Duncan Blast incident, NCIS did nothing to investigate it further. To be sure, CSIS did request NCIS not to "...jeopardize the ongoing CSIS investigation by revealing specifics of the Duncan incident or other details of the [VIU] report" during diffusion

---

<sup>662</sup> Exhibit P-101 CAF0821, p. 11. VPD members also worked at VIU. For a review of the structure and effectiveness of the integrated unit, see Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

<sup>663</sup> See Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

<sup>664</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4027-4029.

<sup>665</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4029-4030, 4042, 4074.

<sup>666</sup> See, for example, CSIS TAs in Exhibit P-101 CAA0110 and CAB0221.

<sup>667</sup> See Section 1.4 (Pre-bombing), Duncan Blast.

<sup>668</sup> Exhibit P-101 CAC0290.

<sup>669</sup> Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4153-4154. Douglas had no recollection of this information and was not able to recall doing anything with respect to his investigations of Parmar in response to this information: Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4058.

<sup>670</sup> See Section 1.6 (Pre-bombing), Khurana Information.



interviews.<sup>671</sup> This request does not, however, seem tantamount to barring any NCIS investigation of the incident itself.<sup>672</sup> CSIS's request to be careful about tipping off Parmar and Gill about what CSIS knew certainly would not have stood in the way of a search of the area, as was done after the bombing.<sup>673</sup>

As late as June 14, 1985, E Division NCIS had to admit to NCIB that it was "... unable to determine the potential for violence against the Indian Consulate or its personnel in Vancouver" because it did not have "...access to intelligence directly from the hard core Sikh extremists."<sup>674</sup> NCIS did not have sources in the Sikh community. It did not have a source recruitment program and it was not otherwise actively trying to develop sources during the pre-bombing period.<sup>675</sup> Douglas indicated that cultural issues, including his impression that people in the Indo-Canadian community were openly mistrustful of the police and were fearful to cooperate with them,<sup>676</sup> were impediments to source development.<sup>677</sup> Meanwhile, the VPD, through its community policing approach, was able to gain trust, develop sources and thereby receive a good deal of intelligence about Sikh extremism.<sup>678</sup> The RCMP apparently devoted little resources to such activities, even if the lack of coded sources could be a "...significant handicap in these types of investigations."<sup>679</sup> Some HQ NCIB members even felt that recruiting sources for purposes of gathering information relevant to the threat assessment process would have been outside the RCMP mandate.<sup>680</sup> Jensen, on the other hand, believed that gathering intelligence from sources in the community was an integral part of intelligence-led policing and that divisional NCIS sections needed to have sources in the community.<sup>681</sup>

In fact, only one RCMP member in British Columbia, at the Surrey Detachment, attempted to use the community policing approach with the Sikh community to recruit more sources.<sup>682</sup> Sgt. Laurie MacDonell, who was working in the Surrey NCIS unit in the pre-bombing period, testified that his unit worked proactively to develop such sources, with the result that the Surrey NCIS unit was able to develop important contacts within the Sikh community who provided insight in terms of who the important extremists were. However, because of the reporting structure of the NCIS units in British Columbia, the E Division NCIS Terrorist/Extremist group at the divisional HQ would not necessarily have had access to this information.

There were a number of NCIS units located within the BC region, including Kamloops, Surrey, and Victoria. The focus of these units was on local community

---

671 Exhibit P-101 CAA0876, p. 1.

672 Testimony of Gary Bass, vol. 87, December 3, 2007, p. 11310.

673 Exhibit P-101 CAA0276, pp. 2-3. See, generally, Section 1.4 (Pre-bombing), Duncan Blast.

674 Exhibit P-101 CAC0438, p. 2; Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2704-2705.

675 Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4040; Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2704-2706.

676 Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4040, 4109.

677 Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4109.

678 See Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

679 Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4108-4110.

680 Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2705-2706.

681 Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1660-1661.

682 Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4149, 4174.



issues and not on the broader national and international implications of terrorism. Investigators in these units nevertheless did come across information in the course of their duties that touched on Sikh extremist issues. Surrey NCIS was dealing with a large number of temple skirmishes and other criminal activity that, while investigated as traditional crime, had significant national security implications by virtue of their connection to Sikh extremism.<sup>683</sup> When information was generated in the E Division HQ NCIS unit and farmed out to another NCIS unit in the Division for investigation, the information obtained would generally be reported back to E Division NCIS. In other cases, NCIS units in BC were not obliged to report their information touching on Sikh extremist issues to E Division NCIS. Even information generated outside of Vancouver relating to the Vancouver area<sup>684</sup> was “not necessarily” funnelled through NCIS.<sup>685</sup> The ability of E Division NCIS to identify potential terrorist/extremist trends in the province was therefore limited, and the unit was unaware of significant information about Sikh extremism in the BC area.

Because of the deficiencies in the flow of information and the lack of active engagement in the Sikh community, the E Division NCIS Terrorist/Extremist group had a limited understanding of the major Sikh extremist players in BC. Douglas did not know about the threats Parmar made that “Sikhs will kill 50,000 Hindus.”<sup>686</sup> While he “recognized the name” Bagri,<sup>687</sup> he was unaware that Bagri “...could be easily manipulated into committing a terrorist act,” or that Bagri had “...toured a number of European countries with a view to galvanizing Sikh extremist elements in order to launch a major attack against Indian and Hindu interests.” He was similarly unfamiliar with the information that “Bagri was planning to hijack an Air India jetliner during 1984 10 in order to demand the release of seven hijackers.”<sup>688</sup> Douglas indicated that he “...wasn’t too familiar with Mr. [Surjan Singh] Gill,”<sup>689</sup> who was identified by CSIS as being “...the brains behind the Babbar Khalsa.”<sup>690</sup>

### ***Lack of Centralization***

In the years preceding and immediately following the Air India bombing, the RCMP threat assessment structure was not organized in a manner to allow for

<sup>683</sup> Testimony of Laurie MacDonell, vol. 76, November 15, 2007, p. 9609.

<sup>684</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4043, 4054-4055, 4065.

<sup>685</sup> For example, a telex (Exhibit P-101 CAC0312) that was sent from Headquarters NCIB to C, O and E Divisions on April 3, 1985 cites information as coming from “E” Division that “Several people in the Indo-Canadian community believe that Consul General Sharma was sent to Ottawa by the Indian government to incite the militants” and that “The Sikh Student Federation is planning an unknown type of overt action in Vancouver against the Indian Consulate” and “The society known as Babbar Khalsa is planning some overt action.” While this information would clearly relate to both the mandate of Douglas’ unit and to the Vancouver area, Douglas had no recollection of this information and indicated that it was possible that information like this would not have reached his unit: Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4060-4061.

<sup>686</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4051. The information was included in a CSIS threat assessment dated October 26, 1984, which was provided to the RCMP P Directorate: Exhibit P-101 CAA0110, p. 2.

<sup>687</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4048.

<sup>688</sup> Exhibit P-101 CAA0110, p. 3; Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4052-4053.

<sup>689</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4053.

<sup>690</sup> Exhibit P-101 CAA0110, p. 3.

sufficient central control over investigations of threats to national security or for the timely receipt of relevant information.

### **Reporting Structure**

The regular RCMP reporting structure was not modified when NSE units were added to NCIS in the Divisions and to NCIB at HQ. Divisional NCIS sections did not report directly to NCIB, but rather through the Criminal Investigations Branch (CIB). This involved reporting up through the regular chain of command within each Division, with the higher levels reporting to their counterparts at HQ. The NSE unit essentially added a new layer in this reporting structure. RCMP units coming across threat information were now to report the information to this new unit rather than through the regular divisional chain of command. The Divisional NCIS NSE unit was then to report the information to HQ NCIB NSE through the DIO to the Criminal Operations Officer in charge of each Division.

This structure was ill-adapted to the threat assessment process because, unlike the structure in place at CSIS (and previously at the RCMP Security Service), it was not centralized or comprehensive. It did not allow NCIB NSE to obtain information directly, which inevitably created delays in gathering threat information and producing threat assessments.<sup>691</sup>

### **Delays**

Both CSIS and the RCMP received information in October 1984 about a plot to bomb an Air India aircraft (the November Plot information).<sup>692</sup> On October 23, 1984, the Vancouver Police Department (VPD) met with CSIS and with an RCMP member working at CISBC<sup>693</sup> to advise them that Person 2 had provided information about the plot. The following day, CSIS advised Airport Policing by telephone, and then sent a telex to Airport Policing and VIP Security on October 26, 1984.<sup>694</sup> On the RCMP side, E Division NCIS was advised of the Person 2 interview directly by the VPD.<sup>695</sup> The information was not sent to NCIB until October 26<sup>th</sup>.<sup>696</sup> NCIB transmitted the information to P Directorate VIP Security on October 30<sup>th</sup>,<sup>697</sup> almost a week after the CSIS call to Airport Policing. NCIB never did relay the information to Airport Policing. Sweeney explained that structural differences between CSIS and the RCMP were partly responsible for the different turnaround times. CSIS HQ would receive the information immediately, whereas RCMP investigators had to “go through channels” to send the information to Ottawa.<sup>698</sup>

---

<sup>691</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2569-2571; Exhibit P-101 CAC0278, p. 4; Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2726.

<sup>692</sup> See, generally, Exhibit P-120(c) and Section 1.1 (Pre-bombing), November 1984 Plot.

<sup>693</sup> For a description of the CISBC structure and mandate, see Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

<sup>694</sup> Exhibit P-120(c), p. 2 (entry for Oct. 23, 1984: doc 7 and entry for Oct. 26, 1984: doc 229-3, p. 5).

<sup>695</sup> Exhibit P-120(c), pp. 1-2 (entry for Oct. 1984: doc 231-3, pp. 2-4). Note that the information was discussed with Sgt. Douglas, who would pursue it.

<sup>696</sup> Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 239-3).

<sup>697</sup> Exhibit P-120(c), p. 2 (entry for Oct. 30, 1984: doc 526-3, p. 29).

<sup>698</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2572, 2637-2638.

Threat information is usually time-sensitive. Delays can have serious, potentially deadly consequences. In the November Plot case, the potential impact of the delay caused by the RCMP reporting structure was eliminated because the same information had been transmitted by CSIS much earlier. An effective threat assessment system cannot rely on such fortuitous circumstances.

Senior echelons at NCIB understood that RCMP reporting procedures meant that the HQ NSE Section would simply not be able to provide a true evaluation of the threat without considerable advance notice that a threat assessment was required.<sup>699</sup> When DIOs complained in the spring of 1985 about short notice to Divisions for threat information requests, NCIB asked that P Directorate provide its requests further in advance<sup>700</sup> and undertook to pass them on to the Divisions as soon as received.<sup>701</sup> The RCMP's inability to provide threat assessments on short notice seems simply to have been accepted as inevitable. Nothing was done to adjust RCMP reporting procedures to allow the threat assessment system to deal with circumstances where advance notice was not possible.

### ***Lack of Direction of Investigative Effort***

Because of the RCMP reporting structure, NCIB NSE was unable to direct the investigative efforts of the Divisions in gathering threat information. The investigative units reported through the Divisional chain of command, and the role of NCIB was limited to trying to "...lead [the Divisions] in areas that [HQ] felt were important." Without formal authority to command divisional investigators, who made their own decisions about the conduct of their investigations,<sup>702</sup> NCIB could not coordinate investigations of national or international import, or even make its own decisions about follow-up or further investigation. NCIB could make suggestions to the investigators<sup>703</sup> but, in general, it did not see its role as proactive, and simply passed on information without asking questions. Thus, in mid-June 1985, NCIB received a report stating that E Division was "...unable to determine the potential for violence against the Indian Consulate or its personnel in Vancouver."<sup>704</sup> NCIB simply transferred the "information" to P Directorate and did not suggest any additional investigation.<sup>705</sup>

The regular RCMP reporting structure did not require ongoing, detailed updates. As a result, NCIB did not receive complete information about the progress of the Divisions' investigations and, lacking the authority, could not formally order the Divisions to provide more information. This minimized the guidance NCIB could give to the Divisions in the conduct of their investigations. When NCIB did attempt to provide guidance or requested updates, its requests were

699 Exhibit P-101 CAC0278, p. 4, CAC0406, p. 4.

700 Exhibit P-101 CAC0406, pp. 3-4.

701 Exhibit P-101 CAC0495, p. 2.

702 Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2578, 2609-2610.

703 Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2610-2611.

704 Exhibit P-101 CAC0438.

705 Exhibit P-101 CAC0442. See also Exhibit P-101 CAC0459, sent to VIP Security, which simply paraphrases the information found in Exhibit P-101 CAC0444, received by NCIB from O Division.

often simply ignored by divisional investigators who continued to pursue their inquiries in accordance with their own theory of the case and provided little more than unexplained conclusions to NCIB.

### ***The November 1984 Bomb Plot and the RCMP Reporting Structure***

In many ways, the November 1984 bomb plot provided a perfect illustration of the impact of the RCMP reporting structure on threat assessment.

When E Division NCIS reported the November Plot information to NCIB for the first time on October 26, 1984, it did not inform NCIB that the same information had previously been obtained independently from another source in September. The Division's message simply stated that the information had previously been "reported" to Montreal authorities and had now "resurfaced."<sup>706</sup> The divisional investigator, Douglas, advised NCIB of his view that the information was of "totally unknown reliability."<sup>707</sup> He did not provide an explanation for this conclusion. NCIB forwarded the information to VIP Security with the caveat that its reliability was doubtful,<sup>708</sup> without having had an opportunity to make its own assessment and without knowing that the information originated from two different sources: Person 1, who reported it to the RCMP in September, and Person 2, who reported it to the VPD in October.<sup>709</sup> E Division NCIS also did not provide NCIB with complete information about the assessment made by the VPD members who had interviewed Person 2 in October 1984.<sup>710</sup> These officers had expressed concern "...that this [November Plot] [was] a reality and [could] be accomplished at some time."<sup>711</sup> The divisional investigator, who at the time had not yet personally interviewed Person 2, only advised NCIB that the information was of "totally unknown reliability"<sup>712</sup> and that the VPD members who interviewed Person 2 believed that it was suspect because Person 2 was desperate to receive bail.<sup>713</sup>

When NCIB was finally informed of the existence of the earlier source for the November Plot information on November 1, 1984,<sup>714</sup> Sweeney, the NSE member in charge of the terrorist desk, was of the view that the matter had to be

<sup>706</sup> Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 239-3). E Division NCIS Sgt. Douglas confirmed that when he reported to Headquarters that the information had "resurfaced," he was aware that there were two sources of this information: Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4087.

<sup>707</sup> Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 239-3).

<sup>708</sup> Exhibit P-120(c), p. 2 (entry for Oct. 30, 1984: doc 526-3, p. 29).

<sup>709</sup> Exhibit P-120(c), p. 1 (entry for Sept. 20, 1984: doc 526-3, p. 26) and pp. 1-2 (entry for Oct. 1984: doc 231-3, pp. 2-4).

<sup>710</sup> The VPD report containing this assessment was provided to E Division on October 23, 1984: see Exhibit P-120(c), p. 2 (entry for Oct. 23, 1984: doc 7), stating that "a copy of interview" was provided and the "report" passed with the understanding that only the intelligence about the airplane bombing would be addressed. The information sent to NCIB by the Division on November 1, 1984 was clearly based on the VPD report: See Exhibit P-120(c), p. 2 (entry for Nov. 1, 1984: doc 526-3, pp. 26-27).

<sup>711</sup> See VPD report summarized at Exhibit P-120(c), pp. 1-2 (entry for Oct. 1984: doc 231-3, pp. 2-4). The officers had also expressed the view that Person 2's information was suspect and that Person 2 had other motives for providing it, but had not seen this as excluding the possibility that it was factual.

<sup>712</sup> Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 239-3).

<sup>713</sup> Exhibit P-120(c), p. 2 (entry for Nov. 1, 1984: doc 526-3, pp. 26-27).

<sup>714</sup> Exhibit P-120(c), p. 1 (entry for Sept. 20, 1984: doc 526-3, p. 26).

investigated further.<sup>715</sup> Because NCIB could not conduct its own investigations,<sup>716</sup> it had to rely on the divisional investigator to conduct these additional inquiries. The investigator (Douglas) had already concluded that the information was not reliable in spite of the fact that it was provided by two sources<sup>717</sup> and had not thought it necessary to report the information when he first received it.

On November 6, 1984, NCIB requested “on an urgent basis” that the divisional unit provide regular updates on the investigation.<sup>718</sup> On November 16<sup>th</sup>, NCIS reported that checks had been conducted on certain associates of Person 2 and that no connections to extremist groups had so far been established.<sup>719</sup> The Division did not provide the names of the associates who were the subject of checks. As a result, NCIB could not research the central RCMP databases to find out if any information unavailable at the Division could be found at HQ.<sup>720</sup>

On November 26<sup>th</sup>, NCIS provided further details of an interview with Person 2. For the first time, NCIB learned that during the interview, Person 2’s lawyer had alleged that Person 2 knew more about the plot than what he was telling the police.<sup>721</sup> Because of the decentralized RCMP structure and the limited authority granted to NCIB, the HQ members did not see it as their role to decide whether or how to investigate further Person 2’s possible knowledge.<sup>722</sup>

NCIS also advised in its November 26<sup>th</sup> message that it had learned from Person 2 that the East Indian males involved in the November Plot resided in what for purposes of this report must be referred to as “x town”, located in what must as well be referred to as “y province.” Divisional checks on Person 2’s associates revealed that three of them had phone numbers from y province. NCIS promised to provide NCIB with the subscriber information for those numbers, which it was in the process of obtaining. NCIB subsequently requested that the NCIS of x town be brought into the investigation once the identity of the subscribers was ascertained.<sup>723</sup> E Division NCIS did not provide this or any other information about the investigation to NCIB for a number of months. On March 20, 1985, four months after the last NCIS report, NCIB wrote to NCIS and to the E Division DIO to request a full update as soon as possible.<sup>724</sup> In response, NCIS did not provide an update on the investigation and did not inform NCIB of the identity of the x town subscribers, but simply stated on April 10<sup>th</sup> that “very little action” had occurred in this matter and that there had “...been no further information received from any sources that would indicate this or any bombing of an Air India Plane will occur.”<sup>725</sup>

<sup>715</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2600-2601.

<sup>716</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2578.

<sup>717</sup> Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 239-3 and entry for Oct. 30, 1984: doc 526-3, p. 29); Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4107.

<sup>718</sup> Exhibit P-120(c), p. 3 (entry for Nov. 6, 1984: doc 526-3, p. 35).

<sup>719</sup> Exhibit P-120(c), p. 3 (entry for Nov. 16, 1984: doc 253-3).

<sup>720</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2605-2609, 2629.

<sup>721</sup> Exhibit P-120(c), p. 3 (entry for Nov. 26, 1984: doc 526-3, p. 40).

<sup>722</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2609-2610.

<sup>723</sup> Exhibit P-120(c), p. 3 (entry for Nov. 26, 1984: doc 526-3, p. 40 and entry for Dec. 4, 1984: doc 526-3, p. 42).

<sup>724</sup> Exhibit P-120(c), p. 3 (entry for March 20, 1985: doc 526-3, p. 44). It was noted in the telex that the last correspondence received from NCIS was dated November 26, 1984.

<sup>725</sup> Exhibit P-120(c), p. 3 (entry for April 10, 1985: doc 526-3, p. 45).

No further information about the November Plot investigation was provided by E Division NCIS until the day of the Air India bombing, when NCIB requested that NCIS interview Person 2 about the crash. NCIS conducted an interview and advised NCIB on June 23<sup>rd</sup> that Person 2 “knew nothing” about the bombing. A report about the interview was requested and promised, but the Division did not provide any report or additional details until many months later.<sup>726</sup> Though NCIB was only informed that Person 2 knew nothing about the bombing, in fact, during the interview, Person 2 had said that he would speak to the police only if they were willing to deal with his pending charges.<sup>727</sup> It was his lawyer who had subsequently told the NCIS investigator during a telephone conversation on the same day that Person 2 did not know anything about the crash.<sup>728</sup>

E Division NCIS provided no further substantive information about the November Plot investigation to NCIB (which was now acting as the Coordination Center for the national Air India Task Force)<sup>729</sup> until December 17, 1985.<sup>730</sup> NCIB made numerous requests for information and updates about the investigation.<sup>731</sup> It also inquired about the identity of the x town subscribers that the Division was to have obtained in November 1984 and provided to NCIB.<sup>732</sup> These requests remained unanswered, except for a telex in October 1985 stating that the Division was compiling material about Person 2 and would reply to the HQ requests for information once the material was obtained.<sup>733</sup>

Meanwhile, in July 1985, E Division had obtained a copy of a VPD report about an interview with Person 2, where alleged November Plot conspirators were named.<sup>734</sup> The Division even noted at the time that the information provided

---

<sup>726</sup> Exhibit P-120(c), pp. 3-4 (entry for June 23, 1985: doc 526-3, p. 13) and p. 5 (entry for Dec. 17, 1985: doc 526-3, pp. 63-65). A telex was said to have been dispatched about this conversation, but no record of the telex could later be found.

<sup>727</sup> Exhibit P-120(c), p. 4 (entry for June 1985: doc 526-3, p. 59) and p. 5 (entry for Dec. 17, 1985: doc 526-3, pp. 63-65). Sweeney testified that he was aware at the time that Person 2 “want[ed] to deal”: Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2616.

<sup>728</sup> Exhibit P-120(c), p. 4 (entry for June 1985: doc 526-3, p. 59) and p. 5 (entry for Dec. 17, 1985: doc 526-3, pp. 63-65).

<sup>729</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2560. See also, generally, Exhibit P-101 CAF0055.

<sup>730</sup> Exhibit P-120(c), p. 5 (entry for Dec. 17, 1985: doc 526-3, pp. 63-65). See also, generally, Exhibit P-120(c), pp. 3-5.

<sup>731</sup> Exhibit P-120(c), p. 4 (entry for Sept. 13, 1985: doc 526-3, p. 47, entry for Sept. 24, 1985: doc 526-3, p. 48 and entry for Oct. 2, 1985: doc 526-3, p. 49), pp. 4-5 (entry for Nov. 25, 1985: doc 526-3, p. 55) and p. 5 (entry for Dec. 11, 1985: doc 526-3, p. 58). See also Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2618-2620, confirming that requests for updates continued to be sent as no response was obtained from the Division.

<sup>732</sup> This information was specifically requested on September 9, 1985: Exhibit P-120(c), p. 4 (entry for Sept. 9, 1985: doc 526-3, p. 46) and the follow-up telexes listed in the above footnote referred to this request as well. The information was specifically requested one more time on December 11, 1985: Exhibit P-120(c), p. 5 (entry for Dec. 11, 1985: doc 526-3, p. 58). Sweeney confirmed during his testimony that the associates referred to in these requests as “...the three individuals who visited Person 2” and as “Person 2’s associates” were in fact the same three individuals from y province whose subscriber information was being obtained by E Division on November 26, 1984 and was to be forwarded to NCIB as per Exhibit P-120(c), p. 3 (entry for Nov. 26, 1984: doc 526-3, p. 40): Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2629-2630.

<sup>733</sup> See Exhibit P-120(c), p. 4 (entry for Oct. 2, 1985: doc 526-3, p. 50).

<sup>734</sup> Exhibit P-120(c), p. 4 (entry for July 10, 1985: doc 493-3 and entry for July 12, 1985: doc 494-3) and pp. 8-9 (entry for May 1986: doc 23), where Randhawa states that all the information he obtained was forwarded to Douglas.



by Person 2 was similar to information received from Person 1 in November 1984.<sup>735</sup> This assessment and the new information about the identity of possible November Plot conspirators was not transmitted to NCIB. The substance of the information provided in July 1985 by Person 2 about the conspirators was discussed for the first time in correspondence transmitted to HQ in April 1986, but neither the details of the interview nor the actual VPD report were provided.<sup>736</sup>

In early December 1985, NCIB was still waiting for a response to its numerous requests for updates and information. On December 6<sup>th</sup>, Sweeney met with CSIS investigator David Ayre who used to work at the BC Region and had been transferred to Ottawa.<sup>737</sup> Because Ayre had been involved in the investigation of the November Plot information with E Division investigator Douglas, Sweeney asked him whether he knew the identity of the x town subscribers who were Person 2's associates.<sup>738</sup> Three days later, Ayre provided NCIB with the names of the associates and advised Sweeney that the E Division investigator was in possession of the long distance tolls for Person 2's phone number for the months preceding his arrest and incarceration in 1984.<sup>739</sup> This was the first time NCIB learned about the telephone tolls.

Having now received from CSIS the information about the identity of the x town subscribers which had been promised by E Division in November of the previous year, Sweeney researched the RCMP HQ database and found that one of the individuals was "...affiliated with what can be termed extremist/terrorist groups within the Sikh community."<sup>740</sup> NCIB sent another request to E Division on December 11, 1985, this time addressing it to the personal attention of Superintendent Les Holmes, the officer in charge of the E Division Air India/Narita Task Force. NCIB explained that as a result of information received from CSIS, one of Person 2's associates was identified as a conspirator to the plot to bomb an Air India plane. NCIB stated that, to date, HQ had received no satisfactory answers to any of its requests from NCIS and asked that a response be provided as soon as possible.<sup>741</sup>

NCIS finally provided a response on December 17, 1985.<sup>742</sup> For the first time, the divisional investigator provided a written account of his June 1985 interview with Person 2. Douglas also finally provided the names of Person 2's x town associates. He explained that when the associates' identities were discovered, the local police of x town had been contacted and had provided background information on the individuals indicating that there was "...no known connection or association to extremist groups."<sup>743</sup>

<sup>735</sup> Exhibit P-120(c), p. 4 (entry for July 12, 1985: doc 494-3) and generally p. 4 and following.

<sup>736</sup> In Exhibit P-120(c), p. 7 (entry for April 2, 1986: doc 526-9, p. 95), the information is referred to as from "confidential sources". When an HQ analyst compiled all relevant correspondence on April 15, 1986, the VPD report was not mentioned. See Exhibit P-120(c), p. 8 (entry for April 15, 1986: doc 526-3, pp. 1-22).

