Symbiosis or Vassalage? National Security Investigations and the Impediments to Success.

Introduction

Symbiosis or vassalage? This question is aimed at the relationship between CSIS and RCMP or more generally between law enforcement and intelligence agencies. In my experience of terrorist investigation for over 28 years in Northern Ireland, I have witnessed the benefits or both the symbiotic relationships with intelligence agencies and also the detriment of subservience or worse the complete disregard for the role of investigators in proactive or reactive terrorist investigation.[1] In the conduct of parallel investigations under distinct legal mandates each agency gathers information and evidence that may be crucial to the execution of the other's mandate. One mandate does not take precedence over the other in the law. The national security threat has created the need, in both organizations, to implement pre-emptive methods that will prevent successful terrorist operations before they occur. [2] The standards of information or evidence-gathering are different as between the organizations, and, in many instances, the divergent goals of investigators in the agencies create tensions. Where both organisations instigate a parallel investigation, the question arises as to who should have primacy, and, when should one organisations needs become subservient to the other- if ever?

On the 17th March 2002 (St Patrick's Day) in Belfast, Northern Ireland, terrorists were able to breach the security of a police establishment that contained the intelligence units responsible for

[1] For the effects of Intelligence Community on terrorist investigations see Jon Moran, "Evaluating Special Branch and the Use of Informant Intelligence in Northern Ireland" (2010) Intelligence and National Security 1; The Billy Wright Inquiry, *The Billy Wright Inquiry Report*, (London:TSO, 2010) at 90;, Peter Gill, "Security Intelligence and Human Rights:Illuminating the 'Heart of Darkness'?" (2009) Intelligence and Nationa;l Security 78 at 93-94 and 97-98

[2] Frédéric Mégret,"Terrorism and Human Rights. A Decade of Canadian Practices" (2011). Available at SSRN: http://ssrn.com/abstract=1762763at p4

the Greater Belfast Region. They were able to make their way to an office where a solitary intelligence officer was on duty. His duty was to monitor the telephones and talk to any informants that made contact. The terrorists overpowered the officer, assaulted and bound him, and left with material from the office. [3] Their objective was to obtain information that would reveal to them the identity of the informants that had been recruited by police intelligence units, MI5 and other military intelligence units operating in the province.

The author of this paper was the Detective Chief Superintendent in charge of the subsequent criminal investigation. In a discussion with the Chief Constable of the RUC, I informed him that I was well aware that a separate and parallel investigation by the services intelligence branch, C3, and MI5 would already be underway. I emphasised that the recent experience of parallel investigations had only resulted in criticism and missed opportunities. The Chief Constable accepted that an effective and national security efficient investigation required the one overall investigation with complete access to all intelligence and operational capabilities. Within one hour I was in a briefing with C3,(the RUC Intelligence Branch), and MI-5. They had already carried out considerable analysis of available intelligence and data. One name in that material provided the first clue. It had almost been discounted as an aberration in the data. Only those involved in an aspect of the criminal investigation would have recognised it. Had parallel operations continued, it may never had been discovered or at least not for some time.

[3] Brian Rowan, "Analysis Behind the Break In", Friday 19th April 2002.
http://news.bbc.co.uk/2/hi/uk_news/northern_ireland/1939219.stm

The Air India report extensively reviewed the relationship between CSIS and the RCMP in national security investigations.[4] The relationship between the two organisations could be improved if this were undertaken together with procedural and legislative amendments that could help to shape operational effectiveness. This paper posits that where the mandates of the RCMP and CSIS overlap, a symbiotic relationship is crucial to the success of national security operations. The paper will consider alternative strategies employed in national security investigations and options that have been suggested as solutions to the national security dilemma.

Mandates and Relationships.

CSIS is a relatively young organisation. Its genesis is found in the recommendations of both the 1969 Report of the Royal Commission on Security (the "Mackenzie Commission")[5] and the Commission of Inquiry Concerning Certain Activities of the Royal Mounted Police (the "McDonald Commission"). [6] Both inquiries recommended that the security mandate should be the responsibility of a civilian agency completely separate from the police function.[7] The current mandate of CSIS is set out in sections 12-20 of the *Canadian Security Intelligence Service Act*.[8] The aspect of the mandate most frequently given voice by CSIS spokespersons is the collection, analysis, production and sharing of information to inform government of the threats to national

[4] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, John C Major Q.C. (Ottawa: Public Works and Government Services Canada, 2010)
[5] Canada. Report of the Royal Commission on Security (The Mackenzie Commission). Minister of Supply and Services Canada, June 1969
[6] Canada. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (the McDonald Commission).*Freedom and Security Under the Law, Second Report.* Ottawa: Minister of Supply and Services Canada, August 1981.
[7] For background on the origins of CSIS see Philip Rosen, *The Canadian Security Intelligence Agency* (Ottawa: Parliamentary Research Branch, 2000) available online at http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/CIR-e/8427-e.pdf
[8] R.S.C. 1985, c. C-23

security.[9] CSIS directors have emphasised that the agency is not a law enforcement agency. They possess no enforcement powers of compulsion or detention. Their objective is to investigate threats prior to the execution of that threat. They do not collect evidence and the information collection methodology does not meet the evidentiary standards required by the courts.[10] CSIS views its role in a national security investigation as separate from, and parallel to, that of law enforcement.[11]

In criminal and national security investigations the role of the police is to prevent, detect and prosecute the crimes through investigation and the collection of evidence. Law enforcement is said to be responsive. Their interest in intelligence is based only in its use to locate 'evil doers' and to assist in their conviction. Police have not been interested in the analysis of intelligence as an aide to plan operations or to tailor a police response to emergent patterns.[12] What fails to be understood is that law enforcement operates in a dynamic environment and has to adapt through necessity. Society has yet to recognise the obvious need for policing to undergo a metamorphosis to cope with the changing police environment, and all the while, the police continue to adhere to the traditional role expected of it.

