National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

The Intelligence-to-Evidence Problem in Canada: Time for Government Action

Ms Nicole Harrack

JCSP 49

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 49

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Exercise Solo Flight – Exercice Solo Flight

The Intelligence-to-Evidence Problem in Canada: Time for Government Action

Ms Nicole Harrack

The I2E Problem in Canada – Time for Government Action

The intelligence-to-evidence (I2E) problem is when "dilemma[s] arise from the challenges and obstacles encountered when actionable intelligence is used to inform criminal investigations and eventual prosecutions, or other government action to address national security threats." [1] The challenge is how to protect intelligence from being disclosed publicly.

In order to improve the I2E problem in Canada, the Canadian government needs to: amend existing legislation so as to give a solid foundation upon which the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) can share information (principally outline a disclosure regime specific to national security), and create a Cabinet-level coordinating body for national security matters.

Decades of commissions, inquiries and 'lessons learned' have made a variety of recommendations as to how Canada can 'solve' its I2E problem. Much of the criticism has focused on the relationship between the RCMP and CSIS, but there have been consistent calls for both legislative changes and "a sophisticated dialogue on national security issues - one framed in a Canadian context."[2] Despite the repetitive nature of the recommendations, Canada's I2E problem remains, and while "the initial years of organizational friction between CSIS and the RCMP have long given way to a genuinely productive partnership. . . ,"[3] it is now time for parliamentarians to act.

THE ROAD LEADING TO CANADA'S I2E PROBLEM IS A LONG ONE

The RCMP as it is known today was officially created by an act of Parliament in 1920, however the RCMP itself cites its origins from the North-West Mounted Police that was created in 1873.[4] The RCMP was originally home to Canada's security service, but after the 1970 front de Liberation du Quebec (FLQ) crisis, the McDonald Commission was created to investigate claims that the RCMP had abused its authority. Its findings were damning of RCMP activity during this time and called for the creation of a civilian intelligence agency; hence the creation of CSIS in July 1984.

---

[1] Public Safety Canada, "Remarks by Director David Vigneault to the Centre for International Governance Innovation," Public Safety Canada, August 20, 2021, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-en.aspx.

[2] Ibid.

[3] Murray, Dave, and Derek Huzulak. "Improving the Intelligence to Evidence (I2E) Model in Canada." *Manitoba Law Journal* 44, no. 1 (2021): 188. https://tinyurl.com/5n8bpckz.

[4] "Royal Canadian Mounted Police," RCMP.ca (/ Gendarmerie royale du Canada, March 26, 2023), https://www.rcmp-grc.gc.ca/corporate-organisation/history-histoire/rcmp-origin-story-histoire-origine-grc-eng.htm.

The McDonald Commission

The Commission saw the need to separate powers traditionally held by intelligence services from those of law enforcement so as to avoid a situation wherein a new agency would be both 'judge and executor'. It was foreseen that CSIS would have a core mandate to collect, analyze and advise government, while threat mitigation and enforcement powers would remain with police of jurisdictions (PoJs). In its advisory role, the Commission presumed CSIS would share information with other government departments who had some type of enforcement mandate (e.g. RCMP)[5]. In fact, the Commission envisioned CSIS and the RCMP conducting joint operations with one another along with a well-developed liaison program so officers of each agency would be imbedded in the other in an effort to "facilitate and control the exchange of information."[6] This was seen as being necessary so as to avoid a duplication of efforts.

Air India Inquiry

In 1985, Canada suffered the worst terrorist attack in its history with the bombing of an Air India flight that resulted in the deaths of more than 320 people. Another inquiry was called and it determined that cooperation between CSIS and RCMP was lacking and the ability of the police to use CSIS collected intelligence as evidence in a criminal proceeding was difficult. The proceeding years saw an increase of liaison officers posted between the two agencies, RCMP officers were given complete access to CSIS holdings, including all of CSIS' terrorist information,[7] but problems remained. As the Air India inquiry noted, CSIS and the RCMP were in the habit of managing their information sharing in a way that served the best interest of each agency, and not that of the greater Canadian good. It furthered that CSIS' efforts to minimize the amount of its information being shared with the RCMP as 'misguided' that would only result in an "impoverished response to terrorist threats."[8]

Canada's Adoption of its Constitution and the Charter

In 1982, the Canadian government passed the *Constitution Act* which ushered in new fundamental rights for all Canadians. As time progressed and legal battles were fought, Supreme Court legal opinions entered into the I2E dialogue, namely *R v. Stinchcombe* (1994), *R v. O'Connor* (1995) and *R v. McNeil* (2009). Each of these three decisions have interpreted what disclosure obligations the Crown has in a criminal proceeding, and what information can be considered 'fruits of an investigation'. These decisions and their interpretations by lawyers have served to further chill relations between CSIS and the RCMP and inhibit the amount of information sharing.

---

[5] Murray, Dave, and Derek Huzulak. "*Improving the Intelligence to Evidence …*", 184.
[6] *Ibid.,* 184.
[7] *Ibid.,* 185.
[8] *Ibid.,* 185.