<sup>737</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2621.

<sup>738</sup> Exhibit P-120(c), p. 5 (entry for Dec. 6, 1985: doc 526-3, p. 56); Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2621-2622. See also Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2629-2630.

<sup>739</sup> Exhibit P-120(c), p. 5 (entry for Dec. 6, 1985: doc 526-3, p. 56).

<sup>740</sup> Exhibit P-120(c), p. 5 (entry for Dec. 6, 1985: doc 526-3, p. 56).

<sup>741</sup> Exhibit P-120(c), p. 5 (entry for Dec. 11, 1985: doc 526-3, p. 58).

<sup>742</sup> Exhibit P-120(c), p. 5 (entry for Dec. 17, 1985: doc 526-3, pp. 63-65).

<sup>743</sup> Exhibit P-120(c), p. 5 (entry for Dec. 17, 1985: doc 526-3, pp. 63-65).



Douglas was asked to explain to the Commission why it took so long for him to respond to Headquarters' requests. He testified that it was "certainly most unusual," but that he was "at a loss" as to why it took so long. It appears that even the decision about how long a divisional investigator should take to respond to a request by HQ was made at the divisional level. Douglas explained that when requests came into the Task Force, they were received by the administrative people who assigned diary dates for response and then disseminated the information. He stated: "I would think if this was me requesting information, I hadn't got after a couple [of days] I'd just pick up the phone and say, 'hey what's the problem, what's going on out here' if it's that important"<sup>744</sup>

In the context of the traditionally decentralized RCMP structure, it appears that the HQ requests for updates, information and specific investigative steps were seen in the Divisions as hindering the investigators' work. As Sweeney explained, RCMP members in the Divisions felt that HQ should let the investigators do their job and that they would provide the information they felt was relevant when it was obtained. This was especially true during the post-bombing period when the E Division Air India Task Force was constantly receiving requests for updates and information.<sup>745</sup>

Though frustrated by the lack of response from E Division,<sup>746</sup> NCIB members had little ability to take action to address the situation. According to Douglas, who was the head of the NCIS Terrorist/Extremist Unit, NCIS "had a free rein" in terms of its relationship with NCIB, so long as it operated within certain guidelines.<sup>747</sup> Because E Division NCIS did not report to NCIB, all that NCIB could do to get information was to contact the investigators' commanding officer within the Division or, after the establishment of HQ Air India Task Force Coordination Center, to have the Officer in Charge (OIC), Chief Superintendent Belanger, sign the request.<sup>748</sup> Sweeney did, in fact, have to contact the OIC of the E Division Task Force in December 1985 in order to obtain a response to NCIB requests that had been left unanswered for months.<sup>749</sup>

Throughout the pre-bombing and early post-bombing investigation of the November Plot information, NCIB was provided with incomplete information, after significant delays. This lack of complete and timely information made it impossible for NCIB to provide any useful contribution.

Without formal authority over divisional investigators, there was little NCIB could do to press forward investigations in which divisional investigators were not especially interested. Even when an analyst at the NCIB Coordination Center for the Air India investigation became interested in the November Plot

<sup>744</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4098-4100.

<sup>745</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2627.

<sup>746</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2624.

<sup>747</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4031.

<sup>748</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2627-2628.

<sup>749</sup> Exhibit P-120(c), p. 5 (entry for Dec. 11, 1985: doc 526-3, p. 58). Shortly after this message, a response was finally received from the divisional investigator: See Exhibit P-120(c), p. 5 (entry for Dec. 17, 1985: doc 526-3, pp. 63-65).

information and concluded that the matter needed to be re-examined in order to ascertain possible connections with the Air India bombing,<sup>750</sup> NCIB was unable to obtain details for months about information in the Division's possession. The divisional investigator had all but discounted the matter from the start,<sup>751</sup> and it took the involvement of senior officers in the Division many months after the Air India bombing, and long after the HQ analyst began to inquire about the information, to get the file reviewed and to have potential conspirators to the Plot interviewed.<sup>752</sup> NCIB appears to have been essentially powerless to remedy inaction at the Divisional level while, at the same time, it had no authority or capability to conduct the type of investigation it thought to be necessary on its own.

### ***Inability to Assess Threat Information Centrally***

The RCMP threat assessment structure made ongoing centralized comprehensive assessment of intelligence and information in the Force's possession impossible.

The RCMP threat assessment system was not set up to collect and process general threat information on an ongoing basis, but rather was designed primarily to respond to specific requests for assessments. NCIB sent information requests to the Divisions in anticipation of specific known events or in reaction to information, but did not generally receive reports about any threat information that divisional NSE units collected on an ongoing basis from other units conducting relevant investigations.<sup>753</sup> Jensen explained that it would neither have been possible nor desirable for all 22,000 RCMP members to report threat information to HQ on an ongoing basis since that would have "...chok[ed] the whole system."<sup>754</sup> What this meant, though, was that all information that was relevant to understand the threat at a particular point in time was never available for immediate analysis in one central location. NCIB had to request information from the Divisions every time a threat assessment requirement arose. It is an inadequate explanation that the amount of potentially relevant information would choke operations. Surely the response should be to devise a better and more efficient system.

The reporting delays associated with the decentralized structure of the Force slowed down the transmission and receipt of information for every request. Without access to relevant threat information in real time, NCIB members could not respond to the seriousness of the threat as it evolved and could not redirect intelligence-gathering activities accordingly.<sup>755</sup> The RCMP system was purely reactive and generally unsuited to prevention on a broader, long-term scale.

<sup>750</sup> See Exhibit P-120(c), p. 4 (entry for Sept. 13, 1985: doc 526-3, p. 47); Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2617.

<sup>751</sup> Douglas maintained the view that the November Plot information was unreliable throughout: See Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 239-3, entry for Oct. 30, 1984: doc 526-3, p. 29 and entry for Nov. 1, 1984: doc 526-3, pp. 26-27) and p. 6 (entry for Feb. 18, 1986: doc 526-3, pp. 74-75 and entry for March 5, 1986: doc 526-3, p. 86). See also Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4107.

<sup>752</sup> See Section 2.3.1 (Post-bombing), November 1984 Plot.

<sup>753</sup> Efforts were at times made to encourage the divisional units to engage in this ongoing collection of information: Exhibit P-101 CAC0283, pp. 2-3, CAC0495, p. 2.

<sup>754</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5448.

<sup>755</sup> Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2726.

CSIS threat assessments did generally attempt to discuss the broader current threat context, but they were not routinely transmitted to NCIB until April 1985.<sup>756</sup> Before that time, P Directorate received both the CSIS and the NCIB threat assessments, but did not automatically pass on the CSIS assessments to NCIB. NCIB could have accessed these assessments through the RCMP central records,<sup>757</sup> but it was not in the practice of regularly searching those records to ensure that its assessment of the threat situation took into account all available information.<sup>758</sup>

The RCMP also received other threat information that was not provided to NCIB. The HQ P Directorate received information about threats to Indian interests and to Air India directly from the Department of External Affairs and from the airline, but this information was often not transmitted to NCIB.<sup>759</sup> The most important example of such information that was never reported or transmitted to NCIB was the June 1<sup>st</sup> Telex about threats to bomb Air India planes using time-delayed devices.<sup>760</sup> In some cases, this sort of information was not even accessible to NCIB through central records as it was not reported to HQ by local airport detachments.<sup>761</sup> Divisional NSE units were instructed to liaise directly with the VIP Security units in their Division, as these units would at times have information not available to HQ.<sup>762</sup> There is documentation that such liaison occurred within the Divisions,<sup>763</sup> but no indication that P Directorate information was obtained and researched at the HQ level to prepare threat assessments.

The VIP Security Branch of P Directorate would at times receive reports from divisional sections outlining demonstrations, threats and disruptions experienced while protecting Indian officials.<sup>764</sup> VIP Security could take special measures in light of the nature of the threat, such as contacting the “bomb squad” and requesting an explosives vapour detector sweep on diplomatic premises, as was done on June 19, 1985 at the Indian High Commission in Ottawa.<sup>765</sup> Information on such measures and about the unfolding of events involving Indian diplomats was relevant to the threat assessment process. It too, however, was not routinely transmitted, or in some instances not transmitted at all, to NCIB or incorporated in the threat assessment process.<sup>766</sup>

<sup>756</sup> Exhibit P-101 CAA0147, CAB0207, CAB0851, pp. 3-8, CAC0291.

<sup>757</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2653.

<sup>758</sup> See, for example, Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2597-2598.

<sup>759</sup> See the following documents, for which there is no record that the information was transmitted to NCIB: Exhibit P-101 CAA0185, Exhibit P-101 CAC0293, Exhibit P-129; Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2732, explaining that NCIB did not receive the June 1<sup>st</sup> Telex.

<sup>760</sup> Exhibit P-101 CAA0185.

<sup>761</sup> For example, a July 1984 telex (see Exhibit P-101 CAA0083, CAA0084) noting that an individual had “... volunteered to carry a bomb in his accompanied baggage with a view to blowing up an Air India plane in order to draw attention to the demands of the Sikhs.” See also Exhibit P-101 CAC0419, a June 7, 1985 telex indicating that “...enforcement of special measures to deal with increased threat of hijacking and sabotage at airports by extremists should be continued till the end of June 85.” See, generally, Section 3.5.3 (Pre-bombing), RCMP Failures in Sharing with CSIS.

<sup>762</sup> Exhibit P-101 CAC0495, p. 4.

<sup>763</sup> See, for example, Exhibit P-101 CAC0285, referring to a D Division NSE report which refers to information found in Exhibit P-101 CAC0271, pp. 2-4, a report from D Division VIP Security to HQ VIP Security.

<sup>764</sup> See, for example, Exhibit P-101 CAC0233, CAC0271.

<sup>765</sup> Exhibit P-101 CAC0441, p. 2; Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2717, 2719.

<sup>766</sup> Sweeney specified NCIB would not be informed, for example, of the VIP decision to contact the “bomb squad”: Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2717-2718.

Assessing and investigating threats to national security requires coordination of potentially disparate pieces of information from a variety of sources which must be pieced together and analyzed. Newly-gathered information can shed light on information already collected, opening new avenues of investigation. A high degree of centralization is necessary for such a process. The reporting gaps in the RCMP structure, as well as NCIB's failure to conduct regular searches of central records,<sup>767</sup> meant that the RCMP threat assessment process was seldom, if ever, in possession of all the necessary information to make the necessary linkages and connections to carry out its role.

### **Limited Analytical Capability**

The NSE members tasked with collecting and assessing threat information often had difficulty appreciating the significance of the information gathered. They did not always see how it related to other information already in the RCMP's possession or understand what information required further investigation and how such inquiries should be conducted.

In E Division, the NSE unit relied on the extremist/terrorist unit of the NCIS for the collection and analysis of threat information.<sup>768</sup> NCIS generally just gathered information and forwarded it with comments to NCIB, relying on the HQ section for analysis of the information. CIS BC could provide an analysis of some of the threat information gathered.<sup>769</sup> However, its primary focus was on organized crime and the nature of the analysis it conducted was very basic and generally only done upon request.<sup>770</sup>

E Division NCIS was often unable to analyze the information in its possession or to use it to calibrate the potential for violence against Indian missions. In May 1985, when the threat to Indian interests in Canada was at a then all-time high,<sup>771</sup> the E Division OIC Operations inexplicably wrote to HQ that "...the assessment [of the threat to Indian interests] in this division at the present moment is at the nil or low threat level"<sup>772</sup> – this, in spite of the fact that Vancouver was considered by CSIS to be a "...hotbed of [Sikh extremism] activity,"<sup>773</sup> where many of the most dangerous Sikh extremist organizations and individuals, such as Parmar and the BK, as well as the ISYF, were operating.<sup>774</sup> On June 14, 1985, shortly after a prominent Sikh extremist commented at the Khurana meeting that something

---

<sup>767</sup> The Commission saw no indication that the information received by P Directorate from DEA or Air India was taken into account by NCIB. In some cases, NCIB members confirmed that they did not review relevant threat information: See, for example, Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2732, confirming that he did not review the June 1<sup>st</sup> Telex.

<sup>768</sup> Exhibit P-101 CAC0495, p. 3.

<sup>769</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4032.

<sup>770</sup> Final Submissions of the Attorney General of Canada, Vol. I, para. 87; Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3933. About the structure and mandate of CISBC, see Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

<sup>771</sup> See Section 1.12 (Pre-bombing), A "Crescendo" of Threats. CSIS, NCIB NSE and other sources indicated that the threat was high: See Exhibit P-101 CAC0338.

<sup>772</sup> Exhibit P-101 CAC0347.

<sup>773</sup> Exhibit P-101 CAB0207, p. 2.

<sup>774</sup> See, generally, Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces. See also April 1985 CSIS threat assessment: Exhibit P-101 CAB0221.

would be done in two weeks about the lack of attacks against Indian officials,<sup>775</sup> E Division NCIS wrote to HQ that it had no intelligence indicating "...that violent or criminal acts are planned for the Consulate or its personnel" and that it was "...unable to determine the potential for violence against the Indian Consulate or its personnel in Vancouver."<sup>776</sup>

The weaknesses in the Divisions' analysis were generally not remedied at the HQ level. Despite documentary references to NCIB's intended analytical role in the new RCMP threat assessment process,<sup>777</sup> NCIB NSE members did not see their role as involving a critical assessment of the overall threat situation or of the specific information received. Rather, they saw it as basically transmitting information to P Directorate and to RCMP Liaison Officers in other jurisdictions.<sup>778</sup> In general, NCIB forwarded correspondence received from the Divisions without providing any value added to the raw information.

### ***Analysis of the November Plot Information***

A graphic illustration of the limited analytic capacity of the RCMP threat assessment system is found in the response to the November Plot information.

When the information was initially received by NCIB, the divisional investigator's assessment that it was doubtful was passed to VIP Security. NCIB stated in its message to VIP Security that the information was forwarded "...in the event you may have an interest or other information", adding that other information had surfaced "...casting serious doubts on the validity/reliability of the information", which appeared to be "fabricated."<sup>779</sup> These comments were not the result of an independent analysis of the information, but were a repetition of the messages and information received from E Division.<sup>780</sup> At the time, NCIB only knew of one source for the information: Person 2. It was not aware of a second source, Person 1, who had earlier provided the same information. When NCIB did learn that there were two sources,<sup>781</sup> which was later said to make it "extremely unlikely" that the information was fabricated,<sup>782</sup> it did not question the Division's initial assessment of the information or contact P Directorate to update the assessment. NCIB did not request any further investigation of the information by the Division and seemed content to ask the Division only to provide updates about its investigation.<sup>783</sup>

<sup>775</sup> See Section 1.6 (Pre-bombing), Khurana Information. It is likely that NCIS was directly advised of this information, which was also available in to NCIS in the VIIU files: See Section 3.5.4 (Pre-bombing), RCMP Failures in Sharing with Local Forces.

<sup>776</sup> Exhibit P-101 CAC0438. See, generally, Section 1.6 (Pre-bombing), Khurana Information.

<sup>777</sup> See Exhibit P-101 CAC0283, p. 2. See also Exhibit P-120(c), p. 3 (entry for Nov. 8, 1984: doc CivLit1).

<sup>778</sup> This is how Sweeney, who was in charge of the terrorist desk at NCIB NSE, described his role in connection with the November Plot: Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2595.

<sup>779</sup> Exhibit P-120(c), p. 2 (entry for Oct. 30, 1984: doc 526-3, p. 29).

<sup>780</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2596-2597.

<sup>781</sup> Exhibit P-120(c), p. 2 (entry for Nov. 1, 1984: doc 526-3, pp. 26-27 and entry for Oct. 30, 1984: doc 526-3, p. 29).

<sup>782</sup> Exhibit P-120(c), p. 8 (entry for April 15, 1986: doc 526-3, pp. 1-22); Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2630-2632.

<sup>783</sup> Exhibit P-120(c), p. 3 (entry for Nov. 6, 1984: doc 526-3, p. 35).

CSIS had access to less information, but took the threat more seriously from the beginning. Even without being informed of the existence of another source, CSIS concluded from the Person 2 information that there was "...a real possibility that Sikhs will damage an Air India plane" and so advised Airport Policing.<sup>784</sup> Sweeney, who was following up the November Plot information, did not have the benefit of the CSIS threat evaluation before sending the E Division assessment to VIP Security.<sup>785</sup>

Aside from the poor information flow, the RCMP's ability to assess the November Plot threat was further impaired by tunnel vision that plagued both the divisional NCIS and HQ NCIB. NCIB members believed that the threat "was over" once Person 2 had been arrested.<sup>786</sup> In fact, the information received from Person 1 indicated that the plot was only put "on hold" after Person 2's arrest, and that Person 2 was actually making efforts to pursue the plot while in jail.<sup>787</sup> Yet, NCIB waited four months, until March 1985, to request an update when the Division stopped providing information about the investigation after November 1984, and even this update request was viewed as a simple routine follow-up matter.<sup>788</sup> NCIB did not appear to take this threat seriously, in spite of the obvious possibility that the plot could still be executed, and in the face of information tending to indicate that it might be.<sup>789</sup>

Even after the actual bombing of Air India Flight 182, the significance of the November Plot information continued to be overlooked. On the day of the bombing, neither the Division nor NCIB thought to pursue Person 2's offer to provide further information in exchange for an agreement or discussions about the unrelated charges he was facing.<sup>790</sup> Instead, they chose to take at face value his lawyer's assertion that Person 2 did not know anything about the Air India crash, and viewed Person 2's information with skepticism throughout the investigation because he was seeking to bargain away his charges.<sup>791</sup> It is ironic in the extreme that Person 2's offer was simply ignored in light of the fact that the unique access to individuals facing criminal charges, who might wish to trade valuable information in exchange for various benefits, was precisely cited as one of the important advantages of the RCMP's involvement in the threat assessment process.<sup>792</sup>

---

<sup>784</sup> Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 229-3, p. 5).

<sup>785</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2565, 2593-2594, 2597-2598.

<sup>786</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2611, 2613-2614.

<sup>787</sup> Exhibit P-120(c), p. 2 (entry for Nov. 1, 1984: doc 526-3, pp. 26-27). See Section 1.1 (Pre-bombing), November 1984 Plot.

<sup>788</sup> Exhibit P-120(c), p. 3 (entry for March 20, 1985: doc 526-3, p. 44); Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2611.

<sup>789</sup> See Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2614, where Sweeney agrees that according to the information available, it was possible that the November Plot could still be executed.

<sup>790</sup> Though Person 2's offer was not reported by NCIS immediately after the interview, Sweeney testified that he was aware in that general time frame that Person 2 "...want[ed] to deal": Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2616.

<sup>791</sup> Exhibit P-120(c), pp. 3-4 (entry for June 23, 1985: doc 526-3, p. 13) and p. 4 (entry for June 1985: doc 526-3, p. 59). See Section 2.3.1 (Post-bombing), November 1984 Plot and Section 1.1 (Pre-bombing), November 1984 Plot.

<sup>792</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5450-5451.



The potential significance of the November Plot information to the Air India investigation was apparently not recognized until September 1985, over two months after the bombing, when an analyst at the HQ Air India Task Force raised the issue and asked that further information be obtained from the Division.<sup>793</sup> This motivated NCIB to begin to request updates from E Division.<sup>794</sup> The analyst had joined NCIB after the bombing for purposes of the Air India investigation, and had to review a significant volume of material before being able to recognize the importance of the November Plot information.<sup>795</sup> Had NCIB NSE had a robust analytical capability from the beginning, the obvious potential relevance of the November Plot information likely would have been recognized earlier.

In any event, in spite of the Air India Task Force analyst's interest, it appears that the November Plot information continued to be viewed as not significant by NCIB members and divisional investigators.<sup>796</sup> Sweeney believed that the information was being pursued only to "tie up loose ends" and that it could not have anything to do with the Air India bombing.<sup>797</sup> E Division simply ignored NCIB's requests for information. In 1986, when the RCMP finally did pursue the November Plot "loose ends", information was uncovered which showed connections between the November Plot and the Air India bombing, including connections between conspirators and sources for the November Plot and Inderjit Singh Reyat.<sup>798</sup> Person 1 also successfully passed a polygraph test substantiating the information provided by Persons 1 and 2.<sup>799</sup> Sweeney testified that the new information obtained would have caused him to view the November Plot issue as more significant in the early stages of the Air India investigation,<sup>800</sup> as would the fact that Person 2 had mentioned the possibility of two planes being bombed before the Air India bombing took place,<sup>801</sup> information which was available to the RCMP but which it never obtained.<sup>802</sup>

The information which would have established the significance of the November Plot and its potential connection with the Air India bombing could only have been obtained through further investigation and follow-up. Because of analytical failures at the divisional and HQ levels, the issue was initially not considered to be worth investigating, and the information did not surface until much later, long after the Air India bombing had occurred and when the investigation was already well under way.<sup>803</sup>

---

<sup>793</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2617.

<sup>794</sup> Exhibit P-120(c), p. 4 (entry for Sept. 13, 1985: doc 526-3, p. 47 and subsequent telexes to the Division);

Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2617.

<sup>795</sup> Exhibit P-120(c), p. 8 (entry for April 15, 1986: doc 526-3, pp. 1-22).

<sup>796</sup> See Section 2.3.1 (Post-bombing), November 1984 Plot.

<sup>797</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2617-2618.

<sup>798</sup> See Section 2.3.1 (Post-bombing), November 1984 Plot.

<sup>799</sup> Exhibit P-120(c), pp. 8-9 (entry for May 1986: doc 23).

<sup>800</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2633-2636.

<sup>801</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2639.

<sup>802</sup> See Section 1.1 (Pre-bombing), November 1984 Plot.

<sup>803</sup> See Section 2.3.1 (Post-bombing), November 1984 Plot.



### ***Duplication of Effort***

The new RCMP threat assessment process created significant duplication of effort with CSIS, often replicating the same functions for the same information, often with no apparent value added.<sup>804</sup>

No effort was made to coordinate the new RCMP functions with CSIS's work in order to focus on information that the intelligence agency was not already pursuing.<sup>805</sup> RCMP Divisions were advised that their NSE units did not specifically need to request information from CSIS when responding to requests for threat information.<sup>806</sup> While NSE was instructed to maintain close liaison with CSIS, it was asked to "...check out threat assessments with CSIS" only where CSIS could provide criminal investigative leads.<sup>807</sup> In the meantime, the CSIS Threat Assessment Unit (TAU) continued its own separate liaison with RCMP Protective Policing.<sup>808</sup> As a result, CSIS Regions and RCMP Divisions would often be sending the same information for inclusion in threat assessments to the same RCMP P Directorate.

In practice, many, if not most, RCMP threat assessments were identical to the CSIS assessments, with both agencies relying on the same sources.<sup>809</sup> Further, because of the RCMP decentralized structure, CSIS HQ often received information from its Regions faster than NCIB did from its Divisions. As a result, more information would generally be available at CSIS HQ than at NCIB.<sup>810</sup> It seems not only duplicative but pointless to have had the RCMP reviewing and forwarding to P Directorate, through various divisional levels, information which CSIS would have sent earlier in any event.<sup>811</sup> Not surprisingly, RCMP divisional officers complained about this inefficient use of their resources.<sup>812</sup>

Further, divisional NSE units were instructed to review various newspapers and other publicly available materials to identify information "...of a criminal threat assessment value."<sup>813</sup> Such open source materials were said to contain "pre-incident" indicators to reflect the level of tension in various communities and to signal the possibility of law enforcement problems.<sup>814</sup> This was precisely the type of research that CSIS routinely performed in furtherance of its mandate to advise of threats to Canada's security. Information about potential "law enforcement problems" relating to security offences would also necessarily implicate the security of Canada and thus also fall within the CSIS mandate.

---

804 Exhibit P-101 CAC0406, p. 3.

805 Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2574-2576.

806 Exhibit P-101 CAC0495, p. 4.

807 Exhibit P-101 CAC0495, p. 4.

808 Exhibit P-101 CAA0039(i), p. 51.

809 Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2574.

810 Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2726-2727.

811 Once received by P Directorate, the information would become available to NCIB through RCMP central records: Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2653-2655.

812 Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2574; Exhibit P-101 CAC0406, p. 3.

813 Exhibit P-101 CAC0495, p. 5.

814 Exhibit P-101 CAC0495, pp. 4-5.

Hence, duplication was inevitable. It made no sense to have both agencies review the same materials for the same purpose. With no explanation about the nature of the information with “criminal threat assessment value”, as opposed to the general threat assessment value CSIS was looking for, there was little hope the work could be effectively coordinated at the regional level.

### **Definition of RCMP Role in the Threat Assessment Process**

In 1986, Ron Atkey, Chairman of the Security Intelligence Review Committee (SIRC), wrote the following margin notes about directives of the Solicitor General on measures to improve CSIS/RCMP cooperation:

Until someone defines the difference between security intelligence and criminal intelligence in this area of common concern; ... all this will represent is a papering over of the cracks.<sup>815</sup>

The lack of a clear and universally accepted definition of the concept of “criminal intelligence” and how it was to be distinguished from “security intelligence” plagued the RCMP in its early attempts to adjust to the creation of CSIS. It was largely because the concept was never properly understood or defined that the RCMP was unable to find its proper place in assessing and responding to the threat of Sikh extremism.

The threat assessment process set up by the RCMP was, in some respects, based on undefined, and in some cases questionable, assumptions about the respective RCMP and CSIS mandates. As a result, it was difficult for the RCMP to develop a unified or coherent vision of the nature, scope and purpose of its involvement in the threat assessment process and to adequately explain the objectives of its threat assessment process to its members. This lack of clarity had an impact on the RCMP’s ability to identify, report and investigate threat information.