---

[9] Canada, Interim Report of the Special Senate Committee on Anti-Terrorism, *Security, Freedom and the Complex Terrorist Threat: Positive Steps Ahead* March 2011(Chair: The Honourable Hugh Segal) at 16-17 online at http://www.parl.gc.ca/Content/SEN/Committee/403/anti/rep/rep03mar11-e.pdf at p23

[10] Jim Judd, Director of CSIS "Speaking Notes for the Canadian Bar Association Panel on National Security and Human Rights" St Johns, Newfoundland on 15th August, 2006. available online at http://www.csis-scrs.gc.ca/nwsrm/spchs/spch15082006-eng.asp

[11] David McClelland, Director General of CSIS, Prairie Region, CSIS Press Conference Statement in respect of terrorist related charges of Manitoba students, 15th March 2011 available online at http://www.csis-scrs.gc.ca/nwsrm/spchs/sttmnt-wnnpg-15032011-eng.asp

[12] Gregory F Treverton, "Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons" (2003) 18 Intelligence and National Security 121at p122

Brodeur notes that the clear dichotomy between the functions of intelligence gathering and the role of policing has never been questioned.[13] Recent inquiries have continued to acknowledge the distinct roles.[14] In the terrorist trial of *Ahmad* Dawson J set out his view of the distinct mandates.

> .... the RCMP is a police force with policing duties described in ss. 17 and 18 of the *RCMP Act*, R.S. 1985, c. R-10, and s. 6 of the *Security Offences Act*, R.S. 1985, c. S-7. One of its main functions and duties is to mount investigations that lead to the successful prosecution of those who break the law. CSIS, on the other hand, is an intelligence gathering agency which collects and analyses information (not evidence) for the purpose of advising government. The RCMP works in a forensic environment where evidence must be collected in a manner which renders it admissible, and is subject to having the fruits of its investigations disclosed publicly in the course of criminal prosecutions. CSIS relies on information from many sources, including foreign governments and intelligence agencies and covert domestic sources. Most of those sources must be protected if CSIS is to remain effective. Intelligence information shared by foreign agencies is received on the basis it will be protected.[15]

The Supreme Court of Canada has recognised that the initial reports that led to the birth of CSIS, and its separate mandate from law enforcement, could not have envisioned the changes that have occurred. The Court has observed that the activities of the RCMP and CSIS have converged as result of the domestic and international terrorist threat.[16] The conclusion of the Supreme Court should come as no surprise. Bob Kaplan, Solicitor General at the time of the formation of CSIS, foresaw that it would not always be possible to delineate between CSIS and RCMP security investigations and predicted that overlaps would occur.[17] The mandates of the intelligence

---

[13] Jean-Paul Brodeur, "The Royal Canadian Mounted Police and the Canadian Security Intelligence Service: A Comparison Between Occupational and Organizational Cultures" in Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, John C Major Q.C. (Ottawa: Public Works and Government Services Canada, 2010) at Vol. 1. Research Studies: Threat Assessment and RCMP/CSIS Co-operation. 182 at p 204.
[14] see Commission of Inquiry into the Actions of Canadian Officials in Relations to Maher Arar: *Report of the Events Relating to Maher Arar, Analysis and Recommendations* (Ottawa: Government Services, 2006) at 312.
[15] *R. v. Ahmad*, 2009 CarswellOnt 9304 (ONSC) (Ruling No 14) at para 32
[16] *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 CarswellNat 1898, 2008 SCC 38, para 26
[17] Ministerial directive, "Bill C-9 and the Conduct of RCMP Security Responsibilities," dated 10 July, 1984. Bob Kaplan, Solicitor General, to the Director of CSIS, July 239, 1984. in Wesley Wark, "The Intelligence-Law Enforcement Nexus: A Study of cooperation between the Canadian Security Intelligence Service and the Royal

agency and law enforcement are distinct, but this distinction should not be taken too far.[18] Practically speaking national security is achieved through both mandates.

Memoranda of understanding (MOU) developed between CSIS and the RCMP have regulated the relationship since CSIS was formed in 1984. Professor Wark has provided an overview of the evolution of the MOU's over the years 1984-2006. In 1990, RCMP relied on CSIS, as the sole intelligence collectors in national security for intelligence relevant to national security investigations. In the current 2006 MOU this reliance has been deleted and the need for cooperation is affirmed in the 'partnership' between the two agencies.[19]

The concept of partnership is simple to articulate and difficult to actualize. There will always be suspicion and tension between the two organisations as the natural result of differing mandates that must in instances of conflict compete for primacy. RCMP national security investigators require intelligence from CSIS in order to focus their resources, develop investigative opportunities and harvest the evidence that can be identified in the acme of the intelligence and evidence chain. In national security cases, the criminal investigators will often pressure the intelligence agency to produce intelligence that is already in their possession or to invest resources in an intelligence collection plan that will meet the investigators intelligence

---

Canadian Mounted Police, 1984-2006, in the Context of the Air India Terrorist Attack" in " the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, John C Major Q.C. (Ottawa: Public Works and Government Services Canada, 2010) at Vol. 1 Research Studies. Threat Assessment and RCMP/CSIS Co-operation. 147 at 168

[18] Dame Stella Rimmington, director MI5 "Intelligence, Security and The Law" James Smart Lecture 3rd November 1994 available online at https://www.mi5.gov.uk/output/director-generals-james-smart-lecture-1994.html

[19] Wesley Wark, "The Intelligence-Law Enforcement Nexus: A Study of cooperation between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, 1984-2006, in the Context of the Air India Terrorist Attack" in " the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, John C Major Q.C. (Ottawa: Public Works and Government Services Canada, 2010) at Vol. 1 Research Studies. Threat Assessment and RCMP/CSIS Co-operation. 147 at 168-172

requirements. Where intelligence is not forthcoming the investigators will have various suspicions about the motives of intelligence agencies. First, they may suspect that there is no appetite to meet the needs of a police national security investigation. Second, they will suspect that the agency is carrying out its own parallel investigation either heading in a different direction to the police operation, or in the belief that the police investigation may interfere with the course of the intelligence operation. Third, the agency is intent in obstructing the police operation to protect their confidential sources or technical deployments.

CSIS is jealous of its secrets. It has openly stated that it has had to withhold information about criminal offences from the police service.[20] This has to be expected from an agency involved in covert activities. The intelligence community operates on a 'need to know' basis.[21] The assessment is made on the individual pieces of intelligence product. However, the 'need to know' is a vague concept and in the Canadian theatre there appears to be no specific guidelines or objective assessment as to when law enforcement "needs to know" such that intelligence must be or may be disseminated. Dissemination from intelligence agencies to law enforcement often depends upon the personal relationships between individuals from respective organisations. The author of this paper was often given access to intelligence product on the basis that it would not be shared with superior officers or anyone else outside of the defined circle of knowledge. Caveats imputed in this way have challenges of their own. Although it may help an investigator focus resources in specific directions, information cannot be acted upon or be brought openly into the actual inquiry.