Landmark Legal Cases

R v. Stinchcombe stated that "the Crown has a legal duty to disclose all relevant information to the defence."[9] It highlighted that an accused's ability 'to make full answer and defence' is a fundamental principle of justice; a right protected by Section 7 of the Charter. It furthered that "the fruits of the investigation which are in its possession are not the property of the Crown for use in securing a conviction but the property of the public to be used to ensure that justice is done."[10] It is important to note that for the purposes of criminal investigations, the Crown refers only to the prosecuting Crown, not other Crown entities such as the police. "Information in the possession of third parties such as boards, social agencies, government departments . . . or foreign law enforcement agencies is not in the possession of the Crown."[11] This court case added no real change to existing understanding of Crown disclosure (i.e. the Crown had always known it should disclose relevant information to the accused so one may mount a full answer and defence), however, it cast doubt on what information could be deemed as relevant. The issue this raised: without a crystal ball, the Crown may not be aware how one piece of information may prove to be relevant at some point in the criminal proceeding. This is why the ruling erred on the side of caution and urged *full* disclosure of information to the defence at the *outset.*

R v O'Connor broadened the type of information that could be subject to disclosure from that of *Stinchcombe*. This case set the precedent that in some cases, records held by third parties are, in fact, relevant and should be disclosed. The Court acknowledged the sensitivity of some records and, in an effort to address this, "set out a strict two-stage procedure for determining when medical records can be disclosed and established guidelines for the application process." This meant that defendants seeking to gain access to files previously considered third party must now "demonstrate that the records they seek are likely to contain information relevant to an issue at trial and that without them, their ability to make full answer and defence would be adversely affected."[12] This was done to avoid a 'fishing expedition' of sorts by defence counsel. What resulted was the process wherein the "trial judge must balance the privacy interests of complainants and third parties with the accused's right to a fair trial."[13]

R v McNeil broadened disclosure once again when it ruled that the disclosure obligation extends to other state authorities. This ruling acknowledged that the Crown prosecutor and police have 'separate and distinct roles' but found that the "police also have a duty to participate in the disclosure process, since it is the obligation of the police to disclose all material related to its investigation of the accused to the Crown."[14] This

---

[9] Peter Bowal, "Stinchcombe: Crown Disclosure of Criminal Evidence," LawNow Magazine (Centre for Public Legal Education Alberta, February 26, 2021),.https://www.lawnow.org/stinchcombe-and-crown-disclosure-of-criminal-evidence-2/

[10] *Ibid.*

[11] *Ibid.*

[12] "R v O'Connor [1995]," West Coast LEAF, November 25, 2014, https://www.westcoastleaf.org/our-work/r-v-oconnor-1995/

[13] *Ibid*.

[14] Jakki Warkentin, "R v McNeil: The Duty to Disclose Police Misconduct Records," canliiconnects.org, March 5, 2015,https://canliiconnects.org/en/commentaries/36168

had the effect of placing police as first party, not third party. *R v McNeil* continued to uphold the general belief that an accused's

> ". . . interest in obtaining information in order to make full answer and defence will outweigh the residual privacy interests of third parties; however, these privacy interests should still be considered. In order to ensure that only relevant interest is produced so that there is no unwarranted invasion on privacy, the court must make orders that are specifically designed to meet the circumstances of the case, possibly making the order subject to conditions or restrictions to the circulation of this information."[15]

These three decisions are generally regarded as enhancing transparency by permitting an increased flow of information whilst simultaneously considering and protecting privacy interests. In an open, free and democratic society, these are arguably all welcome changes. Where it gets complicated is that all of the above-cited cases were decided on purely criminal grounds with no national security nexus. Privacy rights of an individual may not require the same level of protection as those on a national security level. The classification of information, access to the information and the viewing, use and storage of said information all require significant effort and its public disclosure could potentially damage Canada's ability to conduct affairs of state thereby out-weighing the rights of the individual accused.

Privilege – An Important Legal Concept

Invoking privilege is one option that the government has to prevent sensitive information from being disclosed, but even this offers no guarantee. The *Canada Evidence Act* s.38 "sets out a regime for preventing the disclosure of information or documents that contain sensitive or potentially injurious information."[16] Both sensitive and injurious information relate to government held information that the government is required to safeguard to maintain its relations with other states, in matters concerning national defence or national security. In order to determine if the government's privilege is reasonable, a federal court judge must decide if the information "is relevant. . . . would the release of the information be injurious to national security, national defence or international relations? . . . . [and] the judge must find that the public interest in disclosing the information is outweighed by the public interest in protecting it."[17] Based on the above, it is near impossible for CSIS to have any certainty in determining if the information it shares with law enforcement will land in court and become public.

While all of the above cases expanded the definition of disclosure, they did nothing to set boundaries or principles for a criminal proceeding to consider vis-à-vis national security. A lack of national security best practices and rationale means that when a criminal proceeding for a national security threat, such as terrorism, makes it way to

---

[15] *Ibid.*

[16] Leah West, "The Problem of 'Relevance': Intelligence to Evidence Lessons from UK Terrorism Prosecutors," *Manitoba Law Journal* 41, no. 4 (January 1, 2018): p.77. https://tinyurl.com/mr2kpxra.