When the Government decided to create CSIS, there was a perception in the RCMP that a gap was created which would prevent it from carrying out its policing activities, in particular with respect to national security offences and terrorism.<sup>816</sup> Many in the RCMP felt that relying exclusively on CSIS for the Force’s intelligence needs was neither realistic nor workable.<sup>817</sup> Given its own mandate, the Force saw that overlap was inevitable in the field of security offences.<sup>818</sup> It was believed that the RCMP needed to retain a complementary role in intelligence-

---

<sup>815</sup> Exhibit P-101 CAA0484, p. 6. See also Testimony of Ronald Atkey, vol. 49, September 20, 2007, pp. 5981-5982.

<sup>816</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5358-5359, 5396.

<sup>817</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5360, 5373-5374; Testimony of Robert Simmonds, vol. 74, November 8, 2007, pp. 9331-9332, 9338.

<sup>818</sup> Exhibit P-101 CAC0030, pp. 2, 4.

gathering for information connected to law enforcement activities.<sup>819</sup> In particular, Commissioner Simmonds indicated that no clear dividing line could be drawn between the role and responsibilities of CSIS and the RCMP in the realm of counterterrorism.<sup>820</sup> Because terrorist acts are criminal,<sup>821</sup> the RCMP viewed terrorism-related intelligence-gathering work as part of its core law enforcement mandate.<sup>822</sup> Simmonds explained that in his view, the *CSIS Act* did not give CSIS primacy in the area of intelligence-gathering relating to terrorism and did not exclude the RCMP, since no legislative amendments limited the "... traditional and needed role of the police force."<sup>823</sup>

The RCMP adopted the concept of "criminal intelligence" to describe the new role it intended to assume in intelligence-gathering and threat assessment. As Atkey correctly perceived, the distinction between criminal and security intelligence was untenable and incapable of definition. The new RCMP threat assessment process appears simply to have assumed that members would know the difference between "security intelligence" and "criminal intelligence" when they saw it, even though the upper echelons of the Force understood that there was no clear demarcation.<sup>824</sup> The repeated use of equally undefined concepts, such as "legitimate law enforcement interest,"<sup>825</sup> to describe the scope of RCMP intelligence-gathering activities did nothing to ease the confusion about the role of the RCMP and its relationship to CSIS in the area of intelligence collection.

Not surprisingly, members in the Divisions remained unsure of the RCMP's threat assessment mandate and its relationship to CSIS threat assessment.<sup>826</sup> At NCIB itself, there was initially no clear understanding of the role of NSE vis-à-vis the CSIS TAU which continued to have a direct relationship with P Directorate, the main consumer of threat assessments.<sup>827</sup> P Directorate itself was uncertain about the role that NCIB NSE was supposed to carry out and, as a result, did not generally view NCIB as a resource for information or assessments.<sup>828</sup>

At times, the RCMP threat assessment process was misunderstood by those very members in charge of implementing it. The NSE responsibility to collect and report threat assessment information was not understood clearly within the RCMP in light of NSE's lack of an investigative role.<sup>829</sup> At H Division, the DIO, whose duties included assigning follow-up investigations of threat information

<sup>819</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5372.

<sup>820</sup> Exhibit P-101 CAA0474, pp. 8-10; Testimony of Robert Simmonds, vol. 74, November 8, 2007, p. 9345.

<sup>821</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2576. See also Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1666 and Exhibit P-101 CAA0474, p. 8, where Simmonds wrote "...we view terrorists as criminals and we view their activities as crime."

<sup>822</sup> Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2575-2576.

<sup>823</sup> Testimony of Robert Simmonds, vol. 74, November 8, 2007, pp. 9328, 9351-9353.

<sup>824</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1662. See also the Ministerial Directive recognizing this: Exhibit P-101 CAA0081, p. 12.

<sup>825</sup> Exhibit P-101 CAA0039(i), p. 16.

<sup>826</sup> Exhibit P-101 CAC0406, p. 3.

<sup>827</sup> Exhibit P-101 CAA0039(i), p. 51.

<sup>828</sup> Exhibit P-101 CAC0278; Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2578; Testimony of R.E. Muir, vol. 28, May 15, 2007, p. 2934; Testimony of J.B. MacDonald, vol. 27, May 14, 2007, pp. 2809-2810, 2888.

<sup>829</sup> Exhibit P-101 CAC0495, p. 2.

to appropriate investigative units at NSE's request,<sup>830</sup> was of the view that, because of the lack of investigative mandate or capacity at NSE, the RCMP was "totally dependent" on CSIS for intelligence collection and analysis.<sup>831</sup> The Commanding Officer of the same Division, for his part, was under the impression that the purpose for establishing RCMP units to collect intelligence and investigate dissident individuals and groups<sup>832</sup> was "...to replace the RCMP Security Service that was lost when CSIS was established."<sup>833</sup>

Some of the rationales invoked to explain the necessity of the new RCMP threat assessment process also added to the confusion.

The security offences mandate conferred on the RCMP in the *CSIS Act*<sup>834</sup> was sometimes described as a "new" mandate involving additional responsibilities and justifying new activities for the criminal operations side of the Force.<sup>835</sup> In fact, the security offences mandate was not truly new. The RCMP was always responsible for investigating offences relating to national security as part of its federal "security enforcement" duties and was always responsible for a wide range of protective policing activities.<sup>836</sup> The only practical difference which resulted from the legislative statement in the *CSIS Act* was that the RCMP was now granted primary jurisdiction nationwide, whereas traditionally provincial or local forces had been responsible for law enforcement activities in their respective jurisdictions for all offences.<sup>837</sup> Further, the RCMP protective policing responsibilities – sometimes portrayed as expanding and viewed as requiring the Force to acquire its own threat assessment capacity because of an increase in violent or potentially violent activities targeting protected persons and missions<sup>838</sup> – had also formed part of the RCMP's responsibilities for a long time and had not previously been seen as necessitating the creation of an independent threat assessment process on the criminal operations side of the Force.

CSIS's mandate did not prevent it from continuing to provide the necessary threat information and assessments which the Security Service used to provide,<sup>839</sup> and the RCMP's mandate, whether in relation to protective policing or "security offences", did not require it to perform this intelligence-gathering itself. The fact

830 Exhibit P-101 CAC0283, p. 6.

831 Exhibit P-101 CAA0531, p. 2.

832 This was said to have been proposed in a Commissioner's Strategic Issues Paper: Exhibit P-101 CAA0144, p. 1. Note that the Strategic Issues Paper appears to be the document described in Exhibit P-101 CAA0162 as a March 1985 draft Strategic Plan prepared by the Planning and Evaluation Branch.

833 Exhibit P-101 CAA0144, p. 1.

834 S.C. 1984, c. 21, s. 61(1).

835 See, for example, Exhibit P-101 CAC0286, p. 2 and Exhibit P-101 CAC0495, p. 5. The security offences mandate was also perceived as conferring on the RCMP "...new and added responsibilities regarding the protection of Canada's Diplomatic Community," in addition to the traditional RCMP protective policing responsibilities with respect to foreign missions and personnel: Exhibit P-101 CAC0214, p. 2, CAC0216(i), p. 2.

836 Exhibit P-101 CAA0081, pp. 3-4.

837 Exhibit P-101 CAA0081, p. 6; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5398.

838 Exhibit P-101 CAC0283, pp. 4-5, CAC0495, p. 5.

839 According to the Minister, that mandate was, on the contrary, "...sufficiently broad to permit the Service to satisfy RCMP security intelligence needs": Exhibit P-101 CAA0081, pp. 8-9.

that the Security Service had been taken away from the RCMP did not necessarily have to create a gap in the threat assessment process. However, some gaps did already exist in the pre-existing threat assessment process or could have resulted from the creation of a separate intelligence agency. Unfortunately, the new RCMP process did not address these issues.

### **Failure to Address Gaps**

Long before the creation of CSIS, gaps were evident in the Security Service threat assessment process. The Security Service in many respects operated separately from the rest of the RCMP.<sup>840</sup> It often did not have access to the information gathered by the criminal operations side of the Force. As a result, for the four years preceding the creation of CSIS, members of the Security Service Threat Assessment Unit (TAU) had repeatedly requested a role for C Directorate (the criminal operations side of the RCMP) in the threat assessment process. The TAU members attempted to provide threat assessments “more or less” from a Force “perspective”, but could not fully explore and report criminal aspects.<sup>841</sup>

Because the Security Service did not have access to threat information obtained by the RCMP in the conduct of its regular policing activities, relevant information was excluded from its threat assessment process. As a law enforcement agency, the RCMP had unique access to information from a wide range of individuals facing criminal charges and willing to trade information for various benefits or advantages.<sup>842</sup> Proven law enforcement approaches, such as the use of undercover agents, informants, *Criminal Code* wiretaps and search warrants, would inevitably gather intelligence which could serve to prevent terrorist acts.<sup>843</sup> None of this information would normally find its way into the Security Service threat assessment process. The creation of an RCMP threat assessment process after the Service’s separation from the Force would have been a perfect opportunity to address this issue. Instead, the RCMP created a parallel structure and, as it focused on its own requirements and had difficulty ensuring that information was reported centrally in its own system, it did not always provide CSIS with access to the security-related information its investigative units obtained.

Without access to all relevant information, CSIS’s ability to assess the threat was impaired. CSIS complained about what it viewed as the RCMP’s intention to develop “...a completely parallel investigative capability.”<sup>844</sup> SIRC also expressed concerns about the potential RCMP parallel intelligence-gathering capability, which could conflict with CSIS responsibilities and even represent a step backward from the McDonald Commission.<sup>845</sup> Wanting to ensure that it obtained all the intelligence necessary to conduct its protective and preventative policing

<sup>840</sup> Testimony of Robert Simmonds, vol. 74, November 8, 2007, pp. 9317-9318.

<sup>841</sup> Exhibit P-101 CAC0275, p. 2.

<sup>842</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5450.

<sup>843</sup> Exhibit P-101 CAA0474, pp. 8-10.

<sup>844</sup> Exhibit P-101 CAA0162, p. 3, CAA0293, p. 1, CAA0444, CAA0531, p. 1, CAC0029, CAC0030.

<sup>845</sup> Exhibit P-101 CAA0474, CAA0507; Exhibit P-144: *Security Intelligence Review Committee Annual Report 1985-86*, p. 7 [SIRC 1985-86 Annual Report].

operations, the RCMP actually missed the opportunity to resolve an operational problem which could weaken the assessments of the intelligence agency on which it was to rely.

### ***Possibility of Delay***

There were issues related to the creation of a separate intelligence agency which, if left unaddressed, would compromise the utility of CSIS threat assessments to the RCMP. One such issue was the possibility of delay.<sup>846</sup> Security enforcement could be carried out by the RCMP on the basis of CSIS intelligence, but the information would have to be received in a timely manner.<sup>847</sup> For protective policing, delay could lead to the failure to take action in time. For “security offences” investigations, delays could compromise the criminal investigative tools needed for a subsequent prosecution.<sup>848</sup> This real and important concern was not resolved when the RCMP created its own threat assessment process. On the contrary, the RCMP system often involved more delays in the reporting of information than the CSIS system already in place.

### ***Judicial Process Issues***

Other potential issues with the reliance of the RCMP on CSIS threat assessments were related to the judicial process.<sup>849</sup> In cases where threats materialized or conspiracies were hatched, the RCMP would be conducting criminal investigations. If RCMP members sought search warrants or wiretap authorizations under the *Criminal Code*, they could be legally required to disclose any CSIS information in their possession.<sup>850</sup> If CSIS then successfully objected to having its information made public, it could jeopardize subsequent criminal prosecutions.<sup>851</sup> To the extent that the RCMP had to rely on CSIS information in prosecutions, concerns could arise where the information was not collected in accordance with applicable evidentiary standards.<sup>852</sup> Such downstream issues, involving subsequent use of CSIS threat assessment materials were not, strictly speaking, relevant to the actual purpose of threat assessments for protective policing or for preventive purposes, but were understandably of concern to the RCMP.

---

<sup>846</sup> The RCMP needed to receive information in a timely manner in order to be able to take any action necessary: Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5361, 5372-5373; Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1665. See also Exhibit P-101 CAA0474, p. 11, CAC0030, where Simmonds expressed these concerns in August 1986, and Exhibit CAD0027, pp. 3-4, where the Solicitor General expressed the same concerns in May 1985.

<sup>847</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1674.

<sup>848</sup> Exhibit P-101 CAD0027, p. 3.

<sup>849</sup> Testimony of Robert Simmonds, vol. 74, November 8, 2007, pp. 9328, 9331.

<sup>850</sup> See Section 4.4 (Post-bombing), CSIS Information in the Courtroom and Section 4.1 (Post-bombing), Information Sharing and Cooperation in the Air India Investigation.

<sup>851</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1657-1658; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5366, 5369; Testimony of Robert Simmonds, vol. 74, November 8, 2007, pp. 9326-9327, 9329.

<sup>852</sup> See Section 4.3.1 (Post-bombing), Tape Erasure and Section 4.3.2 (Post-bombing), Destruction of Operational Notes.



The issue of subsequent use of intelligence in the judicial process, which already existed in the Security Service days,<sup>853</sup> was not resolved through the creation of the parallel RCMP threat assessment process. On the contrary, the issue became extremely important in the RCMP post-bombing investigation.<sup>854</sup> The model envisaged in the *CSIS Act* and the Ministerial Directive attempted not only to separate intelligence-gathering from criminal investigations and prosecution, but also to avoid duplication. While this strict separation of mandates could create problems in subsequent prosecutions, especially in light of legal disclosure requirements, the creation of a separate RCMP system for assessing “criminal intelligence”, as opposed to the “national security intelligence”, could not achieve the twin goal of before-the-fact prevention through adequate threat assessment and after-the-fact prosecution through access to evidence which could be admissible in a court of law. As shown in the Air India investigation itself, it was inevitable that CSIS would gather some information which could be relevant to subsequent prosecutions, regardless of the existence of an RCMP threat assessment process. Meanwhile, the parallel process deprived CSIS of the opportunity to perform a global assessment of all relevant threat information.

## Conclusion

The threat assessment process set up by the RCMP was not well-adapted to gathering, centrally assessing and investigating threat information. It relied on units that were not sufficiently trained or resourced to perform their intended assessment role. The process was overly decentralized, which prevented the adequate control of investigations. The RCMP reporting structure prevented the Force from being able to respond to threat information in a timely manner. The RCMP proved incapable of drawing on information already in its possession, or of aggregating information from sources to which it had unique access, and it brought no special analytical skills to bear in order to identify the national security significance of information. RCMP threat assessments largely duplicated CSIS’s work, to little positive effect and, in some cases, with negative results.

## 3.5 Information-Sharing Failures

### 3.5.1 CSIS/RCMP Relations and Information-Sharing Policies

#### Introduction

During the period immediately preceding the Air India bombing, information did not always flow smoothly between CSIS and the RCMP. The agencies struggled to make sense of the new legislation and policies focussed on separating their mandates. They tried to implement information-sharing mechanisms within the siloed intelligence system created by government. At times, the efforts of individuals within each agency to maintain and improve information sharing, despite legislative shackles and practical difficulties, were commendable. In

<sup>853</sup> Testimony of Robert Simmonds, vol. 74, November 8, 2007, pp. 9326-9327.

<sup>854</sup> See Section 4.1 (Post-bombing), Information Sharing and Cooperation in the Air India Investigation.



many other instances, however, members of both agencies seemed to lose track of the higher purposes they were pursuing. Growing tensions, high-level debates, mistrust and legalistic arguments often characterized the early relationship between CSIS and the RCMP. Those tensions had an impact on the amount of information exchanged and on the sources of information available to CSIS.

### ***CSIS/RCMP Information-Sharing Policies***

Information sharing between the RCMP and CSIS was recognized as a major area of concern during the CSIS transition. The development of the MOU for the Transfer and Sharing of Information<sup>855</sup> was one of the most important and most contentious issues for the Security Intelligence Transition (SIT) Group.

In the Memorandum of Understanding (MOU), signed immediately after the creation of CSIS on July 17, 1984, the two agencies agreed to share any information relevant to each other's roles and responsibilities as the information became known or available, or upon request. The MOU clearly stated that neither agency would have an unrestricted right of access to the records of the other agency. The MOU assigned to the Solicitor General the role of adjudicator in the case of information-sharing disagreements. While the MOU provided general information-sharing principles, it left the responsibility for establishing specific procedures to implement these principles to the CSIS Director and the RCMP Commissioner.

Professor Wesley Wark described the situation set out by the 1984 MOU as a "... silo arrangement ... connected by an informational ramp", in which information flowed only one way: from CSIS to the RCMP.

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.<sup>856</sup>

The Solicitor General, the Honourable Robert Kaplan, recognized the potential for overlap and duplication between CSIS's security intelligence function, as set out by the *CSIS Act*, and the RCMP's security enforcement function, as set out in the *Security Offences Act* component of the same Act. While the main body of the *CSIS Act* established CSIS as the agency charged with collecting intelligence, the *Security Offences Act* (which began life as a part of the *CSIS Act*) assigned the RCMP primary responsibility to perform peace officer duties in relation to offences deemed to be threats to the security of Canada (security enforcement)

---

<sup>855</sup> Exhibit P-101 CAA0076.

<sup>856</sup> Wesley Wark, "The Intelligence-Law Enforcement Nexus: A study of co-operation between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, 1984-2006, in the Context of the Air India terrorist attack" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation, p. 172.

or offences against internationally protected persons (protective policing). Minister Kaplan issued a Ministerial Directive on July 29, 1984 laying down six principles to guide the discharge of the security responsibilities of CSIS and the RCMP.<sup>857</sup>

- The RCMP will rely on CSIS for intelligence relevant to national security offences;
- CSIS will pass to the RCMP intelligence relevant to RCMP security enforcement and protective security responsibilities;
- The RCMP will pass to CSIS information relevant to the CSIS mandate;
- The RCMP will be the primary recipient of security intelligence on national security offences and responsible, where they consider it necessary, for the passage of such intelligence to local enforcement authorities;
- The RCMP and CSIS will consult and cooperate with each other with respect to the conduct of security investigations;
- The RCMP and CSIS will conduct security investigations in accordance with guidelines, standards and direction provided by the Solicitor General.

The first principle clearly affirmed CSIS primacy in the field of security intelligence: the RCMP would *rely* on CSIS for intelligence relevant to national security offences. Another principle directed the RCMP to pass to CSIS information relevant to its mandate.<sup>858</sup> In effect, CSIS was intended to be a repository of intelligence information, with the RCMP stripped of any mandate to undertake security intelligence analysis. However, Minister Kaplan anticipated the need for close liaison between CSIS and the RCMP to ensure that national security measures were dealt with effectively and efficiently. The Ministerial Directive authorized the RCMP Commissioner to establish a dedicated liaison unit to facilitate information sharing.

In some ways, the Ministerial Directive<sup>859</sup> illustrates the intention for a two-way information flow between CSIS and other agencies, including the RCMP, envisioned by the *CSIS Act*. Yet, the *CSIS Act*, the MOU and the Kaplan directive all also emphasize maintaining separation between the law enforcement and security intelligence functions of the RCMP and CSIS. According to Wark,

---

<sup>857</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, pp. 1468-1469.

<sup>858</sup> Exhibit P-101 CAF0030, pp. 9-10. See the related document focusing on the RCMP role in security investigations at Exhibit P-101 CAA0081.

<sup>859</sup> Exhibit P-101 CAF0030.

intelligence failures have been identified as inevitable consequences of maintaining such separation.

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 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 .... [I]n [the government's] desire to separate out intelligence from law enforcement, it created a system that was overly rigid, that made sense in theory, but wasn't going to make sense at the end of the day, in practice. It took us a long time, I think, to recognize the practical deficiencies of this theory, because we were wedded to the theory – the theory itself.<sup>860</sup>

The Government of Canada had established a siloed intelligence system.<sup>861</sup> The focus was on ensuring that the mandates and roles of CSIS and the RCMP remained distinct and separate, in response to the recommendations of the McDonald Commission. The policies called for cooperation, but failed to provide the operational bridges to ensure efficient and effective cooperation between these “siloed” agencies.<sup>862</sup>

### ***Interagency Relations***

Tensions often arose between the RCMP and the new intelligence agency during the years following the creation of CSIS. The agencies became involved in a number of long-running disputes over their mandates in the national security field, which led to reluctance to share intelligence, both prior to the Air India bombing and in its aftermath. The results were detrimental to the security interests of Canada.

At the senior level, there were debates on matters of principle. The RCMP perceived the “national enforcement” duties granted in the *Security Offences Act* as powers that would require it to develop new intelligence collection capabilities to support its investigations into national security offences. CSIS expressed concern that RCMP intelligence-gathering activities infringed on its mandate. The RCMP vigorously disagreed.<sup>863</sup> The RCMP Deputy Commissioner of Operations and the CSIS Director General of Foreign Liaison are recorded as having a “...rather stark divergence of opinion” about the appropriate roles for the two agencies in national security investigations, and about the RCMP’s

---

<sup>860</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, pp. 1469-1470, 1475.

<sup>861</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, p. 1486.

<sup>862</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, pp. 1486-1487.

<sup>863</sup> See, for example, Exhibit P-101 CAA0444, CAA0531, p. 1, CAC0029, pp. 1-2. See also Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5424.

intention to develop what CSIS saw as a parallel investigative capability.<sup>864</sup> Deputy Commissioner Henry Jensen thought the CSIS concerns were slightly paranoid, and ultimately motivated by a fear that the RCMP might target CSIS sources, reveal their identity or expose them to prosecution.<sup>865</sup> High-level correspondence passed between the agencies on this issue, with the Security Intelligence Review Committee (SIRC) and the Solicitor General being informed and participating.<sup>866</sup>

The RCMP concern was that it was not receiving the information it needed from CSIS. Section 19 of the *CSIS Act* provided that "...the Service *may* disclose information" to police, where the information could be used for "investigation or prosecution" of offences.<sup>867</sup> The MOU about the transfer and sharing of information between CSIS and the RCMP provided that "CSIS *shall* provide ...to the RCMP as it becomes known/available" information relevant to a number of RCMP responsibilities, including the investigation of criminal offences relating to national security.<sup>868</sup> The RCMP interpreted the MOU as making CSIS disclosure mandatory, despite the discretion conferred by the *CSIS Act*.<sup>869</sup> CSIS disagreed and interpreted section 19 as permitting CSIS to disclose, but leaving the final discretion in the hands of the CSIS Director.<sup>870</sup> The discrepancy between the MOU and the *CSIS Act* "...prompted operational confusion between the two agencies on the obligation or discretion to share information,"<sup>871</sup> and left a dysfunctional system, one more susceptible to fail in the war on terror.

Debate arose because of the RCMP view, supported by a Cabinet decision, that it was to play the role of an intermediary between CSIS and local police forces for the purposes of passing on national security intelligence.<sup>872</sup> CSIS rejected this view because the Service feared that unless information could be exchanged directly with local and provincial forces, the police agencies might hold back important intelligence in the belief that CSIS was not being cooperative.<sup>873</sup> CSIS wanted to continue its direct and sustained exchanges of information with local and provincial police forces,<sup>874</sup> while the RCMP feared that such exchanges would cut them out of the information loop and perhaps lead to local forces acting unilaterally on the basis of CSIS information.<sup>875</sup> The result was yet more debate<sup>876</sup> and high-level exchanges of correspondence,<sup>877</sup> including RCMP complaints that CSIS information transfers to local forces violated RCMP/CSIS

---

864 Exhibit P-101 CAA0293.

865 Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5434-5435, 5453.

866 Exhibit P-101 CAA0474, CAC0029, CAC0030.

867 *CSIS Act*, S.C. 1984, c. 21, s. 19 (R.S.C. 1985, c-23, s. 19) [Emphasis added].

868 Exhibit P-101 CAA0076; Exhibit P-105, Tab 2 [Emphasis added].

869 Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1651, 1654-1656, 1676-1677.

870 See Section 4.0 (Post-bombing), The Evolution of the CSIS/RCMP Memoranda of Understanding.

871 Final Submissions of the Attorney General of Canada, Vol. I, para. 61.

872 Exhibit P-101 CAA0081, p. 3. See also Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5400-5401 and Exhibit P-101 CAA0039(i), p. 14, CAA0162, p. 1, CAB0189.

873 Exhibit P-101 CAA0154(i), p. 3; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5398-5399.

874 Exhibit P-101 CAA0154(i), p. 3, CAA0162.

875 Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5399, 5403.

876 Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5400-5401. See Exhibit P-101 CAA0237 and CAB0442, mentioning "interminable discussions leading merely nowhere."

877 Exhibit P-101 CAA0131, CAA0277, CAB0169.

agreements.<sup>878</sup> At times, the RCMP even opposed CSIS participation in Joint Forces Operations, proposing instead that the RCMP act as an intermediary.<sup>879</sup>

There were tensions in the field as well. Sgt. Wayne Douglas, the Head of the NCIS Terrorist/Extremist group at E Division, testified that while there may have been some restrictions on the movement of information between criminal operations and the Security Service section of the Force prior to the creation of CSIS, the relationship was a very good one and there was a "...free flow of information." Members could go to the Security Service building anytime, sit down to have an "informal chat" and move freely around the building – they were "...part of the family". After the creation of CSIS, however, requests for information had to be made formally through the CSIS liaison. It took an unacceptable amount of time to obtain the information, and then some of it would usually be "blacked out". Douglas explained that some RCMP members experienced "frustration", or felt "affronted", when CSIS said it was unable to provide certain information to the RCMP.<sup>880</sup>

Vancouver Police Department (VPD) members of the Vancouver Integrated Intelligence Unit (VIU), to which E Division NCIS was attached, noticed that relations between CSIS and the RCMP appeared strained. Former VIU member Supt. Axel Hovbrender testified that there was a "...fundamental shift in attitude" after the Security Service went over to CSIS. This new tension in RCMP/CSIS relations impacted on the interagency sharing of intelligence and information in the course of everyday operations in the Division.<sup>881</sup> VPD members of the VIU felt that CSIS investigators often used them as a conduit to pass information to the RCMP, because strained relations between CSIS and the RCMP made it more difficult to transmit the information directly.<sup>882</sup>

### **Access to CPIC**

CSIS access to the Canadian Police Information Computer (CPIC) became the subject of acrimonious debate in the years following the creation of the new agency,<sup>883</sup> and led to comment in at least three annual reports from the Security Intelligence Review Committee (SIRC).<sup>884</sup>

---

<sup>878</sup> Exhibit P-101 CAB0189. Ultimately, CSIS took the position that where the RCMP claimed jurisdiction or the Minister established that an investigation was covered by the *Security Offences Act*, CSIS information would be forwarded exclusively to the RCMP, except where a Joint Forces Operation (JFO) was in place, in which case it would be forwarded to all participants simultaneously. In all other cases, all information would continue to be passed to the RCMP pursuant to the MOU, but CSIS could also, at its discretion, pass information directly to local forces without using the RCMP as an intermediary: See Exhibit P-101 CAA0054(i), CAA0162, pp. 6-7, CAA0237, pp. 1-2 and CAA0277, p. 1.