---

[20] SIRC Annual Report 1986-1987 at 25-26

[21] *Re Almrei*, 2009 FC 314 at para 30; *Re Harkat*, 2009 FC 59 at para 26; *Re Harkat*, 2009 FC 204 at para 36; *Royal Canadian Mounted Police Public Complaints Commission v. Canada*, 2005 FCA 213 at para 40 and 46; *Khadr v. Canada (Attorney General)*, 2008 FC 807 at para 65.

Impediments to Information Dissemination and Success in National Security Operations.

The Air India report produced six main concerns from both CSIS and the RCMP that amount to impediments to the dissemination of intelligence and success in national security investigations.

CSIS concerns include:

(1) In their treatment of disseminated information the RCMP endanger sources, disclose allies' confidences and make investigations by CSIS much more difficult.
(2) The scope of *Stinchcombe*[22] disclosure obligations, create a risk of public exposure of intelligence operations and reduce the effectiveness of CSIS.
(3) Closer cooperation with RCMP will blur the lines that separate their distinct functions and mandates.

RCMP argue that:

(4) CSIS does not appreciate the overlap of their mandates in counterterrorism matters.
(5) CSIS have disregarded evidentiary standards in the collection and retention of intelligence product.
(6) CSIS will seek to protect its own investigations in preference to the criminal investigations.[23]

The culmination of these concerns is an atmosphere of ambivalence. CSIS is ambivalent about disseminating product to the RCMP, and, the RCMP is ambivalent about the value of the intelligence disseminated by CSIS.[24] The net effect of this ambivalent attitude is that the capacity to respond to the national security threat to Canada is diminished. The ambivalence limits the potential sharing between agencies and so diminishes the available counter-terrorism strategies.

Addressing the Concerns

Section 19(2) of the *CSIS Act* provides the agency with discretion whether to share information with law enforcement.[25] Therefore there is no statutory duty that compels the dissemination of intelligence to the RCMP. Stanley Cohen asserts that that the discretion given to CSIS to share

[22] *R.v. Stinchcombe*, [1991] 3 S.C.R. 326
[23] *supra* n4 at Vol. 3. The Relationship Between Evidence and Intelligence and the Challenge of Terrorism Prosecutions at p22-33
[24] *ibid* at 25
[25] *supra* n8

information with law enforcement is only actionable when that information has been gathered in *bona fide* investigations and duties in furtherance of the CSIS mandate. Thus he emphasises that CSIS are not to act as a proxy in the collection of intelligence for law enforcement.[26] It is not Cohen's view that section 19 should be interpreted so narrowly as to preclude collecting and sharing national security intelligence that has been gathered from appropriate intelligence requirements.[27] Nor should it be interpreted to preclude sharing material obtained through tasks from the RCMP or other law enforcement agencies given to CSIS in national security investigations. If CSIS are not permitted, or decline, to gather intelligence in this way, the only logical result can be is that the RCMP would, by necessity, have to create their own intelligence collection capabilities outside of CSIS. *De facto,* this appears to be the current approach where the RCMP endeavours to recruit informants in national security investigations with the specific aspiration of encouraging that informant to become an agent and therefore a witness creating two predators and one prey. Moreover if this is the process currently undertaken in is contrary to the rationale for the establishment of a civilian agency in the first place.

The current operationalisation of the 'partnership' agreement, creating two banks of sources and intelligence, is counterproductive. If it is to be construed that the current section 19 does not permit CSIS to facilitate RCMP intelligence needs, then the Act should be amended to permit CSIS to collect national security intelligence in this way. Intelligence is the fuel of the criminal investigative engine. Although the Federal Court[28] and other authors[29] have emphasised that

---

[26] Stanley A. Cohen, *Privacy, Crime and Terror. Legal Rights and Security in a Time of Peril.* (Ontario: Butterworths, 2005) at 407

[27] Discussion with Stanley Cohen July 29th, 2011 on this point.

[28] *Henrie v. Canada (Security Intelligence Review Committee),* [1989] 2F.C. 229.

[29] Stéphane Lefebvre, **"**Canada's Legal Framework for Intelligence" (2010) 23 International Journal of Intelligence and Counter Intelligence 247 at 254

intelligence collection was never intended to meet evidential standards, they completely miss a very important point. The intelligence is a golden thread that runs through proactive and reactive investigations. It provides direction and focus in the decision making process on how an investigation can progress and where evidential opportunities may be exploited. To meet investigative objectives, intelligence does not need to reach the evidential standard.

To maximise the value of intelligence and ensure that its flow is not obstructed, the CSIS concerns must be addressed. The adverse affects of the disclosure of national security intelligence are well articulated by both the courts[30] and academics.[31] Presumably the CSIS concerns over RCMP handling intelligence stems the potential disclosure triggered by its use in various operational activities. The concerns are likely to include the use of CSIS intelligence in the interview of suspects, the inclusion of material in affidavits for warrants of search or wiretaps or other overt activity that can alert terrorist suspects that they are targets and subject of intrusive interest.

The concerns can be resolved in two ways. First, criteria should be developed to determine whether intelligence product falls into that category of intelligence that should be disseminated and assess which agency is best placed to develop or exploit the intelligence. It is difficult to set down a closed set of criteria; however, factors could include any number of the following. (1) The threat to the safety of the public in the disclosure or non disclosure of the intelligence

---

[30] *Khadr v. Canada (Attorney General),* 2008 FC 549, 2008 CarswellNat 1462 at para 70; *Canada (Attorney-General) v. Khawaja*, 2007 FC 490, 219 C.C.C. (3d) 305, [2008] F.C.R. 547 at para 132; *Canada (Attorney-General) v. Kempo* 2004FC 1678,294 F.T.R.1; 2004 CarswellNat 6280 at para51