<sup>879</sup> Exhibit P-101 CAA0162, p. 5.

<sup>880</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4036-4037, 4111-4112.

<sup>881</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3875, 3917-3918.

<sup>882</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3875, 3917.

<sup>883</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1645.

<sup>884</sup> Exhibit P-143: *Security Intelligence Review Committee Annual Report 1984-85* [SIRC 1984-85 Annual Report], p. 13; Exhibit P-144: *SIRC 1985-86 Annual Report*, pp. 22-23; Exhibit P-145: *Security Intelligence Review Committee Annual Report 1986-1987*, pp. 14-15 [SIRC 1986-87 Annual Report].

CPIC, a computerized, radio-linked network available to police officers across Canada, provided instant access to a wide range of information about individuals, including criminal records, police records, missing persons, stolen property, outstanding warrants, vehicle registration and driver's licence information.<sup>885</sup> CPIC made it possible for investigators interested in a particular target, or "person of interest", to be notified any time a police officer, who encountered that person anywhere in the country, queried the name.<sup>886</sup> As peace officers, RCMP Security Service members had full access to CPIC and its data banks in furtherance of their security intelligence probes.<sup>887</sup>

When CSIS was created, the CPIC access, formerly available to Security Service members directly through their own terminals, ceased.<sup>888</sup> The reason given was that once Security Service personnel went over to CSIS, they became civilians, not peace officers, and no longer qualified for access.<sup>889</sup>

SIRC believed that direct access to CPIC was essential for CSIS personnel to carry out their functions,<sup>890</sup> stating that immediate access to vehicle registration information was invaluable in identifying surveillance targets.<sup>891</sup> Without CPIC access, CSIS personnel "...in hot pursuit of a suspected terrorist" could not obtain needed information; at the same time, police officers throughout Canada could use the CPIC terminals in their vehicles for the most trivial purposes, such as enforcing anti-loitering bylaws.<sup>892</sup> Bill Turner of CSIS also explained that it was important to obtain criminal records information about persons CSIS intended to approach to ensure that they had no history of violence so CSIS investigators did not get into a violent situation.<sup>893</sup>

SIRC rejected the "peace officer" rationale for denying CSIS access to CPIC as "nit-picking" – if there was no problem in CPIC access for Security Service members, there should be no problem in access for CSIS investigators doing exactly the same job.<sup>894</sup>

Though access to CPIC was governed by the CPIC Advisory Committee, a board of representatives from provincial, municipal and regional police forces,<sup>895</sup> SIRC

<sup>885</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1645-1647; Exhibit P-144: SIRC 1985-86 Annual Report, p. 22; Exhibit P-145: SIRC 1986-87 Annual Report, p. 14.

<sup>886</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1646. This could be done as a "silent hit", without notification to the officer making the encounter, who could be contacted at a later date to gather additional information or intelligence.

<sup>887</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1646-1647; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5381.

<sup>888</sup> Exhibit P-143: SIRC 1984-85 Annual Report, p. 13.

<sup>889</sup> Exhibit P-145: SIRC 1986-87 Annual Report, p. 14; Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1645, 1648; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5381.

<sup>890</sup> Exhibit P-143: SIRC 1984-85 Annual Report, p. 13; Exhibit P-144: SIRC 1985-86 Annual Report, p. 22; Exhibit P-145: SIRC 1986-87 Annual Report, p. 14.

<sup>891</sup> Exhibit P-145: SIRC 1986-87 Annual Report, p. 14.

<sup>892</sup> Exhibit P-145: SIRC 1986-87 Annual Report, p. 15.

<sup>893</sup> Testimony of Bill Turner, vol. 66, October 25, 2007, pp. 8280-8282.

<sup>894</sup> Exhibit P-145: SIRC 1986-87 Annual Report, pp. 14-15.

<sup>895</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1645-1646; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5381.



was of the view that it was the RCMP that was responsible for the reluctance to grant direct access to CPIC.<sup>896</sup> In its 1986-87 Annual Report, SIRC cited the difficulty in gaining access to CPIC as an example of agencies "...giving priority ... to parochial turf concerns", again pointing the finger at the RCMP.<sup>897</sup> Accurate or not, such allegations illustrate the level of interagency tension in the relationship at the time.

As head of Law Enforcement Services, Jensen was mandated at the time with addressing the CPIC issue on behalf of the RCMP. He testified that the RCMP was not motivated by any "turf war" concerns<sup>898</sup> and denied that the Force had ever objected to direct CPIC access for CSIS.<sup>899</sup> He pointed to objections from municipal and provincial police forces as the cause for denying CPIC access to CSIS.<sup>900</sup> Jensen explained that the RCMP did not have a majority of votes at the CPIC Committee, and was unable to win the support of local forces for RCMP proposals to grant CSIS access. He stated that these proposals were presented and rejected many times at annual CPIC Committee meetings.<sup>901</sup> He explained that, despite extraordinary steps by RCMP in support of CSIS access (including obtaining a director position with the Canadian Association of Chiefs of Police (CACAP) for purposes of lobbying in favour of the proposal), it was not until approximately four or five years after the creation of CSIS that the RCMP proposal finally carried the majority on the issue.<sup>902</sup>

The full record about this matter is somewhat less straightforward. The RCMP's initial position was to support limited CSIS access to CPIC, confined to motor vehicle information.<sup>903</sup> The Force approached the CPIC Committee with this proposal in September 1985<sup>904</sup> and began to make arrangements for the installation of terminals, anticipated for August 1986, once consent from the provinces had been obtained. In 1986, the RCMP also agreed, after considering the matter for some time, to raise the broader issue of CSIS access to criminal records data at the next CPIC Advisory Committee meeting.<sup>905</sup> Meanwhile, however, SIRC entered the debate with strongly worded comments in its 1985-

---

<sup>896</sup> SIRC wrote that the RCMP was a "major participant" in the CPIC Committee which continued to deny direct CPIC access to CSIS: Exhibit P-144: SIRC 1985-86 Annual Report, p. 22.

<sup>897</sup> Exhibit P-145: SIRC 1986-87 Annual Report, p. 15.

<sup>898</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5380-5381, 5452-5453.

<sup>899</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1650. The RCMP was, on the contrary, "...anxious for CSIS to have direct access" to CPIC: Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5393.

<sup>900</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1648-1659. The issues included provincial concerns about making driver's licence and vehicle registration information available without the assurance that it would only be used for legitimate law enforcement purposes.

<sup>901</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1645-1646; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5392-5393. See also Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5469, indicating that the RCMP had made attempts to convince the CPIC Committee to grant access to CSIS since 1984.

<sup>902</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1671-1672; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5393-5394, 5469.

<sup>903</sup> This was after RCMP Identification Services and the CPIC Advisory Secretariat had recommended in July 1985 that the RCMP Commissioner support CSIS's approach for access to RCMP criminal history and motor vehicle databases: Exhibit P-101 CAD0035, p. 3.

<sup>904</sup> Exhibit P-101 CAA0398, CAD0035, p. 3.

<sup>905</sup> Exhibit P-101 CAA0398, CAA0474, pp. 11-12.



86 Report.<sup>906</sup> In response, the RCMP Commissioner wrote to the Solicitor General with a list of factors militating against more general direct access for CSIS. The letter pointed out that, because they were not peace officers, CSIS personnel would not have the necessary powers to fulfill the requirement that CPIC information be verified prior to its use. Unlike peace officers, CSIS personnel had no authority to fingerprint suspects, to stop vehicles to check their occupants or to conduct interviews in the course of criminal investigations as means of verification. Also mentioned was the fact that other police agencies provided access to criminal records information for law enforcement and administration of justice purposes only.<sup>907</sup> Since they were not peace officers, CSIS personnel had no mandate in either area.

When SIRC learned during its 1985-86 review that CSIS still did not have direct access to CPIC, it recommended that the Solicitor General intervene personally.<sup>908</sup> As a result, the Solicitor General wrote to the RCMP Commissioner in August 1986.<sup>909</sup> He directed the RCMP to present and support a request to the CPIC Advisory Committee for CSIS to have access to all CPIC databases for the purposes of counterterrorism investigations, an initiative he described as having been agreed upon between CSIS and the RCMP.<sup>910</sup> As a result of this Solicitor General directive, Jensen was instructed to gain the support of the CPIC Committee, and he ultimately took steps to get involved with the CACP and shepherd through the CSIS request for CPIC access.<sup>911</sup>

Nevertheless, the following year, SIRC was still describing CSIS access to CPIC as “woefully inadequate”, since general access was limited to vehicle registration databanks with only counterterrorism-related access being provided to other databanks.<sup>912</sup> The Review Committee also noted that, as of the end of the 1986-87 review period, the RCMP had only provided four of the long-awaited CPIC terminals<sup>913</sup> to CSIS and had still not made a terminal available at CSIS Headquarters. According to SIRC, there was “no doubt” that the delay reflected a “...continued reluctance to treat CSIS as an equal partner” on the part of the RCMP.<sup>914</sup> Whether accurate or not, the very fact of those allegations is indicative of the difficulties in interagency relations at the time.

### ***Conditions for RCMP Assistance to CSIS***

Due to the lack of resources and the lack of proper advance planning when CSIS was created, the new agency needed access, during its early years, to an array of

---

<sup>906</sup> SIRC implied that the RCMP was responsible for the refusal to provide access to CSIS and was purposefully delaying the installation of computer terminals for CSIS: Exhibit P-144: SIRC 1985-86 Annual Report, pp. 22-23.

<sup>907</sup> Exhibit P-101 CAA0474, pp. 11-12.

<sup>908</sup> Exhibit P-144: SIRC 1985-86 Annual Report, p. 22.

<sup>909</sup> Exhibit P-101 CAC0031. The Solicitor General indicated that the SIRC 1985-86 Annual Report would require a response from him in Parliament.

<sup>910</sup> Exhibit P-101 CAC0031.

<sup>911</sup> Exhibit P-101 CAC0032, p. 2; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5395.

<sup>912</sup> Exhibit P-145: SIRC 1986-87 Annual Report, pp. 14-15.

<sup>913</sup> Exhibit P-144: SIRC 1985-86 Annual Report, p. 22.

<sup>914</sup> Exhibit P-145: SIRC 1986-87 Annual Report, p. 15.

services and facilities available only through the RCMP.<sup>915</sup> These CSIS needs, and the way the RCMP sometimes responded to them, became an additional source of tension between the agencies.

Before CSIS was granted direct access to CPIC, the RCMP provided indirect access, as well as access to criminal records information from its operational files.<sup>916</sup> Pursuant to an agreement between the agencies, the RCMP would provide CSIS with CPIC and RCMP records information upon request.<sup>917</sup> Initially, neither CPIC printouts nor copies of criminal records, including the photographs they contained, were to be provided.<sup>918</sup> This decision was modified within a short time, with the RCMP concluding, on further review, that copies could be provided.<sup>919</sup>

As a condition for providing access to the CPIC and RCMP records information, the RCMP sometimes imposed reporting and record-keeping requirements that were too onerous under the circumstances. The Force asked that its members verify the purpose of the CSIS requests. The information was to be provided only "...for investigation purposes consistent with that Service's mandated responsibilities pursuant to the *CSIS Act*".<sup>920</sup> Access was to be granted only to CPIC information "...that [CSIS] legitimately required to perform their [*sic*] responsibilities".<sup>921</sup> Access was to be determined on a case-by-case and "need-to-know" basis.<sup>922</sup> RCMP detachments were instructed to provide CPIC assistance to CSIS "...when they were satisfied it was a legitimate request". Because of this requirement, CSIS was asked to provide information showing that its requests were made for "business purposes" and were "within their mandate".<sup>923</sup> The RCMP then kept central records of the assistance provided to CSIS and logs of the CSIS CPIC requests.<sup>924</sup> Initially, CSIS was asked to provide an indication of the purpose of its CPIC requests,<sup>925</sup> but this requirement was soon abandoned.<sup>926</sup> Instead, it was decided that the RCMP would log each CSIS request, noting the name of the CSIS member making the request, the CSIS file number, if available,

<sup>915</sup> See Section 3.3.1 (Pre-bombing), *The Infancy of CSIS*.

<sup>916</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1648; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5381-5382. See also Exhibit P-143: SIRC 1984-85 Annual Report, p. 13; Exhibit P-144: SIRC 1985-86 Annual Report, p. 22; Exhibit P-145: SIRC 1986-87 Annual Report, p. 15.

<sup>917</sup> Exhibit P-101 CAA0039(i), p. 26, CAC0018, p. 1; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5382. The interagency agreement did not involve the CPIC Advisory Committee: Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5383.

<sup>918</sup> Exhibit P-101 CAC0018, pp. 1-2; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5383-5384. Criminal records were not contained on CPIC per se, but a reference to their existence and nature was included and other avenues then had to be pursued to obtain the actual records.

<sup>919</sup> Exhibit P-101 CAC0022, CAC0026(i), p. 1. According to Jensen, this review resulted from the RCMP's attempt to be helpful to CSIS and to find a justification to make the access possible, following consultation with legal services: Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5384-5387.

<sup>920</sup> Exhibit P-101 CAA0039(i), pp. 24-25.

<sup>921</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1648.

<sup>922</sup> Exhibit P-101 CAA0039(i), p. 26, CAC0018, p. 1.

<sup>923</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5382.

<sup>924</sup> Exhibit P-101 CAA0039(i), pp. 24, 28.

<sup>925</sup> Exhibit P-101 CAC0027.

<sup>926</sup> CSIS regions stopped including this information as of October 1984, though some RCMP members objected: Exhibit P-101 CAC0027. The requirement was not included in the CSIS telex detailing the procedure to follow for CPIC requests: Exhibit P-101 CAC0026(i), p. 1.

and whether the result of the query was negative or positive.<sup>927</sup> The log was then provided to the CSIS regional director on a monthly basis for him to audit the requests in order to ensure that they were made for legitimate CSIS responsibilities.<sup>928</sup> The RCMP retained copies of the forms it had CSIS fill out to request CPIC and RCMP criminal records information as well as a record of the information it released to CSIS.<sup>929</sup>

These RCMP requirements were problematic for CSIS in light of the highly classified nature of its operations.<sup>930</sup> The RCMP D Division Commanding Officer expressed doubt that “CSIS will be particularly willing to give us much information to identify their case files” and noted that, in any event, he was “... not sure how we will know when the requested information relates to their mandated responsibilities.”<sup>931</sup> CSIS directed its employees, early on, to refrain from including any operational file numbers on the RCMP request forms, since the forms would be retained by the Force.<sup>932</sup> According to Jensen, recording information about the CSIS queries was necessary for audit purposes, to ensure that the integrity of the CPIC system was protected and that no *Privacy Act* violations were committed.<sup>933</sup> The RCMP policed the requests of its own members through a tracking system that could identify requestors, who could then be held accountable if subsequent audit revealed that improper queries were made.<sup>934</sup> Requesting the information from CSIS was to serve the same purpose.<sup>935</sup>

SIRC weighed in on this issue as well. Its 1986-87 Report states that the RCMP system for providing indirect CPIC access to CSIS fostered “...an unwarranted notion that CSIS is a junior partner to the RCMP,” and that it created unnecessary delay for CSIS to obtain the information.<sup>936</sup> As Turner testified, the requirement to fill out a form and wait for the RCMP to provide CPIC information prevented CSIS from “...seiz[ing] the opportunity” to approach individuals of interest immediately, as the Service had to wait to obtain a response to its queries.<sup>937</sup>

In subsequent years, CSIS learned that the RCMP had used its records of CSIS requests for access to CPIC for purposes other than auditing. Turner, who learned about this when he was given access to a Crown database during the preparation for the trial of Malik and Bagri,<sup>938</sup> explained in testimony:

---

927 Exhibit P-101 CAA0039(i), pp. 28-29, CAC0018, p. 1.

928 Exhibit P-101 CAA0039(i), pp. 28-29, CAC0018, p. 1.

929 Exhibit P-101 CAA0039(i), p. 27, CAC0026(i), p. 2.

930 Exhibit P-101 CAC0018, p. 1.

931 Exhibit P-101 CAC0016, p. 1.

932 Exhibit P-101 CAC0026(i), p. 2.

933 Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5383, 5470.

934 Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5382-5383, 5470.

935 Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5470.

936 Exhibit P-145: SIRC 1986-87 Annual Report, p. 15. Jensen also recognized that the system probably required more time for CSIS to complete its work: Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5387.

937 Testimony of Bill Turner, vol. 66, October 25, 2007, pp. 8280-8281.

938 Testimony of Bill Turner, vol. 66, October 25, 2007, pp. 8282-8283.

...we found out later they had an operation called Operation Backtrack, I think it was called.

...

Well, what it entailed is, they would take our CPIC checks and go out and use them as investigative leads. And in the 1980s there was a number of incidents which were somewhat suspicious in that, we would be doing surveillance on a vehicle and then decide to go and approach that person and find out the RCMP had been there a day or two before us.<sup>939</sup>

In connection with its Air India investigation, the RCMP used the records of CSIS CPIC requests to conduct a search of the CSIS queries from early 1985. The names of the individuals queried were then carded by the RCMP, although no further action appears to have been taken.<sup>940</sup> The very possibility that the RCMP could use its records to obtain information about CSIS operations would understandably have given CSIS pause before it requested the CPIC information it needed from the RCMP. As Turner explained, it "...created an atmosphere of suspicion."<sup>941</sup> Former CSIS investigator Laurie testified that he often refrained from including the names of potential sources on the lists sent to the RCMP for CPIC and operational records checks, since he had in the past encountered circumstances where the RCMP used the information on the CSIS lists to approach potential CSIS sources, and this then made the CSIS approach more difficult.<sup>942</sup>

The RCMP also requested and recorded information about CSIS warrants for the interception of private communications (section 21 warrants) in order for the Force to provide operational assistance in executing the warrants. The RCMP had agreed to provide operational assistance when CSIS was created, but on the condition that RCMP members would be able to view the CSIS warrant in advance and maintain a record of all cases where assistance was rendered.<sup>943</sup> This record contained information about the CSIS warrant, the CSIS operative involved, the type of assistance rendered and even the type of investigation being conducted by CSIS in connection with the warrant.<sup>944</sup> The information was used to enable the RCMP to understand the degree and level of support provided to CSIS and to evaluate the need for resources accordingly.<sup>945</sup>

---

939 Testimony of Bill Turner, vol. 66, October 25, 2007, p. 8281.

940 Exhibit P-101 CAF0343(i), p. 79.

941 Testimony of Bill Turner, vol. 66, October 25, 2007, pp. 8281-8282.

942 Testimony of William Laurie, vol. 61, October 15, 2007, pp. 7400-7402. Laurie explained that in cases where the RCMP approached a potential source before CSIS, the source might be more reluctant to speak with CSIS if the source was afraid of police. In cases where the RCMP approached a potential source shortly after CSIS, the source might cease to cooperate out of fear that CSIS might provide information about the source to the police.

943 Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5374-5376; Exhibit P-192, paras. 1-3.

944 Exhibit P-192, paras. 3-4.

945 Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5376-5377.

Jensen explained that it was necessary for the RCMP to view the CSIS warrant, prior to providing assistance, to ensure that RCMP members operated legally and could be held accountable. He did, however, add that recording information about CSIS investigations was also seen by the RCMP as a means to gain a better understanding of CSIS operations and to avoid conflicts if possible.<sup>946</sup> However laudable the motive, requiring the new agency to provide sensitive information in exchange for needed assistance would almost certainly create an atmosphere of suspicion and hostility – one hardly conducive to efficient cooperation.

### **Conclusion**

Interagency tensions affected the free flow of information between CSIS and the RCMP during the pre-bombing period. Some of the formal information-sharing mechanisms put in place only created more debate because of their rigidity and their intrusiveness into CSIS investigations. The system put in place by government, overly focused on the separation of mandates, was less than ideal to encourage close cooperation between the agencies. At times, rather than make the best out of a bad situation, the agencies appear to have made the situation even worse by adhering to inflexible positions in increasingly frequent debates and conflicts.

### **3.5.2 CSIS Failures in Sharing with RCMP**

#### **Introduction**

While CSIS often passed information to the RCMP, particularly in the threat assessments it provided the Protective Policing Directorate (P Directorate), not all information was shared. At times, CSIS limited information-sharing for reasons of secrecy and to avoid “redundancy” in its TA product. In other cases, CSIS failed to include in its TAs background information it had in its possession that would have better allowed the RCMP to interpret the information being provided. In the month preceding the Air India bombing, CSIS failed to include crucial information in the threat assessments it provided to the RCMP.

#### ***Vague, Secretive or Incomplete Assessments***

CSIS TAs tended to be concise and general. They would directly address the particular threat that triggered the TA request, but often failed to include background information that could assist in “connecting the dots”. The conclusions CSIS reached about the level of the threat were not expressed in terms that were meaningful to recipient agencies. Advice that the threat level was high, medium or low provided little assistance to the RCMP in tailoring an appropriate response to the threat.<sup>947</sup>

At times, information about the potential target of the threat (for example Air India or an Indian mission, as opposed to “Indian interests in Canada”), its

<sup>946</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5377-5378, 5380.

<sup>947</sup> See Section 3.3.6 (Pre-bombing), Lack of Meaningful Threat Assessments.

potential nature (for example hijacking or bombing) or its potential authors (for example the names of Sikh extremists under investigation such as Parmar) was simply missing from CSIS threat assessments.<sup>948</sup> At other times, information was deliberately omitted because of secrecy or “efficiency” concerns.

Similar to the practice with internal CSIS communications, sensitive information received from foreign sources might not be included in CSIS’s threat assessments. Often, allied agencies placed caveats on the use of their information, requiring consent before CSIS could distribute the information to other agencies. The CSIS threat assessment product was intended for general distribution among partner agencies, and thus CSIS would not include this sensitive information. From CSIS’s perspective, omitting the information was certainly less cumbersome than attempting to request consent for its distribution. However, from the perspective of the requesting agencies that were deprived of information, this was far from ideal. The RCMP, in particular, was in charge of implementing security measures in response to potential threats, and therefore needed as much precise and detailed information as possible.<sup>949</sup>

Further, in disseminating its threat assessments, CSIS did not necessarily include the information received from the requesting agency. John Henry, Head of the CSIS Threat Assessment Unit (TAU), who was responsible for the transmission of threat assessments between the RCMP and CSIS, explained that it would be redundant or lead to circular reporting to repeat the underlying information in the assessment.<sup>950</sup> That being said, the fact remains that the source of the underlying information could have been identified to avoid circular reporting. Instead, the practice adopted resulted in assessments that provided only a partial picture of the threat situation, and assumed that the TA consumer would be aware from other sources of the underlying information which had been omitted.

### ***Crucial Information Missing in CSIS Threat Assessments***

During the critical month of June 1985, CSIS issued more comprehensive TAs on the Sikh extremist threat in Canada. However, even these TAs failed to include mention of critical information that was in CSIS’s possession.

The Duncan Blast surveillance information, which indicated that Parmar and Reyat were conducting suspicious experiments in the woods (at the time mistakenly believed to involve the firing of a weapon), while provided to the RCMP at the local level, was never included in a CSIS threat assessment.<sup>951</sup> As a result, RCMP Protective Policing was deprived of the benefit of CSIS’s analysis of the reliability of this information and of its impact on the overall threat level. Because the RCMP also failed to report the information internally, P Directorate was, in fact, not even advised of its existence.

---

<sup>948</sup> See Section 3.3.6 (Pre-bombing), Lack of Meaningful Threat Assessments.

<sup>949</sup> See Section 3.3.6 (Pre-bombing), Lack of Meaningful Threat Assessments.

<sup>950</sup> Testimony of John Henry, vol. 25, May 8, 2007, p. 2522.

<sup>951</sup> See Section 1.4 (Pre-bombing), Duncan Blast.



Information about a highly dangerous Sikh extremist possibly conducting experiments with weapons, shortly before the Golden Temple attack anniversary and the Gandhi visit to the US, undoubtedly would have been relevant to the assessment of the security measures necessary to protect Indian diplomats. RCMP P Directorate was entitled to expect that the CSIS TAU would provide this type of highly relevant information, along with its assessment of the threat, at the earliest opportunity. Whether CSIS's failure to do so resulted from an exaggerated focus on protecting the secrecy of its physical surveillance operations,<sup>952</sup> or whether it was the result of an analytical failure to recognize the relevance of the information to the threat assessment process, it was a clear failure on the Service's part in its duty to keep the RCMP and other agencies advised of important threat information.