[31] Nathan Alexander Sales, "Secrecy and National Security Investigations" (2007) 58 Ala. L. Rev. 811 at 818; Mark A. Chinen, "Secrecy and Democratic Decisions" (2009) 27 Quinnipac 1 at 14-15; Stanley A. Cohen, "State Secrecy and Democratic Accountability" (2005-2006) 51 Crim L.Q. 27 at 30; Jo Moran, "Evaluating Special Branch and the Use of Informant Intelligence in Northern Ireland" (2010) 25 Intelligence and National Security 1at 10; *supra* n23 at p83

product[32]. (2) The risk of compromise to a human, technical or a third party source emanating through the control principle is always a concern[33]. (3) The effect of the disclosure on a current ongoing intelligence investigation. (4) Whether there is a current investigation in progress by a law enforcement agency that the intelligence may assist. (5) The opportunity for law enforcement to commence a proactive national security investigation as a result of the intelligence. (6) The impact of non-disclosure of the information on counter-terrorism strategies. (7) Whether the same intelligence or similar intelligence has already been disseminated. (8) The potential that the disseminated information will be disclosed in legal proceedings and the impact that will have. The Air India Report recommended that section 19(2) of the *CSIS Act* be amended to require disclosure of information for use in an investigation or prosecution. This would not be necessary if intelligence, and its product, were managed in line with the above principles.

The second way in which concerns may be managed, in a mutually satisfactory manner, is to settle upon conditions regarding the use of the intelligence once it has been disseminated. Caution must be exercised to ensure that caveats are not inappropriate, or, do not routinely place law enforcement in a position that they are unable to act. It may be that intelligence cannot be used in any investigative technique because it poses too great a risk to the source. If CSIS and the RCMP recognized the need to manage intelligence in creative, proactive, planned and lawful ways, they could effect a move toward a more symbiotic relationship.

---

[32] It is possible that the there could be such a threat and yet the CSIS would be able to manage that threat through their own operational deployments. Alternatively, if there is any question that the threat may not be managed, the information would have to be disseminated, and where that threat affected individuals, those individuals would have to be informed.

[33] Where there is a high likelihood that the source maybe exposed it may be possible to delay the dissemination of the intelligence and discover means to increase the circle of knowledge to reduce the threat of compromise.

In the alternative to disclosure to the police, it has been recommended that CSIS could have the option of submitting the intelligence to the national security advisor (NSA), or, some other more appropriate or agreed upon arbiter, to determine whether in the public interest intelligence should be disseminated.[34] The concern that arises from this suggestion is the introduction of a third party with the authority to influence or direct matters that are operational in nature. It is not a change in legislation that is required in this respect but a change in the culture of the organisations. Whether or not there is an arbiter in the form of the NSA does not solve the threat of disclosure from the criminal prosecution which was the CSIS second concern. To ease the concern there must be a three pronged approach. It is submitted that there needs to be (1) pragmatic changes, (2) procedural and substantive law amendment and (2) privilege and substantial law change. The suggested solution not only addresses the disclosure issue but also addresses the three RCMP concerns.[35] The NSA will be discussed further in a latter part of the paper.

A Pragmatic and Strategic Approach to National Security Investigation.

(i) The Case for Disruption

CSIS seems to have placed great weight on disruption tactics. Disruption has come about as unintended consequence on some occasions, or by design on others, for example letting suspects know that the service has an interest in them can result in the abandonment of terrorist operations. SIRC has questioned CSIS authority to use the tactic and asserted that it is normally a function of law enforcement.[36] SIRC's concern over disruption tactics by CSIS is unwarranted. Moreover CSIS ability to disrupt would be greater enhanced with the close cooperation and use

[34] *supra* n23 at p87 and 90.
[35] *supra* n23
[36] SRIC *Annual Report 09/10 A Time for Reflection* (Ottawa: Public Works and Government Services Canada, (2010) at 16-17

of RCMP resources. As Walker has stated "It is too dangerous to allow the terrorists to move towards their objectives if the results are mass casualties or the use of weapons of mass destruction." [37] Disruption, nonetheless, is a short term policy and can be a dangerous tactic. In Northern Ireland it was employed in various circumstances. First, as often is the case, in some instances, the intelligence picture is incomplete. It may have been interpreted that some activity was taking place but the exact nature of the activity or the destination of an explosive device being transported was unknown or unclear.[38] Second, it may have been necessary to disrupt an activity to assist an informant who may be getting entangled in the actual execution of operation. Third, it could have been that as a result of covert interference in weaponry or explosives, or for national security reasons the normal 'take down' could not occur because of disclosure difficulties that would follow. Alternatively, it simply may be necessary to stimulate certain activity. Nevertheless the danger with disruption is that once the disruption has taken place, and the immediate threat is diverted, there may be insufficient intelligence coverage to follow the actors to the next attempt. This can have catastrophic consequences.

The important point to be made in these disruption tactics, or other tactics in any national security operation, is that the security service can have enhanced capabilities by working on joint national security targets with law enforcement and vice versa. At the outset of any intelligence operation is the intelligence collection phase. It may have to be acknowledged that a criminal prosecution cannot take place because the source or particular methodologies employed cannot

[37]Clive Walker, "Intelligence and anti-terrorism legislation in the United Kingdom" (2005) 44 Crime, Law & Social Change 387at 388.

[38] On the limitations of intelligence **s**ee of Speech of Dame Eliza Manningham-Buller, The Director General Of The Security Service, "The International Terrorist Threat and the Dilemmas in Countering It" The Ridderzaal, Binnenhof, The Hague, Netherlands, 1 September 2005; Rt Hon The Lord Butler of Brockwell KG GCB CVO, *Review of Intelligence on Weapons of Mass Destruction. Report of a Committee of Privy Counsellors* (London: TSO, 2004) at paras 47-52 (UK); Intelligence and Security Committee,(ISC) *Could 7/7 Been Prevented. Review of the Intelligence on the London Terrorist Attacks on 7 July 2005* (London: Crown, 2009) Cmd 7617, at p 5 (UK)

be protected from disclosure. This does not dictate an end to the operation, but rather that it has to be approached from a different perspective, using different intelligence, or plans for the collection of evidence.