Another failure occurred shortly before the bombing. On June 13, 1985, CSIS received information from the Vancouver Police Department about the comment made by Pushpinder Singh during the Khurana meeting, in response to complaints about the lack of killings of Indian diplomats, that "...something would be done in weeks."<sup>953</sup> CSIS waited four days before including this information in a general threat assessment sent to the RCMP on June 18<sup>th</sup>. At that time, CSIS reported the comment, but provided no information about the identity of the Sikh extremist who authored it, nor about his leadership role in the ISYF, a dangerous Sikh extremist organization, nor about his connections with Parmar and the BK.<sup>954</sup> CSIS also did not advise the RCMP of the date of the Khurana meeting (June 12<sup>th</sup>), simply stating that it occurred "early in June."<sup>955</sup> This lack of detail made it impossible for the RCMP to determine the precise time frame when this threat needed to be addressed, or to understand the seriousness of the threat. The fact that the RCMP had access to the Khurana information through other means cannot excuse CSIS's failure to provide Protective Policing with the information necessary to implement security measures in response to this threat.

## Conclusion

CSIS missed the opportunity to produce threat assessments that provided a comprehensive description of the threat situation. In the interests of secrecy and efficiency, CSIS failed to fulfill its role as a repository of threat information, gathered across the government, on the basis of which one could draw critical connections and conclusions.

### 3.5.3 RCMP Failures in Sharing with CSIS

#### Introduction

The RCMP often failed to share relevant information in its possession with CSIS. Because of the prevailing tensions, information was sometimes passed

---

<sup>952</sup> See Section 1.4 (Pre-bombing), Duncan Blast.

<sup>953</sup> See Section 1.6 (Pre-bombing), Khurana Information.

<sup>954</sup> See Section 1.6 (Pre-bombing), Khurana Information.

<sup>955</sup> Exhibit P-101 CAB0321, p. 3.



indirectly between the agencies. This complicated internal dissemination and analysis of the information received, and rendered the information exchanges more inconsistent. RCMP sharing with the new intelligence agency was made more difficult because the Force was unable to establish a workable liaison process or to ensure that its members used the formal sharing mechanism it attempted to implement.

The exchange of information with CSIS was often informal or ad hoc, and a great deal of relevant information was never passed on because the RCMP was unable to report it internally, or because its members were unable to understand the importance of transmitting it to CSIS. As a result, the intelligence agency was not provided with important threat information about Sikh extremism and, specifically, about the threat of attacks against Air India.

### ***Liaison Program and Informal Exchanges***

After the creation of CSIS, the RCMP established a formal liaison program. The newly-created divisional National Security Enforcement (NSE) units and HQ NSE Section were designated to act as the points of contact with CSIS.<sup>956</sup> The NSE units were established for the purpose of collecting, coordinating and disseminating national security criminal intelligence between the RCMP and CSIS.<sup>957</sup> They were to act as the conduit between CSIS and the RCMP to ensure that the transfer of information, whether criminal or biographical data, flowed smoothly between the two agencies. The NSE units also kept records of the information shared and were thus the official channel for the transfer of information.<sup>958</sup>

It was expected that RCMP members would report security-related information to NSE units for inclusion in the RCMP threat assessment process and for communication to CSIS.<sup>959</sup> However, the members received little guidance about what information was to be shared with CSIS. They were instructed to report any “security intelligence information” they came across to NSE for eventual communication to CSIS,<sup>960</sup> but were never told what was meant by the term. The closest explanation of the CSIS mandate may have been in a draft guideline which stated that the information sought by CSIS normally related to a list of foreign countries,<sup>961</sup> and that this type of information would most likely be acquired by RCMP members having contact with or “knowledge of” persons from the listed countries.<sup>962</sup> The guideline stated that such contact could occur through membership in an organization, or attendance at social functions or academic classes by a national of a listed country, or by residing in close proximity to such a national.<sup>963</sup>

<sup>956</sup> Exhibit P-101 CAA0039(i), pp. 14, 50, CAC0286, pp. 2-3, CAF0824, p. 6.

<sup>957</sup> Exhibit P-101 CAA0335, p. 7, CAC0286, pp. 2-3.

<sup>958</sup> Testimony of Michael Roth, vol. 46, September 17, 2007, p. 5600.

<sup>959</sup> See, generally, Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

<sup>960</sup> Exhibit P-101 CAA0039(i), pp. 31-32.

<sup>961</sup> Exhibit P-101 CAA0039(i), pp. 30-31.

<sup>962</sup> Exhibit P-101 CAA0039(i), pp. 30-31.

<sup>963</sup> Exhibit P-101 CAA0039(i), pp. 30-31.

Further, despite the establishment of the official liaison program, significant information continued to be shared through informal channels, without flowing through the NSE units. Sgt. Mike Roth, who was the head of the NSE Unit in E Division, testified that this was a “sore point” for him. He explained that while he was “...tasked to head up a liaison unit and to keep track of the information that would go back and forth,” this system did not work in practice.<sup>964</sup> Although E Division NCIS member Sgt. Wayne Douglas felt that informal contacts and the free flow of information were cut back because requests for information had to be made through the CSIS liaison,<sup>965</sup> individuals within CSIS and the RCMP continued to rely on their informal contacts, and information continued to be transferred without being routed through the liaison unit.<sup>966</sup> The Duncan Blast surveillance information was never provided by CSIS directly to the divisional NSE member.<sup>967</sup> Instead, it was transmitted to the Duncan Detachment<sup>968</sup> and to the VPD members of the VIU.<sup>969</sup>

The limited success of the NSE Unit at E Division as a conduit for sharing information between the two agencies was not unique. During an August 1985 Canada-wide special CSIS operational meeting, the participants found that there were “...varying degrees of cooperation depending upon the region and the RCMP section involved”, but unanimously agreed “...that the NSE liaison group created by the RCMP to deal with CSIS was not a viable or effective means of channelling intelligence/information to either the RCMP or CSIS.”<sup>970</sup>

Roth testified that he did not attempt to force CSIS or RCMP members to use his unit as the route to exchange information, because he was “...more interested in ensuring that the information would flow freely throughout the province, between the RCMP and CSIS.”<sup>971</sup> Having said that, Roth did recognize that a particular piece of information could be valuable to the operations of multiple RCMP units, and for that reason a central unit receiving and disseminating the information was necessary.<sup>972</sup> When the information was not transferred through the formal liaison process, there was no mechanism to ensure that all those who needed it received it.

When information was shared informally, the creation of written records and the reporting of the information became entirely dependent on the individual officer receiving the information. Information exchanged through informal channels was often passed verbally with no records being prepared, with the result that the information was often useful only to the individual member receiving it. This had a negative impact on the RCMP’s ability to analyze its information

<sup>964</sup> Testimony of Michael Roth, vol. 46, September 17, 2007, p. 5604.

<sup>965</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4036-4037.

<sup>966</sup> Testimony of Michael Roth, vol. 46, September 17, 2007, p. 5604.

<sup>967</sup> Testimony of Michael Roth, vol. 46, September 17, 2007, pp. 5605-5606.

<sup>968</sup> Exhibit P-101 CAA0193.

<sup>969</sup> Exhibit P-101 CAA0196. See, generally, Section 1.4 (Pre-bombing), Duncan Blast.

<sup>970</sup> Exhibit P-101 CAB0495.

<sup>971</sup> Testimony of Michael Roth, vol. 46, September 17, 2007, p. 5604.

<sup>972</sup> Testimony of Michael Roth, vol. 46, September 17, 2007, p. 5641.

centrally, and it prevented the Force from taking advantage of information provided by CSIS to enrich its global knowledge base. In the context of the Air India investigation, the RCMP undertook regular file reviews to assess prior information in light of new developments and to find new leads. The absence of records about the information that had been passed informally meant that, later, analysts did not have access to a significant volume of potentially important information. Further, because informal exchanges depend on personal working relationships, the flow of information could vary when the individuals involved changed.<sup>973</sup>

### ***Failures to Share Information Relevant to the Threat of Sikh Extremism***

Because of gaps in training about the threat assessment process, about the role of CSIS and about the nature of the “security intelligence information” members were expected to report,<sup>974</sup> the RCMP was unable to provide CSIS with all the information it needed, even when it was in RCMP possession. Having created its own parallel threat assessment process, the RCMP considered its TA requests to CSIS as requests for the Service’s information about a situation, to add to the RCMP base of knowledge but not for the purpose of allowing CSIS to perform the central analysis of all information. The RCMP (rather than CSIS) took it upon itself to combine the information received from CSIS with the RCMP information for a final threat assessment.<sup>975</sup>

Further, much of the information relevant to the threat of Sikh extremism was never reported and never centrally processed at the RCMP.<sup>976</sup> As a result, it could not be provided to the liaison units and was not shared with CSIS. As an example, the information received from Person 1 in September 1984 about the November Plot to bomb an Air India aircraft was not reported to the NSE unit and, hence, was not shared with CSIS.<sup>977</sup>

The RCMP had access to a great deal of information about threats to Air India and received numerous threat warnings against the airline, in some cases specifically referring to the threat of bombing.<sup>978</sup> Often, this information was not shared with CSIS. The information about threats to Air India received by the

<sup>973</sup> VPD Detective McLean, for example, explained that he observed a decrease in VPD information sharing with CSIS and the RCMP when the individuals involved in the investigation of Sikh extremism at CSIS and VIIU during the pre-bombing period changed: Testimony of Don McLean, vol. 21, May 1, 2007, pp. 2029-2031.

<sup>974</sup> Exhibit P-101 CAA0039(i), pp. 31-32; Testimony of Warren Sweeney, vol. 26, May 9, 2007, pp. 2724-2725. About the lack of general training respecting the role of CSIS and the threat assessment process, see Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

<sup>975</sup> See, generally, Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

<sup>976</sup> See Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

<sup>977</sup> Information about the November Plot was first learned by E Division in September 1984: Exhibit P-120 (c), p. 1 (entry for Sept. 20, 1984: doc 526-3, p. 26), but was only reported to NCIB NSE on October 26<sup>th</sup>, when it was received by the VPD from another source: Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 239-3). See Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2595.

<sup>978</sup> See, for example, Exhibit P-101 CAC0517, p. 2, indicating that threat warnings were received prior to each flight, and Exhibit P-101 CAA0185: the June 1<sup>st</sup> Telex.

RCMP Protective Policing Directorate (P Directorate), which was responsible for VIP Security and Airport Policing,<sup>979</sup> was often not transmitted to NSE and hence could not be shared through the formal liaison process.<sup>980</sup>

P Directorate did have its own, direct liaison with the CSIS Threat Assessment Unit. However, the Protective Policing officers did not consistently share the threat information they received with CSIS, even if they were the very individuals who relied on CSIS threat assessments to carry out their own functions. The Acting Officer in Charge at HQ Airport Policing indicated that he would generally pass some threat information on to CSIS,<sup>981</sup> but would not transmit other information,<sup>982</sup> either because he believed that CSIS already had the information or because he otherwise saw “no need” to share it.<sup>983</sup> In addition, any information about threats to Air India received by RCMP Airport detachments, but not reported to P Directorate at HQ, would obviously be unavailable to be shared with CSIS.

In May 1985, RCMP Airport Policing, at least at the detachment level, received an Air India telex warning about plans for violent activities by terrorists during the first week of June 1985 and about the possibility that civil aviation “...in Punjab and elsewhere” could be a target. It recommended particular vigilance with respect to registered baggage and items such as transistors and cameras. This extremely important telex does not appear to have been shared with CSIS.<sup>984</sup> Information received in July 1984 that an individual had “...volunteered to carry a bomb in his accompanied baggage with a view to blowing up an Air India plane in order to draw attention to the demands of the Sikhs” was apparently never reported to the HQ P Directorate, and hence was not shared with CSIS.<sup>985</sup> October 1984 information that a statement was made during an All India Sikh

---

<sup>979</sup> Air India generally liaised with RCMP Airport Policing officials at the airport level. Air India threats were sometimes sent by local officials to the Airport Policing Branch at Headquarters, which would seek a threat assessment from CSIS in response to this information. Information from the Department of External Affairs was often shared at the Headquarters level, being passed by DEA's Office of Protocol to P Directorate personnel: See Section 4.4 (Pre-bombing), Failures in Sharing of Information.

<sup>980</sup> See the following documents, for which there is no record that the information was transmitted to NSE: Exhibit P-101 CAA0185, CAC0293; Exhibit P-129; Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2732, explaining that NCIB did not receive the June 1<sup>st</sup> Telex. See, generally, Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

<sup>981</sup> See, for example, the information in Exhibit P-101 CAA0084, CAC0129.

<sup>982</sup> See, for example, the information in Exhibit P-101 CAA0045.

<sup>983</sup> See Testimony of J.B. MacDonald, vol. 27, May 14, 2007, pp. 2831-2832, explaining that some information was shared and some was not, and p. 2865, explaining that he saw no need to share the June 1<sup>st</sup> Telex. He also testified, however, that if he had received all the Air India threats that were “...coming in at fast numbers and after about the third or fourth, I might be – ‘Well, let’s make sure that they are getting it, and I would write them’”: Testimony of J.B. MacDonald, vol. 27, May 14, 2007, p. 2839. He did not recall this ever having occurred: Testimony of J.B. MacDonald, vol. 27, May 14, 2007, pp. 2839-2840.

<sup>984</sup> Exhibit P-101 CAA0161, CAA0164. A handwritten note on the cover letter to the telex, which was sent from Air India to the OIC at Toronto's Pearson Detachment, instructs the recipient to share the telex with RCMP's P Directorate, Airport Policing Branch, though there is no other record that it was, in fact, sent or received by Headquarters. There is no indication that the information was provided to CSIS.

<sup>985</sup> Exhibit P-101 CAA0083, CAA0084.

Student Federation meeting that there would be "...one hijacking of an Indian aircraft every month," and that a committee involving Ajaib Singh Bagri had been constituted to plan the hijackings, was also not reported.<sup>986</sup> Fortunately, CSIS was able to obtain this information from other sources,<sup>987</sup> but this was in spite of the system.

The most important failure to transmit threat information was the June 1<sup>st</sup> Telex received by the RCMP from Air India. It will be recalled that this telex warned of "...the likelihood of sabotage attempts being undertaken by Sikh extremists by placing time/delay devised [*sic*] etc in the aircraft of registered baggage," and also mentioned plans to set up "...suicide squads who may attempt to blow up an aircraft."<sup>988</sup> This information was received by the HQ Airport Policing Branch on June 5<sup>th</sup>,<sup>989</sup> but it was not shared with NSE and hence could not be passed to CSIS through this channel.<sup>990</sup> As a result of the information in the June 1<sup>st</sup> Telex, Airport Policing did seek a threat assessment from CSIS,<sup>991</sup> but saw "no need" to provide the telex, or the threat information it contained, to CSIS along with that request.<sup>992</sup> In its responding threat assessment, CSIS could only state that, while the threat against all Indian interests was generally high, it was not aware of any specific threat to Air India.<sup>993</sup>

The June 1<sup>st</sup> Telex was described by the former CSIS employees who testified at this Inquiry as information that would have been important in their threat assessment process.<sup>994</sup> Like most retrospective analysis, threat assessments are largely speculative, and the true impact of CSIS's not having been informed of the June 1<sup>st</sup> Telex and of other threat information can never be known.<sup>995</sup> What is clear, however, is that the failure of the RCMP to transmit such seemingly crucial information to CSIS illustrates the gaps in the RCMP understanding of the nature and value of the CSIS threat assessment process, and demonstrates the depth of the RCMP failure to share information with CSIS.

## Conclusion

The RCMP's information sharing with CSIS during the pre-bombing period, especially in connection with the threat assessment process, was not optimal. Internal weaknesses in the RCMP's ability to identify, report and disseminate information, coupled with gaps in training about the threat assessment process and about CSIS's role, severely hampered the Force's ability to share relevant threat information, including important information about threats to Air India, with CSIS.

---

986 Exhibit P-101 CAA0096, CAA0097.

987 Exhibit P-101 CAA0110, p. 3.

988 Exhibit P-101 CAA0185.

989 Exhibit P-101 CAA0208.

990 Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2732.

991 Exhibit P-101 CAA0198.

992 Testimony of J.B. MacDonald, vol. 27, May 14, 2007, pp. 2813, 2865.

993 Exhibit P-101 CAA0199.

994 See Section 1.2 (Pre-bombing), June 1<sup>st</sup> Telex.

995 Final Submissions of the Attorney General of Canada, Vol. II, para. 191.

Despite the formalized liaison process for information sharing with CSIS, inconsistencies remained in the amount of information shared, the timing of the exchanges, and the reporting of the information received. Informal channels which could circumvent the inefficient liaison process carried with them the price of information remaining inaccessible to the system as a whole.

### **3.5.4 RCMP Failures in Sharing with Local Forces**

#### ***The Importance of Local Police Forces to the Threat Assessment Process***

Police officers working with provincial or municipal police forces had the capacity to contribute significantly to the RCMP's pre-bombing assessment and investigation of the threat of Sikh extremism. As readily acknowledged by RCMP Deputy Commissioner Henry Jensen, the officers "closest to the ground" were likely to have the most access to relevant information, and their notebooks would generally contain "a wealth of intelligence."<sup>996</sup> As such, local police forces were "very crucial elements" for the overall effectiveness of the new RCMP threat assessment process as "...important sources of threat assessment related information."<sup>997</sup> This was particularly true about Sikh extremism in Vancouver, where local police had successfully used a community policing approach to gain access to numerous sources in the Sikh community, from whom they had been able to obtain a wealth of intelligence about Sikh extremist organizations and individuals – information that was not accessible to the RCMP.

Unfortunately, the RCMP was unable to achieve sufficient integration with local forces and to share information efficiently with them. As a result, the RCMP was deprived of their valuable intelligence, especially in connection with Sikh extremism. Acrimonious jurisdictional debates with local forces across the country about the nature and extent of the new RCMP security offences mandate, and the manner in which security intelligence could be shared, caused tensions in the relationships that were likely to affect information flow. In Vancouver, where relations were less strained, the RCMP was nevertheless unable to take full advantage of the extensive knowledge of the Vancouver Police Department (VPD), in spite of an attempt to create integrated structures to facilitate sharing.

RCMP members often failed to appreciate the importance of keeping members of local forces sufficiently informed and, at times, applied an overly rigid approach to the handling of classified information. Provincial and municipal police officers were not kept informed on a routine basis of the overall threat information in the possession of the RCMP, even when that information was directly relevant to the specific areas these forces were investigating. The result was that their ability to recognize the significance of the information to which they had access was impaired, as was their capacity to gather the intelligence, and some information that could have been made readily available by local forces was lost to the threat assessment process.

---

<sup>996</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5422.

<sup>997</sup> Exhibit P-101 CAC0495, p. 3.



### ***RCMP Security Offences Mandate and Relations with Local Forces***

When CSIS was created, the *Security Offences Act*, which gave primacy to the RCMP for criminal offences "...arising out of conduct constituting a threat to the security of Canada" or targeting ... "internationally protected person[s]," was enacted as Part IV of the *CSIS Act*.<sup>998</sup> As a result, the RCMP acquired jurisdiction in an area traditionally reserved to provincial and municipal forces in locations where they were the police of jurisdiction.<sup>999</sup> Local forces had previously expressed their opposition to the proposed expansion of RCMP jurisdiction,<sup>1000</sup> and the *Security Offences Act* was initially not well accepted, creating tensions in the relations between the RCMP and local forces.<sup>1001</sup>

Tensions increased in light of a Cabinet decision designating the RCMP as the primary recipient of CSIS intelligence about security offences and as the intermediary between CSIS and local forces.<sup>1002</sup> The RCMP took the position that this meant CSIS intelligence had to be sent first, and exclusively, to the RCMP. The RCMP would then disseminate the information on an "...as deemed necessary basis,"<sup>1003</sup> and involve other police forces "...to the extent it should."<sup>1004</sup> To CSIS, the RCMP position was akin to a claim of "exclusive" jurisdiction, since the RCMP reserved the sole discretion to decide what CSIS intelligence to pass on to which law enforcement agencies, and when. Not surprisingly, local forces representatives also took issue with the RCMP position, and generally wanted to maintain direct and sustained contact with CSIS.<sup>1005</sup> The local forces were also concerned about the type of matters over which the RCMP intended to exercise its new security offences primary jurisdiction, fearing that the RCMP would attempt to get involved in purely local matters.<sup>1006</sup> Initial meetings about the topic were difficult.<sup>1007</sup> The Ontario police forces favoured use of joint forces operations (JFOs) to resolve issues of jurisdiction.<sup>1008</sup> While the RCMP also generally favoured the JFO approach,<sup>1009</sup> it did have some reservations and concerns about local police taking control of investigations and acting without consulting the RCMP.<sup>1010</sup> Similarly, while not opposed in principle, the RCMP

<sup>998</sup> Exhibit P-107: *Security Offences Act*, ss. 57, 61. See also Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5398.

<sup>999</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5398.

<sup>1000</sup> Exhibit P-101 CAA0162, p. 4.

<sup>1001</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5398, 5401.

<sup>1002</sup> Exhibit P-101 CAA0081, p. 3. See also Exhibit P-101 CAA0162, p. 1, CAA0237, p. 1, CAB0189, CAA0039(i), p. 14; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5400-5401.

<sup>1003</sup> Exhibit P-101 CAA0154(i), p. 3.

<sup>1004</sup> Exhibit P-101 CAB0189, p. 1.

<sup>1005</sup> Exhibit P-101 CAA0162, pp. 2, 4.

<sup>1006</sup> See, for example, Exhibit P-101 CAB0422, p. 3, where a perception among members of the Canadian Association of Chiefs of Police that the RCMP would be investigating threats to provincial legislators or municipal representatives was discussed.

<sup>1007</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5400-5401; Exhibit P-101 CAA0237, p. 1, mentioning ... "interminable discussions leading merely nowhere."

<sup>1008</sup> Exhibit P-101 CAB0422, p. 1.

<sup>1009</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5399, 5402.

<sup>1010</sup> Exhibit P-101 CAA0154(i), p. 2; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5403. The draft RCMP Guideline only provided that the Force would "normally" conduct security investigations in cooperation with local police and that this would be done as part of a formal JFO "under certain circumstances": Exhibit P-101 CAA0039(i), p. 12.



was less enthusiastic than local forces were about direct CSIS participation in JFOs,<sup>1011</sup> sometimes preferring to act as an intermediary between the JFO and CSIS.<sup>1012</sup> In all cases, whether a JFO was formed or not, the RCMP intended to exercise "...its primary responsibility for the investigation" where security offences were involved.<sup>1013</sup>

Relations were particularly tense with the Ontario and Quebec provincial and municipal police forces.<sup>1014</sup> Conflict arose with respect to some of the joint investigations being conducted. The Ottawa City Police (OCP) specifically requested that CSIS intelligence relating to an investigation conducted by a joint RCMP-OCP task force be passed on directly, at the same time as it was transferred to the RCMP.<sup>1015</sup> This proposal was met with strong opposition from the RCMP, who argued that this made it impossible to coordinate the investigation.<sup>1016</sup> The Ontario Provincial Police (OPP) also expressed concerns about joint forces investigations relating to terrorism conducted with the RCMP O Division. According to the OPP, the RCMP had demonstrated an "...unwillingness to share intelligence with other police forces" and an "attitude" of "...taking over areas of investigation," and such issues had ultimately been resolved only through direct contact with CSIS. In general, the OPP was "...unhappy with the RCMP approach" in areas of mutual responsibility like security offences and terrorism.<sup>1017</sup>

RCMP Commissioner Robert Simmonds recognized that local forces would have a "...very important and active role" to play if a terrorist incident occurred in their jurisdiction, and that they would need CSIS information in order to perform their functions.<sup>1018</sup> Yet, the application of the rules surrounding the classification of information, and the adherence to caveats, often prevented local forces from receiving relevant information.<sup>1019</sup> Because provincial and municipal police officers "...for the most part [were] not security-cleared," sometimes the RCMP simply did not pass certain intelligence on to them.<sup>1020</sup> The delays, and refusals to provide that information, which arose as a result of information protection concerns, made relations with provincial and municipal forces more difficult for the RCMP, as they created the impression that the RCMP was purposefully withholding information.<sup>1021</sup> The constant jurisdictional debates as well as

---

1011 Exhibit P-101 CAB0422, p. 3; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5399, 5401-5402.

1012 Exhibit P-101 CAA0162, p. 5.

1013 Exhibit P-101 CAA0039(i), p. 12.

1014 Exhibit P-101 CAA0162, p. 4; Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5405-5406.

1015 Exhibit P-101 CAA0131.

1016 Exhibit P-101 CAB0189; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5403.

1017 Exhibit P-101 CAB0422, pp. 1-3.

1018 Testimony of Robert Simmonds, vol. 74, November 8, 2007, p. 9333.

1019 Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5399.

1020 Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5399. As the security clearance process was lengthy and difficult, local forces constables could not easily be security-cleared to a level sufficient to allow them to receive information relevant to the investigations they could be involved in: See Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5404-5405. Further, when CSIS placed caveats on the information it provided to the RCMP, CSIS consent had to be obtained by the RCMP prior to passing on the information to local forces: Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5399-5400.

1021 Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5400.

the local forces' perception that the RCMP was reluctant to share and prone to take an overly controlling approach, were unlikely to lead to the free flow of information necessary to enable the RCMP to receive, assess and respond to all the relevant threat information collected by local police officers.

### ***Relations with the Vancouver Police Department***

In British Columbia, where the Sikh extremism threat was prominent, RCMP relations with local police were less tense. Since a spirit of cooperation generally prevailed, CSIS information could be passed on to local forces directly without attracting jurisdictional concerns or debates about RCMP primacy.<sup>1022</sup> However, even in Vancouver, the RCMP still had difficulty achieving complete and open sharing of information and inclusive decision-making. While an attempt was made to implement an integrated policing model, the actual sharing of information was often insufficient.

### ***Formal Liaison and Integrated Units***

The RCMP and the Vancouver Police Department (VPD) were both involved in the provincial Coordinated Law Enforcement Unit (CLEU), in charge of setting priorities and coordinating law enforcement activities.<sup>1023</sup> Direct liaison was also maintained between the local force and the RCMP about protective policing operations. The VPD Operational Auxiliary Section (OAS) and the RCMP E Division VIP section were in regular contact to coordinate protective deployment issues.<sup>1024</sup>

In terms of intelligence gathering, the VPD and the RCMP E Division NCIS both participated in the Vancouver Integrated Intelligence Unit (VIU).<sup>1025</sup> In 1984-85, VIU's work was focussed mostly on organized crime and organized criminal groups. A sub-component of VIU, the terrorist/extremist unit, focussed on street disorder and demonstrations and prepared threat assessments for VIP visits in Vancouver.<sup>1026</sup> That unit was also responsible for monitoring groups prone to violence based on political motivations and "...groups or individuals that could pose a threat to the community and to Canada at large." The two members of the Criminal Terrorist/Extremist Group of the RCMP E Division NCIS, who had jurisdiction over the entire province of British Columbia, worked at the VIU terrorist/extremist unit alongside two members of the VPD.<sup>1027</sup>

---

<sup>1022</sup> Exhibit P-101 CAA0162, p. 5.

<sup>1023</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3876-3877. In light of the province-wide mandate of CLEU, the RCMP played a more significant role in operational decisions: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3877. The RCMP is the police of jurisdiction in the province of British Columbia, except in municipalities such as Vancouver which have their own police force.

<sup>1024</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3901-3902.

<sup>1025</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3870, 3871; Testimony of Henry Jensen, vol. 44, June 18, 2007, p. 5423.

<sup>1026</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3870. For this purpose, VPD members of VIU maintained direct contact with the VPD protective unit (OAS): Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3901-3902, 3925-3926.

<sup>1027</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4029, 4034; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3870, 3872.

The terrorist/extremist unit of VIIU was not as integrated as it could have been.<sup>1028</sup> The RCMP and VPD members worked in parallel, with each agency keeping its own separate filing system, reporting through its own separate chain of command, and pursuing its own separate mandate. The RCMP and VPD members did not conduct common operations or work together on integrated files, but rather each organization usually conducted its own independent investigations.<sup>1029</sup> They generally did not share sources, task each other with providing assistance, or coordinate their activities.<sup>1030</sup> This lack of integration resulted in lost opportunities in terms of intelligence gathering for both agencies.<sup>1031</sup> The consequences were particularly serious for the RCMP, in terms of its ability to assess and respond to the threat of Sikh extremism prior to the Air India bombing. The RCMP lost opportunities to benefit from the VPD information and to share its own information to assist the VPD in gathering more information. Since the VPD had developed a more extensive understanding of Sikh extremism in British Columbia, and had access to more sources in the community, the RCMP might have been in a better position to gather sufficient information to prevent the bombing if it had taken advantage of the VPD's potential contribution to the fullest extent possible.

### ***Investigation of Sikh Extremism in Vancouver***

The VPD members of VIIU personally investigated Sikh extremism and also received information gathered by other VPD units. The VPD had a special unit called the Indo-Canadian Liaison Team (ICLT) which assisted the Vancouver Indo-Canadian community with a wide range of issues. The ICLT's functions included: redirecting domestic violence matters to appropriate agencies; providing security for elections at temples; dealing with disputes or issues which arose in ashrams (Hindu temples) or gurdwaras (Sikh temples); and assisting VPD detectives conducting investigations in the Indo-Canadian community. The ICLT was also involved in addressing some of the community issues associated with Sikh extremism, such as threats and intimidation. As a result of its community policing approach, it was able to collect intelligence information about Sikh extremists operating in the Lower Mainland of British Columbia.<sup>1032</sup>

During the period preceding the Air India bombing, ICLT members liaised with temple and business leaders from the community, analyzed local media content and essentially integrated themselves into the community. The ICLT spent a great deal of time in the community, discussing current issues with community members and familiarizing themselves with the language and traditions of

<sup>1028</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3920.

<sup>1029</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3871-3873; Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4030.

<sup>1030</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4033; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3872-3873, 3877-3878. On occasion, the VPD members made specific requests for information about Sikh communities located in areas outside of VPD jurisdiction, such as Surrey, but they eventually established their own relations with the RCMP Detachments involved and communicated with them directly: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3877-3878.

<sup>1031</sup> Axel Hovbrender, who was a VPD member of VIIU between 1982 and 1986, indicated that in light of the limited resources available, "...working together in a cooperative and collaborative way is always a benefit": Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3920.

<sup>1032</sup> Testimony of Don McLean, vol. 21, May 1, 2007, pp. 1988-1989, 2021.

the community. They were able to gain the community's trust and to become accepted. VPD Cst. Don McLean explained in testimony that, eventually, ICLT members could walk into any temple, at any time, in uniform, and speak to anyone present without any problem. As a result of this relationship of trust, the ICLT gained access to sources and informants in the community who provided information about Sikh extremism.<sup>1033</sup>

The ICLT had access to sources among both moderates and extremists. McLean explained that the view supporting the violent overthrow of the Government of India was only held by a few individuals in the community, and that they used threats and force to attempt to gain support for their position.<sup>1034</sup> By investigating numerous cases of threats, intimidation and assaults against moderates in the Sikh community, and even bringing some cases to successful prosecution, the ICLT continued to gain trust and received more information.<sup>1035</sup> ICLT members could even task members of the Vancouver Sikh community with developing sources in other communities in order to receive information about prominent BC extremists when they travelled to other jurisdictions.<sup>1036</sup> In this manner, ICLT member McLean was able to learn on June 27, 1985 that, approximately two weeks before the Air India bombing, members of a Toronto Sikh temple associated with the Babbar Khalsa were told not to fly Air India, as it would be unsafe to do so.<sup>1037</sup>

The ICLT reported all of the intelligence information it received about Sikh extremism to the VPD members of VIU.<sup>1038</sup> As a result of the information they received, VPD members of VIU became interested in the issue as early as 1983.<sup>1039</sup> For the most part, they processed the information gathered by the ICLT, but they also developed a few community sources of their own.<sup>1040</sup> In the aftermath of the Golden Temple attack in June 1984, the VPD was able to accumulate a significant amount of information and to develop an in-depth knowledge of the main Sikh extremist organizations and individuals active in British Columbia. The local force was aware early on of the activities of prominent Sikh extremists who were advocating violence, such as Talwinder Singh Parmar, Ajaib Singh Bagri and Surjan Singh Gill, and of their leadership role in the Babbar Khalsa (BK).<sup>1041</sup> The VPD was also aware of the activities of

<sup>1033</sup> Testimony of Don McLean, vol. 21, May 1, 2007, p. 2023; Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4123-4126, 4149, 4171.

<sup>1034</sup> Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4131, 4137.

<sup>1035</sup> Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4130-4131; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3883-3884.

<sup>1036</sup> Testimony of Don McLean, vol. 35, May 29, 2007, p. 4133; Testimony of Don McLean, vol. 21, May 1, 2007, p. 2016.

<sup>1037</sup> Exhibit P-404, p. 3; Exhibit P-101 CAA0281, p. 1.

<sup>1038</sup> Testimony of Don McLean, vol. 21, May 1, 2007, pp. 1994-1995; Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4126-4127.

<sup>1039</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3871. See also, Testimony of Don McLean, vol. 21, May 1, 2007, pp. 2021-2022.

<sup>1040</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3878, 3895-3896. Hovbrender did indicate, though, that his sources provided mostly information that was generally known in the community and not specific or actionable in a criminal investigation: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3896-3897.

<sup>1041</sup> Testimony of Don McLean, vol. 21, May 1, 2007, pp. 1996-1997; Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4126-4127, 4141-4143. See also, Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3884-3888, 3890, 3898.

the International Sikh Youth Federation (ISYF),<sup>1042</sup> a Sikh extremist organization with a significant membership and heavy involvement in acts of violence and intimidation in the community.<sup>1043</sup> It knew specifically of the leadership role played in that organization by Pushpinder Singh, an extremist recently arrived from India in 1985.<sup>1044</sup> VPD members had information about connections among Sikh extremist individuals and organizations. They were aware of a connection between ISYF spokesperson Manmohan Singh and BK member Surjan Singh Gill,<sup>1045</sup> and also obtained information indicating that Ripudaman Singh Malik was a close associate of Parmar's and was financially supporting him.<sup>1046</sup>

In January 1985, VPD members of VIU and ICLT members prepared a comprehensive analysis of the VPD's information about Sikh extremism, in collaboration with a CLEU analyst.<sup>1047</sup> This intelligence document contained a flow chart of significant events, including demonstrations, threats and violent offences, as well as lists and charts identifying and describing linkages among Sikh extremist individuals and organizations known to the VPD.<sup>1048</sup> The document also included approximately one hundred profile sheets for prominent Sikh extremists and individuals associated with extremist organizations who had "...a high threat potential to use criminal acts and violence as a means of achieving their (potential) goals."<sup>1049</sup>

Meanwhile, the RCMP E Division NCIS, whose Terrorist/Extremist Group was investigating Sikh extremism and working with the VPD at VIU, did not use a community policing approach. Generally, E Division NCIS found the community mistrustful of police and unwilling to cooperate.<sup>1050</sup> In fact, NCIS did not have sources in the Sikh community and was not actively trying to develop such sources. As a result, the RCMP did not have access to the same type of valuable intelligence about Sikh extremism that the ICLT was collecting and often had

<sup>1042</sup> Formerly known as the Sikh Student Federation (SSF): See Exhibit P-101 CAB0360, p. 5.

<sup>1043</sup> Testimony of Don McLean, vol. 35, May 29, 2007, p. 4129; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3887.

<sup>1044</sup> Testimony of Don McLean, vol. 21, May 1, 2007, pp. 1997, 2001; Exhibit P-101 CAB0306, p. 2. McLean described Pushpinder Singh as a "terrorist": Exhibit P-101 CAC0487, p. 5.

<sup>1045</sup> Testimony of Don McLean, vol. 35, May 29, 2007, p. 4143.

<sup>1046</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3886.

<sup>1047</sup> Exhibit P-391, document 124 (Public Production # 3254); Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4132-4133; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3879-3881, 3882-3884: The purpose of the document was to assist VPD, RCMP and CLEU management in operational decisions and future investigations. It was used by the VPD to provide context for analysis of incoming intelligence and to orient ongoing intelligence-gathering activities and criminal investigations relating to threats and intimidation in the community.

<sup>1048</sup> Exhibit P-391, document 124 (Public Production # 3254); Testimony of Don McLean, vol. 35, May 29, 2007, p. 4132; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3881.

<sup>1049</sup> Exhibit P-391, document 124 (Public Production # 3254), p. 5. Ten such profile sheets are included at pp. 89-98 of the document. The others were not produced in the version of the document provided to the Commission.

<sup>1050</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4040, 4109. McLean has testified that no other police force in British Columbia was using the community policing approach at the time, except for one RCMP officer who was working at the Surrey Detachment: Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4149, 4174.

to rely on the ICLT for information.<sup>1051</sup> The RCMP found itself having to resort to the ICLT's assistance outside of the VPD's territorial jurisdiction. In one case, an assault in Duncan, the RCMP had no leads and turned the investigation over to the ICLT, which had previously obtained information about the assault and was able to bring the case to court and obtain a conviction.<sup>1052</sup>

Despite the high level of intimidation in the Vancouver Sikh community, and the generalized fear of reprisals against those who cooperated with police,<sup>1053</sup> the ICLT always continued to receive information.<sup>1054</sup> In general, the VPD members of VIIU, with the support of the ICLT, gathered much more information about Sikh extremism than the RCMP members of VIIU, who were less able to devote priority attention to the issue.<sup>1055</sup>

## **Information Sharing and Cooperation Failures**

### ***Information Exchange and Access to Files***

Information was mostly shared between the VPD and RCMP members of VIIU in an informal manner, in the context of the everyday discussions that took place between the individual members who were working in the same office space. All information received by the VPD members was documented and preserved in the VPD files kept at VIIU. The VPD VIIU files were searchable through a manual index card system and were fully accessible to the RCMP members of VIIU.<sup>1056</sup>

The RCMP, on the other hand, did not provide free and complete access to its VIIU files.<sup>1057</sup> RCMP VIIU member Sgt. Wayne Douglas testified that access to the RCMP files was "readily available," without providing more detail.<sup>1058</sup> However, VPD member of VIIU, Supt. Axel Hovbrender, explained that the RCMP files were kept separately in an office that the VPD members could not access. He added that the separate filing systems were a concern among VPD managers at VIIU, and that the lack of access to RCMP files was viewed by some as a symptom of a more general lack of RCMP sharing with municipal forces.<sup>1059</sup> Douglas did admit that the RCMP kept their filing cabinets locked more than the VPD did "for security reasons."<sup>1060</sup> This is consistent with the general RCMP approach towards

---

<sup>1051</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4040.

<sup>1052</sup> Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4129-4130, 4168-4169.

<sup>1053</sup> Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4131-4132. McLean compared the level of intimidation to that found in communities suffering intimidation from organized criminal groups.

<sup>1054</sup> In general, however, the sources who spoke with the ICLT provided their information confidentially, on the understanding that their identity would remain protected: Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4171-4172.

<sup>1055</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3878. The RCMP NCIS Terrorist/Extremist unit had "...lots of other files to look after," which made it difficult, resource-wise and time-wise, to engage in active source development in the Sikh community: Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4109.

<sup>1056</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3872-3874; Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4030, 4040.

<sup>1057</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3874.

<sup>1058</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4030.

<sup>1059</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3874, 3878-3879, 3923.

<sup>1060</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4030.



caveats and classification,<sup>1061</sup> and, in particular, with the RCMP's concern about the lack of security clearance of municipal officers.<sup>1062</sup> In the case of the VIIU, the impact of the lack of access is evident because much of the relevant information in the possession of the RCMP was not known to the VPD.

### ***RCMP Failures to Share Information with the VPD***

At the operational level, relations were very collegial between the VPD and the RCMP members of the VIIU Terrorist/Extremist unit. As a result of the good working relationship, the VPD members believed that they were receiving all the information they needed from their RCMP colleagues through their regular informal exchanges. Hence, they did not specifically request access to the RCMP files that were kept in a separate area.<sup>1063</sup> Even the RCMP members of VIIU were apparently under the impression that they discussed all of the information they were aware of with their VPD colleagues.<sup>1064</sup> In fact, however, relevant RCMP information was not always shared with the VPD members of VIIU.

VPD members were not advised of the October 1984 information received by the RCMP from External Affairs indicating that the ISYF was planning to hijack an Air India aircraft and that Bagri was nominated on a committee to plan the attack.<sup>1065</sup> Information about the 1984 BK threat to kidnap or kill the Indian Consul General in Vancouver, and about the BK's threatening letters, postmarked in Vancouver and sent to high officials in India, was also not shared with the VPD members of VIIU.<sup>1066</sup> The RCMP members did not advise their VPD colleagues of the arrest of an ISYF member with parts of an Uzi machine gun at Vancouver airport in March 1985, or of the fact that the remaining parts of the weapon were discovered on the suspect's travelling companion in London.<sup>1067</sup> The RCMP also did not advise the VPD members of the April 1985 information indicating that Parmar's group was "...working on a highly secret project,"<sup>1068</sup> or of the information received in late June 1985 about a plot by four Sikhs from Vancouver Island to purchase automatic weapons and hand grenades and to commit criminal acts with possible political overtones.<sup>1069</sup> Similarly, when the RCMP received information in May 1985 about a plot by extremists to bomb the Indian Consulate in Vancouver on June 6, 1985,<sup>1070</sup> it was not provided to VPD members of VIIU or to the ICLT.<sup>1071</sup>

---

<sup>1061</sup> See, generally, Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3916, 3924. See also Volume One, The Inquiry Process, for a discussion of the national security "over-claiming" by Government agencies.

<sup>1062</sup> Testimony of Henry Jensen, vol. 44, June 18, 2007, pp. 5399, 5404-5405.

<sup>1063</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3872, 3874-3875, 3923-3924.

<sup>1064</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4118-4119.

<sup>1065</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3887; Exhibit P-101 CAA0103, CAA0099.

<sup>1066</sup> Exhibit P-101 CAC0317; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3904.

<sup>1067</sup> Exhibit P-101 CAB0207, p. 2, CAC0291; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3890-3892.

<sup>1068</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3902-3903; Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4134-4135; Exhibit P-101 CAC0290, p. 3.

<sup>1069</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3900-3901; Exhibit P-101 CAB0329.

<sup>1070</sup> Exhibit P-101 CAC0364, p. 2.

<sup>1071</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3900; Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4135-4137.



Douglas did not advise his VPD colleagues of the information received by the RCMP from Person 1 in September 1984 about a plot to bomb an Air India aircraft (the November Plot information). The VPD members of VIIU only found out about this plot when the same information was subsequently provided to another VPD unit by Person 2.<sup>1072</sup> Douglas was aware of the Person 2 information,<sup>1073</sup> and would most likely have had discussions about it with his VPD colleagues at VIIU, but nevertheless did not advise them that similar information had been received from a different source in the past.<sup>1074</sup>

VIIU also did not have access to relevant information because of gaps in internal RCMP information sharing. In instances where RCMP members of VIIU were not themselves provided with all relevant information in the RCMP's possession, they could not share it with their VPD colleagues. This was the case for the CSIS threat assessments prior to April 1985, and for threat information received by the RCMP Protective Policing Directorate from DEA or Air India.<sup>1075</sup> As a result, the VPD members of VIIU were not provided with the information contained in the October 1984 CSIS threat assessment which detailed threats made by Parmar to kill Hindus.<sup>1076</sup> This information pointed to threats of a different nature from the threats against the Indian Government and its representatives, which were generally known to the VPD. It would have assisted the VPD in its intelligence-gathering activities.<sup>1077</sup> Further, the November 1984 information about a plot to kidnap the Indian Consul General in Vancouver or Toronto, which was known to E Division VIP security, was not passed to the VPD.<sup>1078</sup> The VIP Security information indicating that the Vancouver ISYF was planning to physically assault the Indian Consul General and other members of the Vancouver Consulate on April 13, 1985, naming ISYF spokesperson Manmohan Singh as one of the individuals "... entrusted with the task," was also never provided to the VPD members of VIIU.<sup>1079</sup> Similarly, the June 1<sup>st</sup> Telex about threats to bomb Air India planes using time-delayed devices, like most of the threat information received from the airline, was not shared with the VPD.<sup>1080</sup>

ICLT member McLean testified that he was, in fact, never provided with any information about threats to Air India.<sup>1081</sup> As a result, he was prevented from exploring all possible avenues of investigation with respect to the Khurana

<sup>1072</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3904-3905; Exhibit P-391, document 124 (Public Production # 3254), p. 64.

<sup>1073</sup> Exhibit P-120(c), p. 1 (entry for Oct., 1984: doc 231-3, pp. 2-4).

<sup>1074</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3905.

<sup>1075</sup> See Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

<sup>1076</sup> Exhibit P-101 CAA0110, pp. 2-3; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3889-3890.

<sup>1077</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3889.

<sup>1078</sup> Exhibit P-101 CAB0169; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3901-3902. The information may have been passed on to the VPD OAS and then not relayed to VIIU: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3902, 3926.

<sup>1079</sup> Exhibit P-101 CAC0293; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3892-3893. Hovbrender indicated that the VPD members of VIIU were never made aware of information this specific with respect to threats against the Consul General on a specific date.

<sup>1080</sup> Exhibit P-101 CAA0185. The telex was not transmitted to NCIB at HQ: Testimony of Warren Sweeney, vol. 26, May 9, 2007, p. 2732, and hence could not be disseminated to the divisional NCIS section.

<sup>1081</sup> Testimony of Don McLean, vol. 21, May 1, 2007, p. 2012. Even the November Plot information from Person 2, which was included in the VPD analytical document (Exhibit P-391, document 124 (Public Production # 3254), p. 64) was not transmitted to McLean by either the RCMP or the VPD.

information about ISYF leader Pushpinder Singh's comment that something would happen in two weeks.<sup>1082</sup> While the VPD members of VIIU or of the ICLT were not responsible for airport policing or for the protection of Indian missions,<sup>1083</sup> the VPD needed access to the RCMP threat information in order to better identify, report, assess and further investigate the information that could come from its sources. As Hovbrender explained, information is the "life-blood of intelligence." Having as much information as possible is essential, from an intelligence perspective, to discern patterns and make the appropriate analysis. The RCMP tended to protect or classify its information more strictly, and did not share it freely. While there could be valid reasons to protect information, the RCMP failure to share more openly with the VPD prevented the ground-level officers, who had the most access to sources of information, from using that access to obtain additional threat information, and from analyzing and understanding relevant threat patterns.<sup>1084</sup>

If the RCMP had sought to act as the exclusive intermediary for the passage of CSIS information about Sikh extremism to local forces, as it was contemplating doing in May 1985,<sup>1085</sup> the situation would have been even more difficult. As it was, the VPD was able to obtain at least some information from CSIS, such as the Duncan Blast surveillance information,<sup>1086</sup> and did maintain its close liaison with the intelligence agency.<sup>1087</sup> Whatever the merits of making the RCMP the primary recipient of CSIS intelligence in cases with a potential national scope,<sup>1088</sup> this approach would only be beneficial if there was a sufficient flow of information to the officers with the most ability to gather additional information, regardless of the police force to which they belonged.

### ***RCMP Failures to Access and Report VPD Information***

The VPD members of VIIU attempted to provide their RCMP colleagues with all the relevant information in their possession during the course of their informal discussions, directing them to relevant VPD files where necessary.<sup>1089</sup> However, the RCMP members of VIIU often did not report to RCMP Headquarters the VPD information which was conveyed to them or available in the VPD files.

The internal procedures in place at the RCMP did not provide for exchanges of reports at the desk level. The RCMP members of VIIU working at the operational level were not expected to take the initiative of researching VPD files to find relevant information.<sup>1090</sup> Instead, the VPD VIIU reports were reviewed at a more senior RCMP level, where the decision was taken about whether to disseminate

<sup>1082</sup> See Section 1.6 (Pre-bombing), Khurana Information.

<sup>1083</sup> Testimony of Don McLean, vol. 35, May 29, 2007, p. 4170.

<sup>1084</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3916.

<sup>1085</sup> See Exhibit P-101 CAA0154(i), p. 3, where the RCMP suggests that the Sikh extremist problem should be recognized as involving its security offences mandate.

<sup>1086</sup> Testimony of Don McLean, vol. 35, May 29, 2007, p. 4139; Exhibit P-403; Exhibit P-101 CAA0196.

<sup>1087</sup> Testimony of Don McLean, vol. 35, May 29, 2007, p. 4128; Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3876. See, for example, Exhibit P-101 CAB0048.

<sup>1088</sup> Testimony of Robert Simmonds, vol. 74, November 8, 2007, p. 9333.

<sup>1089</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3872, 3874.

<sup>1090</sup> See, generally, Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4033-4035.

them to operational personnel as deemed necessary. Because of this structure, the sharing of information was not always timely<sup>1091</sup> and, as observed in the case of information relevant to the threat of Sikh extremism, because the relevance of the information was not always recognized, it was not always disseminated within the RCMP.

It appears that RCMP E Division members only began to recognize the value of VPD information after the Air India bombing, when this information was finally reported in detail and used in the course of the investigation. Shortly after the bombing, the RCMP took copies of all Sikh extremism-related VPD reports found at VIIU and at the ICLT, and asked ICLT member McLean to provide briefings about Sikh militants in the community and Sikh extremists who were most likely involved in the bombing.<sup>1092</sup> At the time, McLean spoke about the Khurana information, which, in light of the Pushpinder Singh comment two weeks before the bombing that something would happen in two weeks, tended to indicate ISYF members could be involved.<sup>1093</sup> Details of the Khurana information were then provided to RCMP HQ by E Division on June 25<sup>th</sup> and RCMP members of VIIU began to investigate local factions of the ISYF.<sup>1094</sup>

The Khurana information had not been reported to HQ before the bombing,<sup>1095</sup> even though it was available to RCMP VIIU members as of June 13<sup>th</sup> in a report sent to the VPD VIIU members, and would most likely have been discussed with the RCMP members as well.<sup>1096</sup> Instead, on June 14<sup>th</sup>, E Division NCIS advised HQ that it had no intelligence indicating violent or criminal acts were planned for the Consulate and was "...unable to determine the potential for violence" against Indian officials in Vancouver.<sup>1097</sup> Similarly, information obtained by Hovbrender, that the leader of the BK International in London had stated in 1984 that anyone who flew Air India would be killed in Britain or in India by the BK, was included in an RCMP affidavit in support of a wiretap application in connection with the Air India investigation in 1996. The information had been available at VIIU since early June 1985.<sup>1098</sup> There is no indication that it was accessed or reported by the RCMP members of VIIU prior to the bombing.

The RCMP members of VIIU also did not access or report the general intelligence gathered by their VPD colleagues which identified the main players in the BC

---

<sup>1091</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4034, 4113.

<sup>1092</sup> Testimony of Don McLean, vol. 21, May 1, 2007, pp. 1986, 2037; Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4143-4144, 4157-4159.

<sup>1093</sup> Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4143-4144. See, generally, Exhibit P-101 CAC0487, CAA0249.

<sup>1094</sup> Exhibit P-101 CAA0249.

<sup>1095</sup> RCMP HQ NCIB member Sgt. Sweeney testified that he only learned about this information on the day of the bombing from VPD Cst. McLean: Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2641; Exhibit P-101 CAF0035, p. 28.

<sup>1096</sup> See report submitted to VIIU on June 13: Exhibit P-101 CAC0487; Testimony of Don McLean, vol. 21, May 1, 2007, pp. 2000-2001. About the likelihood of the information having been discussed, see Testimony of Don McLean, vol. 21, May 1, 2007, p. 2026; Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2641-2642; Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4070.

<sup>1097</sup> Exhibit P-101 CAC0438, p. 2.

<sup>1098</sup> Exhibit P-101 CAD0180, pp. 20-21.