(ii) The Case for the National Security Investigation

The current approach to counter-terrorist investigations should change. There should be less preoccupation with respective mandates and more focus on the overall objective of national security. Protecting Canada and Canadians at home and abroad, ensuring Canada is not a base for threats to our allies, and contributing to international security are the core objectives of the current national security policy.[39] Joint proactive investigations, in appropriate circumstances, between CSIS and RCMP are the most effective and efficient way to achieve these objectives. There is no suggestion of a merger between intelligence and criminal investigation teams. Rather, at senior officer levels, both strategic and tactical decisions are taken to advance investigations. Parallel investigations using de-confliction processes to ensure that one organisation does not trample over the other only serve to inculcate the competition between the organisations who will fish in the same pond.[40] In a nutshell CSIS collect information on terrorist suspects and activities. Their investigations use all manners of human intelligence and technical capabilities. Although not collecting the intelligence for law enforcement, they may exercise their discretion to pass on intelligence that RCMP may use as leads in their investigations or, to initiate an investigation.[41] On the other hand, and, at the same time, the RCMP has their own

---

[39] Canada. Privy Council Office, "Securing an Open Society: Canada's National Security Policy" (Her Majesty the Queen in Right of Canada, 2004) at p5-6 available online at http://www.pco-bcp.gc.ca/docs/information/publications/natsec-secnat/natsec-secnat-eng.pdf

[40] see *supra* n13 p 195 re CSIS efforts to solve terrorist crime.

[41] see comments of Jim Judd, Director of CSIS at the Global Futures Forum Conference in Vancouver on 15th April 2008 re CSIS use of intelligence in criminal prosecutions. available online at http://www.csis-scrs.gc.ca/nwsrm/spchs/spch15042008-eng.asp

independent investigations in which they will recruit informants, with a view to employing them as agents. They will also use physical and technical surveillance in efforts to collect evidence. CSIS will get access to the RCMP product. Nonetheless, at the risk of repetition, this model has made it necessary for the RCMP to employ an intelligence capability that encroaches into the mandate given to CSIS and under the guise of evidence collection. It runs the risk of two organisations pursuing their different mandates in a proliferation of antagonistic operational behaviours.

Counter-terrorism has both law enforcement and intelligence equities.[42] Proactive investigation in this field must have both intelligence collection capability and evidential harvesting expertise working under the cover of one strategic approach and one investigation. Two investigatory teams or organisations with two different functions and one common objective! From the strategic perspective the one common objective must begin with the strategic assessment that identifies and maps the threats caused to Canada by various groups and individuals. Target selection follows and policy decisions must be taken around the most effective strategies to employ to disrupt, disable or dismantle the groups or organisations that present the threat. Intelligence agencies, when entering into a specific joint investigation, should have knowledge of and training around the investigative standards required and the extent of the record keeping demanded in a criminal investigation.[43] Investigative methods may be selected with a view to the court room, and so, the agency will remain in a better position to protect other sources and methods that would not be in the public interest to disclose.[44]

---

[42] Todd Masse, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States. Report for Congress* (U.S.: Congressional Research Service, 19 May 2003) at 11

[43] *supra* n16 at para 39

[44] Stewart A. Baker "Should Spies Be Cops" (Winter 1994-95) 97 Foreign Policy 36 at p49

In the review of the intelligence on the London terrorist attacks on 7th July 2005 the Intelligence Committee noted, with approval, the use of Executive Liaison Groups (ELG's). In this group MI-5 and the police worked the investigation together. Intelligence was shared, including raw product, and decisions were made on how evidence could be gathered to bring about the successful prosecution of suspects in court. The Group recognised the primacy of the security service in the intelligence collection phase, and, the group as a whole made the decision when it was appropriate for primacy to pass to the police to progress to the prosecution phase. [45] Operation Crevice had an ELG and Canadian case of *Khawaja* was part of that operation.[46] This format with key stakeholders around a table, making strategic decisions on what targets should be pursued, decisions around the different phases of the investigation, who has primacy and to what standard of collection of information, provides an effective and efficient platform. This platform also allows for an exchange of information and advice with the expertise from both dimensions of national security investigations. It aids in the identification of early disclosure problems and the development of a plan that enables those involved in the investigations to keep one 'eye' and one 'ear' on emergent disclosure impediments. The early identification of potential disclosure impediments to prosecution can be critically analysed and the likely result of an application under section 38 *Canada Evidence Act* [47]assessed. Manget would argue that intelligence collectors cannot conduct their activities with one eye looking over their shoulder at the potential of some future prosecution of individuals.[48] There is no suggestion that the process is an easy one. Nonetheless it has been quite evident that the view of many intelligence operatives and some police officers is that the vast majority of intelligence deserves automatic

[45] Intelligence and Security Committee, *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005* . Cm7617 (England: Crown, 2009) at 8-9 (UK)
[46] *ibid*
[47] R.S.C. 1985, c. C-5
[48]Fred F. Manget "Intelligence and the Criminal Law System" (2006) 17 Stan. L. & Pol'y Rev. 415 at 425

protection and should not be revealed to the court. That view has to change and the strategic platform suggested can be of value. Changes to procedural and substantive law can also assist the disclosure process without affecting the accused and his right to a fair trial.

Change to Procedure and Substantive Law.

Disclosure obligations in the context of the criminal trial are set out in the common law. A major concern of CSIS in becoming part of a joint or entwined investigation is the likelihood that CSIS would be subject to *Stinchcombe*.[49] In *Ahmad,* Dawson J concluded that CSIS was not subject to *Stinchcombe* under the Supreme Court's decision in *McNeil* but were to be regarded as a third party for the purposes of disclosure.[50] However, the judge based his decision on the fact that CSIS had conducted a parallel investigation. Had that not been the case he would have concluded that CSIS had a corollary duty to disclose.[51]

Stinchcombe sets the low threshold of discovery to include both exculpatory information and inculpatory information[52], unless information in possession of the prosecution is clearly irrelevant or privileged[53]. Relevance is decided on the basis of the charges preferred and on reasonable possible defences open to the accused.[54] In *Egger* "one measure of the relevance of information in the Crown's hands is its usefulness to the defence: if it is of some use, it is relevant and should be disclosed". [55] In *Chaplin* the judge defined relevance as "there being a

[49] see *R.v. Malik,* [2002] B.C.J. No 3219 (S.C.) at para 8-10
[50] *R. v. McNeil,* [2009] 1 S.C.R. 66 at para 14
[51] *supra* n15
[52] *supra* n22 at para 29
[53] *ibid* at para 20
[54] *R. v. Taillefer; R. v. Duguay* [2003] 3 S.C.R. 307 at para 59
[55] *R.v. Egger,* [1993] 2 S.C.R. 451 at para 20

reasonable possibility of being useful to the accused making a full answer and defence."[56] Finally, of some assistance are the comments of Cory J. in *Dixon*. In the court's consideration of disclosure in an appeal, the test for relevancy is that the accused must show that the undisclosed information could have been used in meeting the case for the Crown, advancing a defence or otherwise making a decision which could have affected the conduct of the defence...."[57]

The Air India report considered the threshold of disclosure and recommended that no change be made to it. They did form the view that the *Stinchcombe* threshold of 'clearly irrelevant' should not be the standard test for prosecutors to assess the relevance of material for the purpose of disclosure. Instead, they urged that only relevant material be produced and that the remainder of the material, not clearly irrelevant, be made available for defence inspection at a secure location. The Commission dismissed, without any real analysis, the idea of legislating for a threshold that required only exculpatory information and that which would undermine the case of the prosecution.[58] In the United Kingdom case of *R.v.H and C* the House of Lords has declared that :

> If material does not weaken the prosecution case or strengthen that of the defendant, there is no requirement to disclose it. For this purpose the parties' respective cases should not be restrictively analysed. But they must be carefully analysed, to ascertain the specific facts the prosecution seek to establish and the specific grounds on which the charges are resisted. The trial process is not well served if the defence are permitted to make general and unspecified allegations and then seek far-reaching disclosure in the hope that material may turn up to make them good. Neutral material or material damaging to the defendant need not be disclosed and should not be brought to the attention of the court. Only in truly borderline cases should the prosecution seek a judicial ruling on the disclosability of material in its hands. [59]

---

[56] *R.v. Chaplin*, [1995] S.C.R. 727 at para 30
[57] *R v. Dixon*, [1998] 1 S.C.R. 80 at para 22-23.
[58] *supra* n23 at p121 -123
[59] *R .v.H and C*, [2004] UKHL 3 at 35 (UK)

Legislation has been recently enacted in Scotland. The prosecutor there has a duty to review all the information that may be relevant to the case for or against the accused of which the prosecutor is aware and disclose the information to the accused if:

> (a) the information would materially weaken or undermine the evidence that is likely to be led by the prosecutor in the proceedings against the accused,
> (b) the information would materially strengthen the accused's case, or
> (c) the information is likely to form part of the evidence to be led by the prosecutor in the proceedings against the accused.[60]

The term materiality has not been defined under the Act. It was a term used at common law prior the codification of disclosure. Critics, before and after the legislation, voiced concern that the term is vague and "inherently malleable" with the potential for a subjective as opposed to an objective assessment of the material.[61]

Moreover, the Australian[62] and New Zealand[63] approach to relevancy is much less liberal than Canadian system. Contrary to the recommendation of the Air India Inquiry it is submitted that a new test of relevance should be legislated. The intelligence community would see a substantial reduction in the amount of disclosure required of them either under a first party disclosure package of *Stinchcombe* or the corollary duty of 'other investigating state authority of *McNeil*.[64]

Changes to Privilege in Substantive Law

I. A New National Security Privilege

The Air India Inquiry recommended that the NSA would have an enhanced role to decide whether or not CSIS intelligence would be disseminated to investigators or prosecutors. A class

---

[60] *Criminal Justice and Licensing (Scotland) Act 2010* asp 13
[61] Findlay Stark "Legislating the Duty of Disclosure" (2009) 13 Edinburgh L. Rev. 493 at 494.
[62] *R v Mallard*, [2005] HCA 68 (Australia)
[63] *The Criminal Disclosure Act* 2008 No 38, Section 8 (New Zealand)
[64] *supra* n50 at para 14

privilege would cover the deliberations of the NSA where CSIS would seek to withhold intelligence from further distribution to those outside the organisation. A deliberation on whether any circulation of the product would take place would require the NSA to apply a public interest test. The class privilege was required to protect the deliberation process and seems to be based on the need to promote candour in discussions, the fact that all material would relate to national security, that the material submitted to the NSA was that which CSIS do not want disseminated any further because of issues such as ongoing national security investigations or the fact that in evaluating the activities of national security activities weaknesses and gaps in the system might be revealed.[65]

There is a strong case against creating of a new class privilege. Justice Binder in *Trang #2* noted the common law tendency to reject the creation of any new class privileges.[66] The Supreme Court has rejected the notion of creating a class privilege at common law, and, was sceptical of any legislative enactment. [67] The justifications given in support of the national security privilege are also weak. The candour argument was rejected in *Carey v. Ontario*[68]. The particular case involved cabinet documents. The court examined the English jurisprudence and rejected the inference that candour would be affected by the lack of confidentiality provided by the loss of the class privilege.[69] The suggestion that the NSA would only consider national security material that may be subject of a non dissemination decision by the NSA does not support a class privilege approach. Once the material has been submitted to the NSA and deliberations have taken place, the result will be either (a) dissemination, in which case the NSA deliberation is

[65] *supra* n23 at p142
[66] *R. v. Trang*, 2002 ABQB 19, 168 C.C.C. (3d) 145, 2002 CarswellAlta 153 at para 46 (S.C.)
[67] *R. v. National Post*, 2010 CarswellOnt 2776; 2010 SCC 16, at para 42
[68] [1986] 2 S.C.R. 637
[69] *ibid* at para 44-50

irrelevant, (b) a further review to be carried out at a later time i.e. a delay in further dissemination or (c) a direction that the material will not be disseminated. In the case of either (b) or (c) no disclosure obligation arises unless a parallel investigation by RCMP or other agency is taking place and an O'Connor application is anticipated. If disclosure obligations arise in this way, then section 38 is the appropriate mechanism for a prohibition order on disclosure where the judiciary are well practiced in balancing the competing public interests.

In respect of the last justification it is difficult to imagine how these oversight duties would impact on disclosure obligations unless the NSA was involved in some operational role. In addition since the NSA does not currently have an operational role there is a question of both his suitability to carry out the role and the operational capacity of the office of the NSA in its current form. The rationale that the establishment of a new class privilege is necessary to protect the disclosure of gaps or weaknesses in the national security framework is hard to justify. It is unlikely that any weaknesses or gaps identified would be disclosed. In considering step 3 of *Ribic*[70] it is extremely improbable that the balancing process would result in a finding that the public interest in disclosure outweighed the public interest in non disclosure.