Sikh extremist movement and the possible connections among extremist individuals.<sup>1099</sup> Douglas was unaware of the importance of many of the players in the movement and did not know about many of the threats they issued.<sup>1100</sup> RCMP HQ was not provided with this background intelligence and was not aware, for example, of the identity and role of ISYF leader Pushpinder Singh and ISYF spokesperson Manmohan Singh.<sup>1101</sup> The RCMP members of VIIU also did not report to RCMP HQ the information about possible connections between the ISYF and the BK, two of the most militant and dangerous Sikh extremist organizations. These linkages were suggested by the Khurana meeting, where a connection between Parmar and Pushpinder Singh was identified,<sup>1102</sup> and found in the VIIU report about the Duncan Blast surveillance, where an early June 1985 meeting at the residence of Surjan Singh Gill involving BK and ISYF members was discussed.<sup>1103</sup> Similarly, the October 1984 VPD information indicating that Ripudaman Singh Malik was financially supporting Parmar was not reported to RCMP HQ prior to the bombing.<sup>1104</sup> The RCMP VIIU members had access to the VPD general intelligence and could consult the analytical VPD document containing profile sheets and link charts,<sup>1105</sup> but they apparently did not appreciate the importance of developing their own understanding of the Sikh extremist movement and of reporting this knowledge to RCMP HQ.

Since CSIS sometimes used the VPD members of VIIU as an indirect conduit to pass on information to the RCMP,<sup>1106</sup> the failure of RCMP VIIU members to access VPD information and files might have deprived the RCMP of information which CSIS intended it to have. CSIS provided complete details of its Duncan

---

1099 In fact, members of the NCIS E Division Terrorist/Extremist unit had a very poor understanding of the main Sikh extremist players in the pre-bombing period. For example, Douglas, who was the head of the unit, testified that he "recognized the name" Ajaib Singh Bagri, but was unaware of significant threat information indicating the dangers he posed. Moreover, Douglas was "not too familiar" with Surjan Singh Gill: See Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4048, 4051-4053.

1100 See Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

1101 Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2641. See, generally, Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process (under the heading Failures to Identify and Report Background Intelligence).

1102 Exhibit P-101 CAC0487, p. 4. The report was available in the VPD VIIU files and the information was most likely discussed with the RCMP members: Testimony of Don McLean, vol. 21, May 1, 2007, p. 2026; Testimony of Warren Sweeney, vol. 25, May 8, 2007, pp. 2641-2642; Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4070.

1103 Exhibit P-101 CAA0196, p. 2. The report was available in the VPD VIIU files and the information was most likely discussed with the RCMP members: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3907; Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4033-4034. See also Exhibit P-101 CAA0876, indicating that a briefing was provided to NCIS members about the report.

1104 The information was shared with the RCMP during informal discussions at VIIU: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3886. We find no indication in the record that it was reported and Malik did not become a key suspect in the Air India investigation until many years after the bombing.

1105 Former RCMP member of VIIU Sgt. Douglas could not recall whether he saw the document before or after the Air India bombing: Testimony of Wayne Douglas, vol. 34, May 28, 2007, p. 4035. The document was not only available in the VPD files, but was formally passed on to RCMP E Division NCIS and to CISBC: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3882, 3918. Because CLEU approval was required to prepare the analysis, the RCMP would also have been aware of the existence and purpose of the document: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3880.

1106 See Section 3.5.3 (Pre-bombing), RCMP Failures in Sharing with CSIS.

Blast surveillance information to the VPD.<sup>1107</sup> The information was included in a VIIU report prepared on June 6, 1985, only two days after the Duncan Blast.<sup>1108</sup> This report was fully accessible to the RCMP members of VIIU, the information it contained was most likely discussed informally with them during the following days, and a briefing about the report was provided by the VPD to RCMP members who were to conduct diffusion interviews with Parmar and Gill.<sup>1109</sup> The information was not reported to RCMP HQ, and any benefit of the CSIS information was lost to the RCMP because of the failure of the members of the integrated unit to access, research, recognize and report relevant VPD information.

### ***Deficiencies in Information Exchange Mechanisms***

At VIIU, there was no written policy or formal mechanism for sharing of information. Where information was passed verbally, as was often the case,<sup>1110</sup> written records of the information exchanged were generally not kept. This made it difficult, if not impossible, for officers to later track what information had been passed.<sup>1111</sup> This lack of formalized process impacted on the agencies' ability to report internally the information received for central analysis. The benefit from the VPD information to the RCMP as a whole depended on the individual officer receiving the information deciding to include it in a report or other record. This reliance on individual discretion and ad hoc decisions had a negative impact on the RCMP's overall ability to assess and respond to the threat of Sikh extremism.

As was the case with RCMP/CSIS information sharing, information exchanges depended on personal working relationships. The amount of information shared could vary when the individuals involved changed. McLean explained that he observed a decrease in VPD information sharing with CSIS and the RCMP when the individuals involved in the investigation of Sikh extremism at CSIS and at VIIU during the pre-bombing period changed.<sup>1112</sup> Without a more formalized process, such inconsistencies were inevitable.

### ***Failure to Coordinate Investigations***

Because the VPD and RCMP members of VIIU did not conduct common operations or work together on integrated files,<sup>1113</sup> opportunities were lost to coordinate the investigation of information about the threat of Sikh extremism. No attempt

<sup>1107</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3906. See, generally, Section 1.4 (Pre-bombing), Duncan Blast.

<sup>1108</sup> Exhibit P-101 CAA0196.

<sup>1109</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3907; Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4033-4034; Exhibit P-101 CAA0876. See Section 1.4 (Pre-bombing), Duncan Blast.

<sup>1110</sup> This was the case at VIIU: Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3872. ICLT members also occasionally had informal discussions with RCMP members, though they generally expected their information to be shared with the RCMP through the discussions held at VIIU: Testimony of Don McLean, vol. 21, May 1, 2007, p. 2029; Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4127, 4129, 4167-4168.

<sup>1111</sup> Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4112-4113.

<sup>1112</sup> Testimony of Don McLean, vol. 21, May 1, 2007, pp. 2029-2031.

<sup>1113</sup> Testimony of Axel Hovbrender, vol. 33, May 24, 2007, pp. 3872-3873, 3877-3878.

was made to coordinate the investigation of the Khurana information, as the RCMP expressed no interest in investigating it prior to the bombing and left the VPD to conduct its own inquiries without requesting follow-up reports.<sup>1114</sup> ICLT members were not consulted, in any way, prior to the diffusion interviews of Parmar and Surjan Singh Gill in preparation for the Gandhi visit to the US, and were not even aware of the interviews.<sup>1115</sup> Given their knowledge and their reputation in the community, the participation of ICLT members in these and other RCMP investigative initiatives, at a time when the Air India bombing plot was most likely in the final planning stages, would clearly have been helpful.

### ***Failures to Manage and Access Information from the Criminal Intelligence Service of British Columbia***

During the period preceding the Air India bombing, significant information about the threat of Sikh extremism was shared by members of the VPD with an organization called the Criminal Intelligence Service of British Columbia (CIS BC). A number of important CIS BC documents – including the report by the VPD about its October 1984 interview of Person 2 in connection with the November Plot information<sup>1116</sup> and the VIIU report on the Duncan Blast<sup>1117</sup> – were not accessed by RCMP investigators until significantly after the bombing, if at all. Given the nature and status of the CIS BC organization in 1985, the information should have been obtained by the RCMP.

In 1985, CIS BC operated under the umbrella of the Criminal Intelligence Service of Canada.<sup>1118</sup> The Criminal Intelligence Service of Canada was a program that "...encompassed all the criminal intelligence units of the various provincial and municipal forces in Canada, devoted to organized crime."<sup>1119</sup> Each province had a provincial CIS bureau, which collected information and reports provided to it by feeder law enforcement organizations, including municipal forces and RCMP detachments. The organization served as a repository of criminal intelligence information on individuals and businesses of interest,<sup>1120</sup> which could be searched and accessed by law enforcement personnel.<sup>1121</sup> The contribution of information by municipal forces was voluntary, and not all municipal forces sent their information to the bureau. Within the RCMP, NCIS units were regular

---

<sup>1114</sup> See Section 1.6 (Pre-bombing), Khurana Information.

<sup>1115</sup> Testimony of Don McLean, vol. 35, May 29, 2007, pp. 4139, 4156-4157. Exhibit P-101 CAA0871, p. 1, CAA0876.

<sup>1116</sup> Exhibit P-120(c), p. 1, (entry for Oct., 1984: doc 231-3, pp. 2-4).

<sup>1117</sup> Exhibit P-101 CAA0196.

<sup>1118</sup> Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3929.

<sup>1119</sup> Testimony of Henry Jensen, vol. 18, March 7, 2007, p. 1644.

<sup>1120</sup> Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3929.

<sup>1121</sup> When officers wanted to obtain information about particular individuals or groups, they could contact CIS BC through their intelligence unit and obtain access to the material in CIS BC's holdings: Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3932.



contributors of information to the organization.<sup>1122</sup> While CIS was mainly focused on organized crime, it would occasionally receive information about terrorist/extremist issues.<sup>1123</sup>

CIS BC was located at RCMP E Division Headquarters in Vancouver,<sup>1124</sup> and, at the time, it was part of the RCMP structure and staffed and administered entirely by RCMP employees. According to the RCMP Organizational Chart for the period following the creation of CSIS, the Director of CIS reported to the RCMP Deputy Commissioner Operations.<sup>1125</sup> It also appears that at least some members of the VPD at the time viewed CIS BC as a branch of the RCMP.<sup>1126</sup> However, the members who administered CIS BC strove, as much as possible, to operate it as an independent provincial bureau.<sup>1127</sup> Over time, apparently, there evolved a functional independence for CIS BC, with different police forces assigning their personnel to staff the bureau, and the organization came to be recognized as a type of “mini-Interpol.”<sup>1128</sup>

CIS BC organized its information using an index card system. When reports were received, CIS BC officials would read through the reports and create cards for individuals and groups not yet in the CIS BC database, and add additional references for individuals already in the system.<sup>1129</sup> Certain information would also be loaded, by CIS BC and other CIS provincial units, into a searchable national database called the Automated Criminal Intelligence Information System (ACIIS). If a search was done on ACIIS, biographical information that was inputted by other provinces would also show up, and there would be a mechanism to allow investigators to contact the other CIS units to obtain the information in their holdings. However, not all the names and information for individuals identified by CIS BC (or other provincial bureaus) and indexed locally were entered onto ACIIS. Former RCMP Corporal Bob Stubbings, who worked at CIS BC from December 1980 until June 1985, explained that, while individuals like Surjan Singh Gill and Talwinder Singh Parmar were carded, as indicated in the Duncan Blast VIU report, there was no indication that those names had been inputted onto ACIIS.<sup>1130</sup>

Douglas, who headed the RCMP E Division NCIS Terrorist/Extremist Group, testified that he remembered making “...frequent trips to CIS BC on numerous

---

<sup>1122</sup> Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3930.

<sup>1123</sup> At the same time, according to an October 1984 report, CIS BC had no separate file relating to the Indo-Canadian community, which meant that it was not necessarily a resource to which one could refer to easily to obtain a general overview of criminal extremist activity or prominent extremist members in that community: Exhibit P-391, document 124 (Public Production # 3254), p. 14. CIS BC also conducted some analytical work, mainly limited to basic linkage analysis, upon request by various units: Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3933.

<sup>1124</sup> Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3931.

<sup>1125</sup> Exhibit P-110; Testimony of Henry Jensen, vol. 18, March 7, 2007, pp. 1642-1643.

<sup>1126</sup> For example, there is a reference in a VPD Investigation Report respecting a meeting that was held to discuss the VPD's recent investigation of Person 2, where the officer noted that he met with “RCMP CIS BC”: P-120(c), p. 2, (entry for Oct., 23, 1984: doc 7).

<sup>1127</sup> Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3930.

<sup>1128</sup> Testimony of Rick Crook, vol. 20, April 30, 2007, pp. 1923-1924.

<sup>1129</sup> Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3936.

<sup>1130</sup> Testimony of Bob Stubbings, vol. 33, May 24, 2007, pp. 3929, 3931, 3933-3934, 3939.



things.”<sup>1131</sup> Nevertheless, it appears that important information was not consulted in the pre-bombing period, despite the fact that CIS BC files were readily accessible, that CIS BC was housed in the same building as NCIS, and that it was staffed entirely by RCMP members.<sup>1132</sup>

On October 23, 1984, the VPD provided CIS BC with a copy of the report about the interview of Person 2 that had been conducted by Detectives Crook and Warwick,<sup>1133</sup> during which Person 2 disclosed detailed information about an alleged plot to bomb two Air India aircraft.<sup>1134</sup> The report indicated that the interview had been taped and that there could be “two bombs” involved. It also implied that the plot might still go ahead, whether or not Person 2 was in custody, a fact of which Douglas, who was responsible for the investigation of the November Plot, was unaware.<sup>1135</sup> There is no indication that this report was accessed by RCMP NCIS investigators in the pre-bombing period. In fact, there is no evidence that RCMP investigators at any point, either before the bombing or in the years immediately following, requested the transcript of the taped interview from the VPD.<sup>1136</sup> Had this information been reviewed at the time, including the alleged possibility of two planes being involved (which was unknown to Douglas until very recently),<sup>1137</sup> the RCMP might have taken the post-bombing investigation of the November Plot more seriously.<sup>1138</sup>

The VPD VIIU Duncan Blast report, which contained details of the CSIS surveillance of Parmar on June 4, 1985, as well as other contextual threat information,<sup>1139</sup> was received by CIS BC on June 10<sup>th</sup>.<sup>1140</sup> From that date it was fully accessible to the RCMP.<sup>1141</sup> There is no indication that this report was, in fact, accessed by RCMP members in the pre-bombing period. At the time the VIIU report was received by CIS BC, information about Talwinder Singh Parmar, Surjan Singh Gill, and the Babbar Khalsa was already within the CIS BC database.<sup>1142</sup> This was all important intelligence information that the RCMP could, and should, have reviewed.

## Conclusion

In jurisdictions where there were tensions in the RCMP relations with local police forces, there would inevitably have been a negative impact on the receipt by the RCMP of information from those officers, who were often closest to the ground, with the most access to relevant information. Even where relations were less strained, as in Vancouver, the RCMP did not freely share its information nor did

---

1131 Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4032-4033.

1132 Testimony of Bob Stubbings, vol. 33, May 24, 2007, p. 3929.

1133 Exhibit P-120(c), p. 1 (entry for Oct., 1984: doc 231-3, pp. 2-4).

1134 Exhibit P-121, pp. 3-4.

1135 Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4085, 4094.

1136 See Exhibit P-121.

1137 Testimony of Wayne Douglas, vol. 34, May 28, 2007, pp. 4085, 4094.

1138 Testimony of Warren Sweeney, vol. 25, May 8, 2007, p. 2639.

1139 Exhibit P-101 CAA0196.

1140 Exhibit P-101 CAA0862.

1141 Testimony of Axel Hovbrender, vol. 33, May 24, 2007, p. 3907.

1142 Testimony of Bob Stubbings, vol. 33, May 24, 2007, pp. 3936-3937.

it access the local police information available. Where information was actually shared, the RCMP often did not effectively coordinate follow-up or keep proper records.

### 3.6 Lack of Government-Wide Coordination in the Threat Assessment Process

#### The “Mosaic Effect” as a Danger and as a Positive Resource

The “mosaic effect” is a well-known concept in intelligence and security communities. It is commonly invoked as a reason to exempt information from disclosure. The effect refers to the possibility that a seemingly innocuous piece of information can be pieced together with others to reveal a sensitive matter not apparent from any of the individual pieces. The Attorney General of Canada (AGC), in its opening statement, highlighted the *threat* of the mosaic effect in relation to national security.

Sensitivity of information [is] often only apparent to those who are aware of the underlying context ... in the hands of an informed reader apparently trivial or unrelated pieces of information ... can be used to construct a more comprehensive picture when compared with information already known by the recipient or available from another source.<sup>1143</sup>

The AGC warned that the mosaic effect could be used by those hoping to do harm to the national security interests of Canada. However, the mosaic effect can also be deployed positively by the Canadian intelligence community to protect those very same interests. Careful analysis of information reviewed by the Commission reveals that, in the period leading up to the Air India and Narita bombings, a lack of effective communication deprived CSIS – whose role it was to piece such information together – of the opportunity to do so. This meant that the threat assessments produced by CSIS analysts from the information that was actually passed to them were not as fully-informed as they might have been. In turn, reasonable precautions that might have been implemented by protective agencies had they received fully-informed threat assessments were not put into place.

Various government agencies and police forces had information that, if pieced together, could have provided a comprehensive picture of the intentions of Sikh extremists in 1985. However, these agencies failed to share their information openly with CSIS, the agency assigned the exclusive authority to collect security intelligence and produce threat assessments to advise all of government.<sup>1144</sup> At

<sup>1143</sup> Statement by Barney Brucker, Transcripts, vol. 12, November 6, 2006, p. 1064.

<sup>1144</sup> This principle was set out in the 1984 MOU (Exhibit P-101 CAA0076) and 1984 Ministerial Directive issued by Solicitor General Robert Kaplan (Exhibit P-101 CAF0030, pp. 9-10).

the creation of CSIS, the Government of Canada appears to have assumed that other agencies would have relatively little to contribute of security intelligence value from their own sources and knowledge, and thus, little operational guidance was provided to ensure the proper transfer of the information to CSIS.<sup>1145</sup>

Gordon Osbaldeston<sup>1146</sup> made note of this deficiency in his 1987 report:

...despite some improvements that have been made since separation, strategic intelligence is still inadequate. A complaint often heard was that CSIS tended to produce threat assessments in a vacuum, assessments could have benefited from assistance available elsewhere in the intelligence community.<sup>1147</sup>

Professor Martin Rudner, one of Canada's leading experts in the field of intelligence and international terrorism,<sup>1148</sup> characterized the intelligence system in Canada as essentially "routine collection-led."

In Canada, [our intelligence system] is essentially collection-led. This is the notion that the various components of the Intelligence community, the Security Intelligence Service, that's CSIS, the community – the Communications Security Establishment, that's our signals agency; the RCMP, FINTRAC, each of them goes about their business with diligence, no question; competence, no question. But it's routine business. Each of them does the job as they understand it and each of them collects the Intelligence that they routinely decide to collect, and that's what constitutes in fact the collection of Intelligence in Canada.<sup>1149</sup>

Rudner testified that the problem with this system is that the agencies routinely collect information but share it only when its perceived relevance meets special criteria upon which one can justify conducting an investigation.<sup>1150</sup> Each agency collects information in a silo without a sufficiently detailed awareness of the priorities of the other agencies. No one agency has the capacity to "connect

<sup>1145</sup> Testimony of Wesley Wark, vol. 16, March 5, 2007, pp. 1468-1469, 1486-1487.

<sup>1146</sup> Gordon Osbaldeston headed the Independent Advisory Team which produced an October 1987 report, "People and Process in Transition", for the Solicitor General on CSIS recruitment and operational policies (Exhibit P-101 CAA0569).

<sup>1147</sup> Exhibit P-101 CAA0569, p. 19.

<sup>1148</sup> Testimony of Martin Rudner, vol. 92, December 10, 2007, p. 12209.

<sup>1149</sup> Testimony of Martin Rudner, vol. 92, December 10, 2007, p. 12243.

<sup>1150</sup> Testimony of Martin Rudner, vol. 92, December 10, 2007, p. 12244.

the dots” to see the complete picture created by the intelligence collected by the various agencies and to link together all the activities required for an all-of-government approach to intervening in the terrorism cycle.<sup>1151</sup>

It should have been clear that other agencies would collect information relevant to national security. Despite this, the Government of Canada failed to provide meaningful guidance on how and when to share information with CSIS, resulting in a situation where agencies were expending tremendous efforts to collect bits of information that ultimately never went anywhere. This lack of government-wide coordination in the threat assessment process deprived CSIS of the ability to put together the pieces of the mosaic in order to produce threat assessments which were fully informed by the information gathered across the government.

### **Collecting the Pieces of the Puzzle**

The *CSIS Act* assigned CSIS the primary responsibility for advising the Government of threats to the security of Canada.<sup>1152</sup> To ensure that CSIS produced comprehensive threat assessments, the Act allowed CSIS to enter into cooperative information-sharing agreements with police forces across Canada and with other federal and provincial government departments.<sup>1153</sup>

The Office of the Solicitor General produced a document in 1984<sup>1154</sup> to illustrate the responsibilities and cooperative arrangements envisioned by the *CSIS Act*. The chart, shown in Figure 1, illustrates the intended two-way information flow between CSIS and other agencies, including the RCMP, other government departments, local police forces and foreign agencies.<sup>1155</sup> In effect, CSIS was intended to be the repository for all sourced intelligence information from which it could draw to produce the most comprehensive and informed assessments to advise the Government on threats to national security.

---

1151 Testimony of Martin Rudner, vol. 92, December 10, 2007, p. 12245; Exhibit P-101 CAF0063, p. 4.

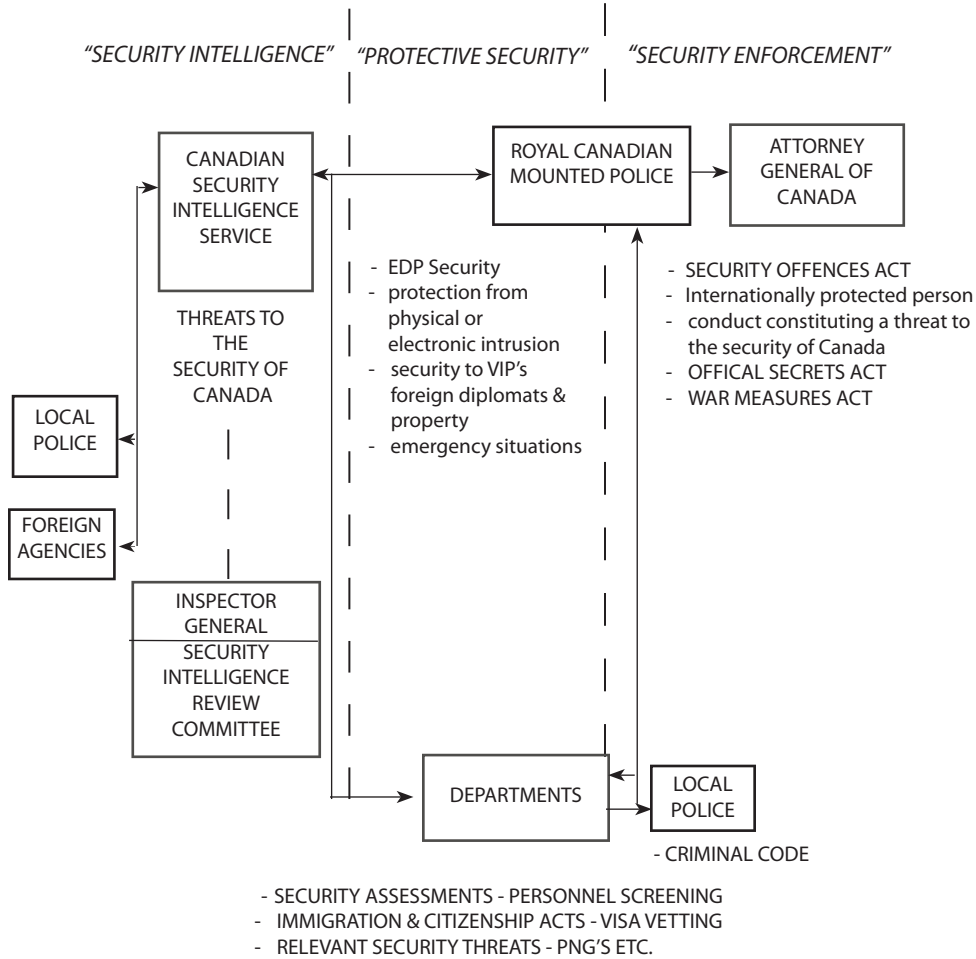
1152 *CSIS Act*, s. 12.

1153 *CSIS Act*, s. 17.

1154 Exhibit P-101 CAF0030.

1155 Exhibit P-101 CAF0030, p. 14.

### THE CSIS ACT AND THE CANADIAN SECURITY SYSTEM



**Figure 1: Division of National Security Responsibilities outlined by the CSIS Act**

CSIS threat assessments would have been strengthened by an ability to draw on the knowledge of the Government of Canada as a whole. In the pre-bombing eriod, CSIS was able to draw on only limited resources for the investigation of the serious emerging threat of Sikh extremism.<sup>1156</sup> It had few, if any, sources within the Canadian Sikh community, particularly in the BC Region. Any additional information would have enhanced CSIS's understanding of the Sikh extremist phenomon.

<sup>1156</sup> See Section 3.3.3 (Pre-bombing), Failure to Allocate Resources.

Several government agencies and police forces were collecting information, which was potentially relevant to CSIS's threat assessments, from sources that were often otherwise unavailable to the Service.<sup>1157</sup> The Department of External Affairs provided the RCMP and CSIS with the mass of threat information received from the Government of India (GOI) in the year prior to the bombings.<sup>1158</sup> This foreign intelligence was critical and, at times, the sole source of information on the Sikh extremist threat – both within and outside Canada. CSIS often initially learned about important threat information through foreign intelligence, including the identity and possible role of Talwinder Singh Parmar and the fact of the very existence of the Babbar Khalsa in Canada. Local police forces, such as the Vancouver Police Department (VPD), could provide an essential “on-the-ground” perspective gained through their community policing role. The VPD had an outreach unit, the Indo-Canadian Liaison Team (ICLT), which was responsible for attending to the policing needs of the Sikh community.<sup>1159</sup> The VPD's access to the community helped compensate for CSIS's lack of human sources in the pre-bombing period. Through its sources, the VPD gathered and passed critical information to CSIS, including the November 1984 bomb plot information and the ‘wait two weeks’ comment at the Khurana meeting.<sup>1160</sup> Transport Canada received information from foreign aviation security organizations,<sup>1161</sup> airports and airlines,<sup>1162</sup> including Air India. The RCMP would often obtain information relevant to national security threats while carrying out its security enforcement and protective policing mandates. The Communications Security Establishment (CSE) collected Signals Intelligence (SIGINT), an important source of timely information on the diplomatic, military, economic, security and commercial activities, intentions and capabilities of foreign governments, individuals and corporations. Other agencies, including the Department of National Defence (DND), Canada Employment and Immigration Commission (CEIC) and Revenue Canada, provided specialized intelligence in their respective fields.