II. Other Options for Changes in Substantive Law

It has been suggested that another class privilege could be created to protect national security information. The privilege would apply to CSIS information, or to an aspect of CSIS material such as third party material claimed under the third party rule, or, to some aspect of material

[70] *Ribic v. Canada (Attorney General),* 2003 FCA 246, 185 C.C.C. (3d) 129, [2005] 1 F.C.R., 2003 CarswellNat 4708 at para 29

shared by CSIS with the RCMP.[71] This statute based privilege would need to be *Charter* compliant and would almost certainly face a constitutional challenge at the first opportunity. Considering how privilege has evolved in Canada and elsewhere over the past three decades it is unlikely that there would be much support either publicly or politically for the new privilege. Furthermore, it would be unlikely that this privilege would assist in the resolution of the prosecution's disclose or dismiss dilemma. The absolute character of a class privilege of this kind could leave the court, before which an accused appears, ignorant of the fact relevant material exists, or, it could subject such material to the exactitude of the innocence at stake test. The result is going to be the same. The court is likely to give broad interpretation to the test and present the Crown with the usual choice to proceed with disclosure or halt the prosecution. The class privilege creates a pragmatic solution that lacks a strategic focus. The focus should be on reducing the risk created to national security while preserving the rights of the accused to a fair trial.

It is submitted that a change to the process in section 38 of the *Canada Evidence Act*[72] is appropriate in balancing the competing demands of the right to know versus the need to keep secret. Hamish Stewart has raised concerns that the section 38 process forces the accused to reveal the defence strategy to the Attorney-General in compliance with requirements under section 38.01.[73] There is no demand to reveal the defence strategy within the legislation. However a modest mandatory defence disclosure in the context of the section 38 process would assist the designated judge to reach a more measured and balanced decision on disclosure. Moreover defence disclosure ensures that the Crown are in a better position to establish the

[71] Kent Roach, " The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence" in *supra* n4 at Vol. 3 Research Studies. Terrorist Prosecutions. 346 at 347
[72] R.S.C. 1985, c. C-5
[73] Hamish Stewart, "Public Interest Immunity after Bill C-36" 47 Crim. L. Q 249 at 260.

relevance of information which serves the objective of full disclosure. The Supreme Court in *Stinchcombe* has not ruled out the possibility of reciprocal defence disclosure in general.[74] Calls in Canada for mandatory defence disclosure[75] have been aggressively rejected.[76] However there are various exceptions already in existence. Alibi evidence,[77] special defences, [78] expert evidence[79] *Charter* applications, [80] the adducement of a complainant's sexual history [81] and the use of form 17 in Ontario[82] are all examples of some form of defence disclosure.

In *Ribic*[83] and *Khawaja*[84] the Federal Court has suggested a necessity of defence disclosure in the section 38 process in order to ensure a meaningful review of the material sought by the defence. Various mechanisms are available to the accused within the current process that include *ex parte* hearings under s38.11(2) and, or, conditions attached to the disclosure that the details revealed by the defence cannot be revealed to the prosecution counsel.[85] In the extradition case of *Khadr* benefit was found in having counsel for the respondent present during what would normally be *ex parte* hearings by the applicant. Their presence was permitted on the understanding that the information revealed would not be communicated to the state requesting extradition. Subsequent

---

[74] *supra* n22 at para 11-12
[75] Goran Tomljanovic "Defence Disclosure: Is the Right to "Full Answer" the Right to Ambush" (2002-2003) 40 Alta. L. Rev. 689 at 693; David Tanovich; Lawrence Crocker "Dancing with Stinchcombe's Ghost: A Modest Proposal for Reciprocal Defence Disclosure" (1994) 26 C.R. (4th) 333
[76] Michael Tochor, Keith Kilbrack "Defence Disclosure: Is it written in Stone?" (2000) 43 Crim. L.Q. 393; C.B. Davidson, "Putting Ghosts to Rest: A Reply to the 'Modest Proposal' for Defence Disclosure of Tanovich and Crocker" (1995), 43 C.R. (4th) 105; Don Stuart *Charter Justice in Canadian Law* Fifth Edition (Ontario:Carswell 2010) at 188
[77] *R. v. Cleghorn*, [1995] 3 S.C.R. 175 at para 3-4;
[78] *R.v. Stone*, [1999] 2 S.C.R. 290 at para 98 and 99
[79] *Criminal Code*, R.S.C. 1985, c. C-46, s 657.3(3)(a) and (c)
[80] *R.v. Dwernychuck* , [1992] A.J. No. 1058 (Alta.C.A.), *R. v. Wiebe*, [2007] A.J. No. 135 (Alta. Prov Ct.)
[81] *supra* n79 *at* s276.1
[82] Form 17 available at http://www.ontariocourts.on.ca/scj/en/about/forms/Form17.pdf
[83] *supra* n70 at para 29
[84] *Canada (Attorney General) v. Khawaja* , 2007 FCA 342, 228 C.C.C.(3d) 1, 2007 CarswellNat 3603 at para 35
[85] *supra* n70 para 30

discussions in *ex parte* hearings on relevance with the aid of amicus curiae were more candid and measured.[86]

The premature release of intelligence gathered in national security investigations can affect the safety of Canadians and have a devastating effect of current or future operations.[87] Mandatory defence disclosure should be employed in the balancing test at both step 1 and 3 of *Ribic* test. This would ensure that there would be no fishing expeditions or attempts to force the prosecution into an unwarranted disclose or withdraw dilemma. From the defence perspective the production of a detailed defence statement that ties the material they seek into the charges or claim forces the government to disclose only relevant material or forces the state to withdraw the charges.[88]

III. Privilege for National Security Sources

The Air India report has considered, in detail, the current ambiguity that lies between the difference in police informer privilege and case by case privilege applicable to sources handled by the Intelligence agency. There should be no difference made between a person who supplies information to law enforcement and those provided to the CSIS. This recommendation is contrary to the conclusions reached by Simon Noel, J in *Re Harkat*,[89] the recent case in the Federal Court of Appeal [90]and the conclusions drawn by the Air India Commission.[91]