### **The Failure to Put the Pieces Together**

While it was clear that other agencies were collecting relevant threat information, there was a lack of consistent criteria to guide when information should be passed to CSIS. Worse, information was generally passed to CSIS through informal channels. Each agency perceived its information-sharing responsibilities differently, resulting in inconsistent and ad hoc practices for sharing information with CSIS.

Some agencies took an entirely open approach to information sharing. The VPD relationship with CSIS fostered the most effective information-sharing practices. The Indo-Canadian Liaison Team dealt directly with CSIS BC Region investigators to ensure that relevant information was identified and passed

---

<sup>1157</sup> See Section 2.0 (Pre-bombing), *The Intelligence Cycle and Intelligence Community*.

<sup>1158</sup> See Section 2.2 (Pre-bombing), *Failure to Appreciate the Nature and Seriousness of the Threat*.

<sup>1159</sup> Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3764.

<sup>1160</sup> See Section 1.1 (Pre-bombing), *November 1984 Plot* and Section 1.6 (Pre-bombing), *Khurana Information*.

<sup>1161</sup> These organizations include the ICAO and US Federal Aviation Administration.

<sup>1162</sup> Exhibit P-101 CAF0551, p. 4.



in a timely manner.<sup>1163</sup> External Affairs diligently passed the abundance of threat information transmitted to it by the GOI to the RCMP VIP Security Branch. Transport Canada placed considerable importance on the analysis and assessment of threats as provided by CSIS,<sup>1164</sup> and often forwarded threat information it received to the RCMP Airport Policing Branch. The RCMP Protective Policing Directorate (VIP Security and Airport Policing) liaised directly with CSIS to request threat assessments relevant to RCMP protective duties. Both External Affairs and Transport Canada appear to have operated with the understanding that the information they passed to the RCMP would be passed to CSIS through the threat assessment process. It is logical that the RCMP should have passed on all the threat information to CSIS regardless of whether the originating agency specifically requested this transfer. However, failures in the RCMP's information-sharing practices opened up the possibility that full and complete sharing with CSIS of third agency information did not occur.

The RCMP often failed to share relevant information with CSIS.<sup>1165</sup> At times this failure was inadvertent, as RCMP officers lacked training about the nature of intelligence that needed to be passed to CSIS. Also, the RCMP often failed to process information centrally, with the result that the RCMP liaison units responsible for sharing information with CSIS were themselves not even cognizant of relevant information in the RCMP's possession. At other times, the failure to share relevant information with CSIS resulted from the RCMP perception that it, not CSIS, would combine the information for a final assessment.<sup>1166</sup> When the RCMP requested threat assessments from CSIS, the Force did not always share the underlying information that had triggered the requests because RCMP Protective Policing members failed to understand CSIS's need for such information.

The most deficient system of dissemination was that employed by CSE. While other agencies failed to share information due to a lack of formal procedures or a lack of adherence to these procedures (when they existed), the CSE's formal system of dissemination itself was seriously flawed. SIGINT is considered highly sensitive and CSE maintained exclusive control over its dissemination within the Government of Canada. In the pre-bombing period, the CSIS Sikh Desk received its SIGINT reporting through a CSE liaison officer, Pierre LaCompte. Each morning LaCompte searched the CSE database, which contained, on average, approximately 1,000 new reports each weekday,<sup>1167</sup> and brought reports that he considered relevant to CSIS premises for review by the Sikh Desk analysts. The Desk analysts had to return the reports to LaCompte immediately after reading them, and were warned to treat the information with extreme caution.<sup>1168</sup> The major flaw in this system was that the determination of what was relevant

---

1163 Testimony of Ray Kobzey, vol. 32, May 23, 2007, p. 3764.

1164 Exhibit P-364, p. 2.

1165 See Section 3.5.3 (Pre-bombing), RCMP Failures in Sharing with CSIS.

1166 See, generally, Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

1167 Testimony of Pierre LaCompte, vol. 90, December 6, 2007, p. 11914.

1168 Testimony of Bob Burgoyne, vol. 30, May 17, 2007, pp. 3406-3408.

for CSIS purposes was left to an official of the CSE, an organization that was deliberately geared to collect, but not to analyze, intelligence information.<sup>1169</sup> LaCompte was a junior CSE officer who made the important decision on what information should and should not be disseminated to CSIS, informed only by brief meetings with Sikh Desk analysts to identify general search parameters. LaCompte performed this task not only for CSIS, but also the Solicitor General's office and, at times, the RCMP.<sup>1170</sup> With this wide range of clients, LaCompte could not have been aware of the details nor the latest developments in the Sikh extremism file, and easily could have missed the nuances in the information available in the CSE database.

A general lack of interdepartmental dialogue hampered the ability of all agencies to provide context for the information that was to be passed or to gain an awareness of CSIS's investigations, which might better have enabled them to identify relevant information in their holdings. External Affairs and Transport Canada did not generally pass their information directly to CSIS and, thus, there was little opportunity for any dialogue that could have allowed CSIS to benefit from these agencies' perspectives on the context behind the information passed. There was no forum for CSIS HQ Sikh Desk analysts to "brainstorm" with government agencies and police forces about the Sikh extremist threat.<sup>1171</sup> This situation is somewhat ironic in light of the commonly pronounced concern by the RCMP that CSIS lacked the ability to identify "criminality" and, hence, information that needed to be passed to the RCMP. Brief reflection would have indicated that a lack of information about the RCMP's interests and investigations, combined with limited access to RCMP information, would have made the identification of "criminality" even more difficult for CSIS. It should also have been clear that the reciprocal situation would be equally problematic: i.e. that other agencies would lack the expertise and knowledge to identify information in their holdings relevant to CSIS's sensitive and secretive investigations. Agencies were collecting information "for collection's sake"; significant collection efforts undertaken by these agencies, particularly the CSE, were effectively wasted as relevant information languished unshared in their holdings due to an inability to identify its importance to CSIS investigations.

CSIS itself appeared not to recognize the importance of other agencies' information to its own threat assessment product. In making its assessments, CSIS would draw on the information from its own resources, but did not explicitly ask other agencies for any relevant information they might have had.<sup>1172</sup> John Henry, Head of the CSIS Threat Assessment Unit (TAU), was responsible for the transmission of threat assessments between the RCMP and CSIS. He testified that he "hoped" that the agencies requesting threat assessments would send information relevant to the threat assessment on their own initiative, or that the

<sup>1169</sup> Testimony of William Sheahan, vol. 90, December 6, 2007, p. 11902; Testimony of Pierre LaCompte, vol. 90, December 6, 2007, p. 11926.

<sup>1170</sup> Testimony of Pierre LaCompte, vol. 90, December 6, 2007, p. 11914.

<sup>1171</sup> Testimony of Bob Burgoyne, vol. 31, May 22, 2007, p. 3491. Burgoyne noted that CSIS BC Region investigators had excellent contacts within the police services and reported back to CSIS HQ. However, the Sikh Desk analysts at HQ who drafted the TAs had no direct contact.

<sup>1172</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2540-2541.

CSIS operational desk preparing the threat assessment would inquire to see if other government agencies held relevant information.<sup>1173</sup> In the pre-bombing period, there was no sign that CSIS vigorously addressed the lack of information sharing by other agencies.

The end result was a situation in which CSIS was the central intelligence agency, with an abundance of threat information of unknown reliability from the Indian government, few resources to corroborate this information through its own investigations and little assistance from other agencies. This situation made the sheer volume of threat information from the Indian government appear as if it was “crying wolf,” particularly in light of the lack of corroborating information from other sources. The deficiencies in CSIS’s own investigation<sup>1174</sup> could have been mitigated by the full and open sharing of information by other government agencies and police forces. Had information been properly shared, CSIS might have been in a better position to evaluate the significance of information that was already in its possession, instead of being forced to interpret a mosaic with several pieces missing and some areas overly represented. More significantly, however, with regard to the most important information in relation to threats to Air India in the year leading up to the bombings, CSIS appears to have been in possession of none of the pieces of the mosaic.

### **The Missing Pieces**

The first incident in which the mosaic effect might have been applied relates to the November 1984 Bomb Plot.<sup>1175</sup> Information that Sikh extremists were organizing to put a bomb on an Air India plane was first obtained through Person 1 by the RCMP’s Vancouver Drug Squad (VDS) in September 1984. The RCMP VDS did not share this information with its own HQ, nor did it share it with outside agencies, despite its clear relevance to the mandates of both Transport Canada and CSIS. Over a month later, the VPD obtained similar information from an independent source, Person 2, and informed an RCMP member of CIS BC and a CSIS BC Region member on October 23<sup>rd</sup>. Effectively, the bomb plot, known to the RCMP since mid-September 1984, reached CSIS only in late October 1984 through another source. Even then, the RCMP E Division NCIS Extremist/Terrorist Section was aware that the Person 2 information had also previously been provided by another, independent source (Person 1), and did not advise CSIS of the corroboration.

Several threats were made that action would be taken against Air India during the month of October. Knowledge of the November 1984 plot information obtained by the RCMP in September would have been clearly relevant in this tense climate. In early October, the GOI warned of the threat that Sikh extremists in foreign countries would stage a spectacular event to coincide with the Hindu

---

<sup>1173</sup> Testimony of John Henry, vol. 25, May 8, 2007, pp. 2541-2542.

<sup>1174</sup> See Section 3.3.3 (Pre-bombing), Failure to Allocate Resources.

<sup>1175</sup> See Section 1.1 (Pre-bombing), November 1984 Plot and Exhibit P-120(c): November 1984 Plot – Chronology.

festivals that month.<sup>1176</sup> The blowing up of an Air India plane was listed as a possible means of attack.<sup>1177</sup> The GOI warned that Bagri was planning to attack an Air India plane in October.<sup>1178</sup> The GOI further warned that Sikh extremists in London had decided to hijack an Air India flight specifically in North America. On October 17<sup>th</sup>, the RCMP requested a TA from CSIS on the basis of this information, but failed to pass on the November 1984 plot information as it had not been transmitted internally within the RCMP to the Protective Policing Branch that made the TA request.<sup>1179</sup> On October 22<sup>nd</sup>, CSIS provided a TA concluding that the possibility of a hijacking in Canada was remote, but could not be ruled out.<sup>1180</sup> The TA noted that CSIS had no independent information to corroborate the threats. Days later, after CSIS received the November 1984 plot information from the VPD, it issued an updated TA concluding that "...there is a real possibility that Sikhs will damage an Air India plane."<sup>1181</sup>

This radical change in the CSIS assessment of the risk from "remote" to "a real possibility" demonstrates the dramatic influence of new information in CSIS threat assessments. Had the RCMP passed information about the November 1984 bomb plot to CSIS in September, CSIS would have undoubtedly viewed the threats of actions to be taken in October with more urgency, and pursued more vigorously its investigation into these threats. Conversely, the change in the CSIS position also demonstrates the potential for a real threat to be discounted because of an important piece of information not being passed on for CSIS to consider.

In any event, no hijacking or sabotage of an Air India airplane occurred in October or November of 1984, so that in the short term, there were no disastrous consequences from the failure to pass on relevant information. However, the RCMP continued to discount the information it received, which indicated that the bomb plot had been postponed rather than abandoned, when Person 2 was incarcerated in October 1984.<sup>1182</sup> This lax attitude led to growing internal RCMP indifference to any kind of follow-up. It may also account for the RCMP's failure to pass along to CSIS this information and previous information – only discovered in 1986 in RCMP files – indicating that Person 1 had made statements to police in September 1984 about a man in Duncan who could manufacture "nitro" for blowing up an Air India flight. These latter two pieces of the possible mosaic were particularly relevant to CSIS's ability to understand the threat, as they were to the subsequent police investigations.

The most striking instance of the failure to benefit from the mosaic effect is the oft-discussed June 1<sup>st</sup> Telex.<sup>1183</sup> The RCMP obtained this critical information

1176 Exhibit P-101 CAA0101, p. 1.

1177 Exhibit P-101 CAA0101, p. 1.

1178 Exhibit P-101 CAA0097, CAA0101, p. 2.

1179 Exhibit P-101 CAA0103.

1180 Exhibit P-101 CAB0149.

1181 Exhibit P-120(c), p. 2 (entry for Oct. 26, 1984: doc 229-3, p. 5).

1182 See Section 1.1 (Pre-bombing), November 1984 Plot and Exhibit P-120(c): November 1984 Plot – Chronology.

1183 See Section 1.2 (Pre-bombing), June 1<sup>st</sup> Telex.

warning all Air India stations of the threat by Sikh extremists of sabotage attempts by time/delay devices or explosives in registered baggage and calling for the implementation of five counter-sabotage measures.<sup>1184</sup> The RCMP detachment at Toronto's Pearson Airport received the June 1<sup>st</sup> Telex from Air India officials and passed the information to the RCMP HQ Airport Policing Branch. The Airport Policing Branch responded by requesting an updated threat assessment from CSIS, but failed to pass the actual June 1<sup>st</sup> Telex to CSIS. At the Inquiry, CSIS HQ Sikh Desk analysts confirmed that they had never seen the information in the June 1<sup>st</sup> Telex. CSIS issued a TA in response to the RCMP request based on the information in its possession. Without the benefit of this new information, CSIS concluded that the "threat potential" to Air India was "high," but that it was not aware of any "specific threats" at the time.<sup>1185</sup>

CSE received information independently that corroborated the underlying information in the June 1<sup>st</sup> Telex, indicating that specific security measures were to be undertaken by all Air India stations both within and outside of India during June 1985. Shortly after the RCMP received a copy of the June 1<sup>st</sup> Telex through Air India, separate CSE information indicated an increase in specific security measures, substantially similar to those listed in the June 1<sup>st</sup> Telex, which were being undertaken at Indian airports in light of threats of hijackings and bombings by Sikh extremists. Security audits were being undertaken at several Indian airports in response to this threat. Other CSE information at the time noted that the GOI had recently shown an increased interest in the security of airports against the Sikh terrorist threat in the month of June 1985.

There is no record that any of this information was passed on by CSE to CSIS or to any Canadian government personnel. William ("Bill") Sheahan, who serviced high-level DEA clients with specific interests in Sikh extremist issues, maintained weekly distribution notes, none of which mentioned any of these documents. LaCompte, who delivered CSE reports to the CSIS Sikh Desk, recalled the November 1984 plot when asked about relevant reporting immediately after the bombings, but did not recall these more recent relevant documents.

The failure by the RCMP to pass on the June 1<sup>st</sup> Telex is difficult to understand. It deprived CSIS of a clear and direct warning, attributed to the intelligence section of India's state-owned airline, that Sikh extremists were targeting Air India flights for sabotage. The only reason cited by Sgt. J.B. ("Joe") MacDonald of RCMP HQ Airport Policing for not passing the June 1<sup>st</sup> Telex was that he saw "no need" to share the information with CSIS.<sup>1186</sup>

Evidence before the Commission indicates that at times there was a perception among RCMP and Transport officials that threat warnings sent by Air India, such as the June 1<sup>st</sup> Telex, were provided simply for the purpose of obtaining additional security for Air India flights at no extra cost.<sup>1187</sup> This sort of reasoning would have been put into question, if not refuted altogether, by the CSE information that the GOI was assiduously pursuing these very same security upgrades for

---

1184 Exhibit P-101 CAA0185.

1185 Exhibit P-101 CAA0199.

1186 See Section 1.2 (Pre-bombing), June 1<sup>st</sup> Telex.

1187 See Section 1.2 (Pre-bombing), June 1<sup>st</sup> Telex.

Air India flights, both inside and outside India, because of fears of violence from extremists and undertaking real measures in response to the threat. At the time, all Indian airports and major airlines were nationalized. The cost of any requirement to implement increased security at Indian airports would have been borne by the Indian government. Thus, a call for increased security at Indian airports could not have been an attempt to obtain security for free. Had CSIS been able to analyze the June 1<sup>st</sup> Telex in light of the CSE information, it might have been able to warn the RCMP that both pieces of information likely related to a *bona fide* threat.

In the end, of course, CSIS had none of the information in question: neither the June 1<sup>st</sup> Telex, nor any of the CSE information about the increased security measures in Indian airports. Each of these items of information might have seemed relatively inconclusive or ambiguous on its own. However, when pieced together by a trained analyst, a much clearer, and undoubtedly alarming, picture probably would have been discerned.

Had CSIS been given the additional information, namely, that the November Bomb Plot had only been postponed, as well as the information about the man in Duncan who could manufacture “nitro” for blowing up an aircraft in flight, an even clearer mosaic pattern should have emerged. The pattern would have pointed to the seriousness of the threat to Air India as well as to the potential that it could involve sabotage and not only hijacking, the concealment of a bomb in checked baggage as the possible mode of sabotage, and the real possibility that the focus of an attack against an Air India plane might be in Canada, carried out by Canadian residents.

It is, of course, also possible that, even if the June 1<sup>st</sup> Telex and the CSE information had been passed to CSIS, the Sikh desk would still have been unable to “connect the dots”, or that the pattern would have been lost amid other information given to CSIS. The critical point is that CSIS never had the opportunity to assemble the mosaic because those key pieces were never given to it.

As a result, when CSIS issued its final TA<sup>1188</sup> before the bombings on June 18, 1985, it made no reference to the threat to Air India or to any aviation security threats, and had little more to report other than that the general threat was only “slightly less serious”, a conclusion apparently reached on the basis of what they thought to be common sense.

The failure to coordinate government-wide information led to a situation where the lack of information-sharing with CSIS by various agencies resulted in CSIS returning a virtually meaningless threat assessment in the critical week before the bombings. Critical information remained siloed within each agency’s holdings, robbing CSIS of the opportunity to effectively carry out its mandate to assemble the puzzle for the benefit of national security.

---

<sup>1188</sup> Exhibit P-101 CAB0321.



### Why Was the Information Not Passed to CSIS?

There has never been an official explanation for the failure of the RCMP to send the June 1<sup>st</sup> Telex to CSIS at the time that it asked CSIS for an updated assessment of the threat against Air India, aside from MacDonald's testimony that he saw "no need" to share the information. The threat assessment update request was made in direct response to the RCMP's having been given the telex by Air India, and the (inaccurate) representation by the RCMP to the Honourable Bob Rae that it had passed the telex on to CSIS along with the update request demonstrates, if nothing else, the obvious conclusion that it should have been passed on, as the Attorney General of Canada conceded in its Final Submissions.<sup>1189</sup> Against the backdrop of erratic RCMP internal communications and poor training about the threat assessment process and the nature of intelligence that needed to be passed to CSIS,<sup>1190</sup> the failure to communicate externally is not surprising.

As for the failure of CSE to communicate potentially relevant information, the explanation seems clearer and seems to be rooted in a faulty structural design. CSE was deliberately given a mandate to collect signals intelligence (defined earlier) but not to analyze it. As such, it was structurally incapable of determining for itself the relevance of all but the most obvious intelligence it might collect, having instead to rely on general relevance criteria and markers provided by CSIS, the RCMP, DEA, or other clients. This would seem like a recipe for almost certainly missing at least some of the relevant information that might not fit exactly within the predetermined criteria. LaCompte testified that, in his daily search, he would look for reports "...impacting on Canadian security."<sup>1191</sup> Using the limiter "Canadian security" had the potential to miss capturing threat information warning of similar threat situations in other countries that could have provided context to threats in Canada. In June 1985, several CSE reports indicated several threats to major Indian targets were being made by Sikh extremists and the GOI was taking steps to verify and respond to these threats. In fact, as warned, bombings did occur at major public locations in India. After the Air India Flight 182 and Narita bombings, reporting continued to emphasize the importance of implementing specific security measures in light of the ongoing terrorist threat, specifically referencing the instructions to increase airport security measures sent to all Air India stations worldwide nearly one month prior. None of this reporting appears to have been disseminated outside of CSE. All this information represents more missing pieces of the puzzle.

### Recognition of the Lack of Coordination

The Canadian government recognized the deficiency in the lack of government-wide coordination in the threat assessment process in the pre-bombing period. A May 31, 1985 report of the PCO Intelligence and Security Coordinator<sup>1192</sup>

<sup>1189</sup> See Section 1.2 (Pre-bombing), June 1<sup>st</sup> Telex.

<sup>1190</sup> See Section 3.4 (Pre-bombing), Deficiencies in RCMP Threat Assessment Structure and Process.

<sup>1191</sup> Testimony of Pierre LaCompte, vol. 90, December 6, 2007, p. 11914.

<sup>1192</sup> The Intelligence and Security Coordinator position was created in February 1985 and filled by Blair Seaborn. Seaborn also acted as Chair for the Interdepartmental Committee on Security and Intelligence (ICSI), a high level interdepartmental committee mandated to produce policy-neutral threat assessments. See Section 2.0 (Pre-bombing), The Intelligence Cycle and Intelligence Community, for more detailed information.

recognized the "...obvious need for greater interdepartmental coordination." It recommended the establishment of frequent interdepartmental reviews of threat assessments by a group composed of External Affairs, CSIS, RCMP, CSE, PCO and DND (and CEIC and Transport Canada as required).<sup>1193</sup>

In May 1985, an ad hoc working group on Sikh terrorism was formed by External Affairs under the direction of James Bartleman, with participation from several agencies including the RCMP, CSIS, CSE and the Solicitor General. Its mandate was to ensure that all relevant material was looked at, and that nothing "... fell between the cracks."<sup>1194</sup> William Warden, who was the Canadian High Commissioner in New Delhi from 1983 to 1986, was in Canada in May 1985 and attended the early meetings of the ad hoc working group. He felt that the meetings showed the first attempt by the government machinery to coordinate the knowledge of various agencies:

[I]n May '85, when I attended that meeting ... I was underwhelmed in the sense that the issue had been around – for months at that point, and my feeling at that time was, why didn't we do this months ago instead of waiting until May of '85? But nonetheless, I have to say that by May of '85, I did feel that finally the machinery was starting to get its act together, and in fact information was coming in, ... there was a lot of close interaction on the part of the agencies; the Indian Government had its excellent sources in Canada, the CSIS, the RCMP, and people were starting to pull together.<sup>1195</sup>

These efforts show that the Government of Canada was acting to correct the known deficiency in the threat assessment process. The failure to pass on the relevant information described in this section demonstrates that these actions came too late to affect the Government's assessment of the Sikh extremist threat before the Air India and Narita bombings.

## Conclusion

The lack of coordination in the threat assessment process between CSIS and other intelligence collection agencies within the Government of Canada deprived CSIS of information that might have allowed CSIS to apply the mosaic effect. CSIS was (and continues to be) aware of the dangers of the mosaic effect, using it as a basis for protecting certain sensitive information from dissemination. However, this very technique could have led to a dramatic benefit for the threat assessment process, if CSIS had been provided with relevant information held by other government agencies.

---

<sup>1193</sup> Exhibit P-101 CAF0060.

<sup>1194</sup> Testimony of James Bartleman, vol. 22, May 3, 2007, p. 2105; Testimony of William Warden, vol. 24, May 7, 2007, p. 2427; Exhibit P-101 CAA0017.

<sup>1195</sup> Testimony of William Warden, vol. 24, May 7, 2007, pp. 2388, 2413, 2427.

Several government agencies were collecting and disseminating intelligence relevant to CSIS's investigation of Sikh extremism. Because of a lack of clear guidance from the Government of Canada about when and how this information should be passed on to strengthen CSIS's threat assessment product, information-sharing practices were inconsistent across government agencies and police forces. The VPD had the best information-sharing practices, consulting directly with CSIS and sharing important information. External Affairs and Transport Canada's information-sharing systems were hampered by the fact that they relied on the RCMP to pass information to CSIS. The RCMP and CSE clearly limited the information they shared with CSIS. The RCMP failed to share largely because of internal communication breakdowns and a lack of training and, at times, because of its perception that it, not CSIS, would produce the final threat assessment. CSE often failed to share information because its system to identify and disseminate relevant information was fundamentally flawed. CSE personnel were tasked to identify relevant information but did not have the analytical capacity or the requisite knowledge of CSIS's intelligence investigations. The result was that relevant information could, and did, remain unnoticed within CSE holdings.

The major deficiency was that these front-line collection agencies made determinations about the relevance of information without in-depth knowledge of CSIS's investigations. The collectors would only pass intelligence that had reached a threshold of being obviously relevant. This system would inevitably result in missed opportunities to apply the mosaic effect, opportunities which might have allowed CSIS to put together a more complete picture of the facts. A better method of dissemination would have been to have personnel with knowledge of CSIS investigations and programs review the collected intelligence and select the relevant material. Such personnel would have been far more qualified to assess the relevancy of intelligence information. Unfortunately, such a system was not in place in 1985, and critical information like the June 1<sup>st</sup> Telex and related CSE information was not made available to inform the CSIS assessment of the threat to Air India.

The evidence shows that the Government of Canada was aware of the need to improve communications and coordination among agencies with regard to threat assessment and threat response in the pre-bombing period. However, the Government was slow to improve this recognized deficiency. Ultimately, the silos within the various agencies created a system where each agency could claim to be adequately carrying out its mandate, while still allowing intelligence failures to occur as a result of the lack of coordination of the respective mandates. In effect, while each agency was doing its job, it was the structure of this overarching system that allowed information-sharing failures to occur. These failures impaired the Government's ability properly to assess the threat of Sikh extremism.

The undeniable conclusion from the foregoing is that had information been efficiently shared among agencies rather than being retained in various silos, CSIS would have been able to assemble enough of the "mosaic" to provide a well-informed threat assessment to the RCMP. This might have been useful in a criminal investigation context, and might have prevented the destruction of Air India Flight 182 and the murder of 329 people.