---

[86] *Khadr v. Canada(Attorney Genera)l,* 2008 FC 549 at 22
[87] Stanley A. Cohen, "State Secrecy and Democratic Accountability" (2005-2006) 51 Crim L. Q 27 at 30, Nathan Alexander Sales, "Secrecy and National Security Investigations" (2007) 58 Ala. L. Rev. 811 at 818
[88] Saul M. Pilchen and Benjamin B. Klubes, "Using the Classified Information Procedures Act in Criminal Cases: A Primer for Defense Counsel" (1993-1994)31 Am. Crim. L. Rev. 191 at 208
[89] *Harkat (Re),* 2009 FC 204, [2009] 4 F.C.R. 370
[90] *Attorney General of Canada v. Almalki, Kalifah and Almalki,* [2011] FCA 199 at para 34
[91] *supra* n 4 at Vol. 3. The Relationship Between Evidence and Intelligence and the Challenge of Terrorism Prosecutions at p 133-139

In *Harkat* the reasons given for the distinction in the protection given between the intelligence sources and police informants was simply based on the fact that the sources were recruited by a civilian agency. If the mandate for national security still remained with the RCMP as it did prior to 1984 police informant privilege would have applied. The confidential sources who perform the functions 'on the ground' are performing the same roles in the context of national security whether they are handled by the police service or by the intelligence service. Drawing again from the experience in Northern Ireland, until October 2006 the primacy for national security intelligence in the province was with the police service. MI-5 did have an involvement, they handled a much smaller number of sources and on some occasions there was a joint handling relationship between MI5 and the police service. When primacy passed to MI5 in October 2006 responsibility for the sources already part of the stable also passed to the security service. In handling many, if not most of the sources, the police handlers continued to work alongside MI5 as handlers.[92] The moral of the story is that the sources, whether recruited by police or the security service, perform the same role. 'Police' in police informant privilege requires to be interpreted broadly.

Simon Noel J. did protect the confidentiality for the source under the Wigmore principles which extends a common law case by case privilege if the following four conditions are meet the common law privilege is extended or recognized:

(1) The communications must originate in a confidence that they will not be disclosed.
(2) This element of confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties.

[92] The author was a member of the Police Service of Northern Ireland, formerly the Royal Ulster Constabulary and was involved discussions in preparation for the transfer of primacy to the Security Service.

(3) The relation must be one which in the opinion of the community ought to be sedulously fostered.
(4) The injury that would inure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of the litigation.[93]

A Response to Air India on Informant Privilege

The Air India Inquiry highlighted several reasons that militated against the value of police informer police to CSIS Sources.[94] Comments have been added below each of the arguments given.

1. *Parliament made a decision not to give CSIS law enforcement powers. The informer privilege, at least in Canada, has traditionally been reserved for police informers;*

Police powers are not required in order acknowledge the policy behind the privilege. The same policy reasons behind informer privilege apply equally to CSIS sources.

2. *CSIS deals with informers under its mandate to investigate threats to the security of Canada. It will often be premature at the time of such investigations to make promises that effectively give informers a veto over whether they can be called as witnesses or whether any identifying information about them is disclosed in a subsequent terrorism prosecution;*

It is difficult to reconcile how in the criminal context that a person may need to be given the assurance of confidentiality in order to secure information about a burglary, when a potential CSIS source who has access to suspect terrorists, a building where suspect terrorists live or attend, or, has observed some suspicious activity that could develop into a national security interest does not qualify for the same assurance given to the informant in respect of a burglary. The fact that the potential source is talking to a covert agency, would lead to an expectation by the source that his identity and fact of cooperation would remain secret. In dealing with terrorism prosecutions in Northern Ireland it was not infrequent that where the identity of a national security source had to be disclosed or material would have to be disclosed that may lead to the identity of the source, the prosecution had to be withdrawn.

3. The identities of CSIS sources can already be protected through applications for public interest immunity and national security confidentiality under sections 37 and 38 of the Canada Evidence Act or through the recognition of a case-by-case privilege. Extending informer

---

[93] John Henry Wigmore, *McNaughton Revision, Vol.8*, (Boston: Little, Brown & Co., 1961,) at 527 quoted in *Harkat (Re)*, 2009 FC 204, [2009] 4 F.C.R. 370 at para 20

[94] *supra* n4 at Vol. 3. The Relationship Between Evidence and Intelligence and the Challenge of Terrorism Prosecutions at p 133-139

privilege to CSIS informers is not necessary because section 18 of the CSIS Act makes it an offence .....to disclose information about a confidential source of information or assistance to CSIS.

The sub-comment from the Commission recognised that the protection offered is a weak privilege than that compared with police informer privilege. The risk taken by those involved in National Security investigations should receive the recognition it deserves.

4. Extending police informer privilege to CSIS sources might lead to judges weakening the protections of informer privilege by gradually allowing the privilege to be defeated by exceptions in addition to the existing innocence-at-stake exception.

Informant privilege is well established in Canadian Jurisprudence and has witnessed a consistent approach from the Supreme Court of Canada and the lower courts. Parliament has always to option to codify the common law to ensure that the policy behind it is not diminished.

To some extent the Inquiry is sitting on the fence. The recommendation in the report was against codifying a police informant privilege for CSIS sources although the door was left open for the potential that the judge made law may result in the applicability of informant privilege to CSIS sources. However the Federal Court of Appeal has stated that the court is ill equipped to extend the privilege to CSIS and would usurp the function of Parliament were it to do so.[95] It is not a huge leap to ratify informant privilege to this extent. The added benefit to the treatment of CSIS sources in this way ensures that on any occasion there is a handover of the source from one organisation to another, as arose in the case of *Malik and Bagri,*[96] there are no issues as to what policy should apply or at what stage does one policy stop and the other start. So long as the conditions of the privilege are met both organisations and the source will have some certainty.

Conclusions

[95] *supra* n90 at para 30
[96] *R. v. Malik and Bagri*, 2004 BCSC 554, 119 C.R.R. (2d) 39

The relationship between the RCMP and CSIS must be a symbiotic one if there is to be successful outcomes in national security investigations. Each organisation brings to an investigation a different skill base, different resources and a different operational capacity. In order to address the concerns of both organisations some changes can be made. The suggested changes involve pragmatic, procedural and substantive law changes. The changes suggested do not interfere with the accused right to a full answer and defence, or, if it does the limitations suggested are reasonable given the threat to the safety of Canadians and their allies.