[17] *Ibid.*, 77-78.

court, the Crown has only case law such as the cases cited above on which to inform its disclosure requirements and that of police. There is no set of guiding principles as to where CSIS information may fit and under what circumstances its information can be seen, held and protected. To sum up in another way:

> "The application of the Canadian disclosure regime to terrorism prosecutions results in unending litigation about the provision and protection of information. This litigation is not only inefficient, it creates uncertainty for CSIS who is unable to predict whether their information will be subject to Stinchcombe disclosure, sought in an O'Connor application for third party information, or released by the Federal Court following a s.38 application. For an organization whose mandate cannot be met without collecting secrets, working covertly, and protecting the anonymity of its sources and employees this uncertainty is a nightmare."[18]

Bifurcation: Uniquely Canadian

An additional headache to address is the fact that Canada's current legal process vis-à-vis terrorism, mandates that it is the purview of a *federal* court judge, *not* the presiding trial court judge who is to determine if information can be protected on national security grounds (i.e. Section 38 protection under the *Canada Evidence Act*). This is referred to as bifurcation and Canada is the only Five Eye (FVEY) nation with this system[19]. This means that the presiding judge *does not* see the information that will not be disclosed to the defence so is unable to definitively say whether or not the trial has been conducted fairly. When the trial judge is in doubt, there is a greater chance for the case to be suspended which is problematic for two reasons: one, an accused terrorist can go free which poses security repercussions, and two, the accused, while freed, may still face negative repercussions to their livelihood / reputation, etc. because they have been accused, but not ruled innocent.

INTELLIGENCE VS EVIDENCE: HOW DID THE LINE GET BLURRED?

Richard Fadden, a former CSIS Director has made several public appearances and given statements to various media outlets explaining the differences between intelligence and evidence and by extension, the mandates of the agencies involved in national security investigations. As he noted, ". . . . CSIS, police and the legal system have different mandates."[20] In an effort to protect Canadian citizens from their state, the police have their own professional standards - evidentiary standards they must meet so as to protect Canadians from "overly easy investigations by the police."[21] Intelligence agencies, on the

---

[18] *Ibid*.,78.

[19] "Protecting Canadians and Their Rights: A New Road Map for Canada's National Security," ourcommons.ca (Library of Parliament, May 2017), p.31 https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP8874869/securp09/securp09-e.pdf.

[20] Catharine Tunney and Peter Zimonjic, "'Intelligence Is Not Truth': Why Prosecuting Foreign Election Interference Is Rare ," CBC.ca (CBC/Radio Canada, March 2, 2023), https://www.cbc.ca/news/politics/fadden-vigneault-intelligence-bar-evidence-1.6765673

[21] *Ibid.*

other hand, differ and the differences are not specific to just CSIS, but rather intelligence services in general. Intelligence services "collect a lot of intelligence and a lot of it is not used because it doesn't reach the bar of being convincing enough from the perspective of those professional standards."[22]

Bruce Berkowitz, a former CIA employee and research fellow at the Hoover Institution, wrote about the differences between intelligence and evidence and gave a reason as to how the current situation unfolded. As he noted to the Washington Post in 2003, "Detective work and intelligence collection may resemble each other, but they are really completely different."[23] When considering how a police officer does their job, they aim to meet "a specific legal standard – probable cause . . . . or beyond a reasonable doubt. . . .. It depends on whether you want to start an investigation, put a suspect in jail or win a civil suit. Intelligence . . . . rarely tries to prove anything; its main purpose is to inform officials . . . ."[24]

Another difference between the two; they work according to different time schedules. Intelligence analysts are working to determine if there is a problem or the nature of an impending problem whereas police officers usually react / respond after a crime has been committed. "Law enforcement agencies take their time and doggedly pursue as many leads as they can. Intelligence analysts usually operate against the clock. There is a critical point in time where officials have to "go with what they've got," ambiguous or not."[25]

Some key historical moments are likely what led to the blurriness of intelligence and evidence and a shifting of responsibility from policy makers and law enforcement to intelligence analysts. One example is when in the 1970s, "monitoring arms control treaties became an important intelligence mission. The issue was whether the Soviet Union was in violation of an agreement."[26] Then in the early 1990s, post US Embassy bombings in East Africa, "a new buzzword began percolating through intelligence circles. . . . [i]ntelligence officials began saying their goal was to provide actionable intelligence."[27] While initially intended to mean information "precise and timely enough to tell you where to put a bomb or intercept a target,"[28] it has since evolved to refer "to data so clear and so thorough that policymakers can, literally, base a decision to take action on it."[29] The crux is that "the burden of making policy decisions [have been moved] from the shoulders of officials and politicians (where it belongs) to the shoulders of case officers and analysts (where it does not)."[30] For senior officials, this shift was

---

[22] *Ibid*.

[23] Bruce Berkowitz, "The Big Difference Between Intelligence and Evidence," rand.org (RAND, February 2, 2003), https://www.rand.org/blog/2003/02/the-big-difference-between-intelligence-and-evidence.html

[24] *Ibid*.

[25] *Ibid*.

[26] *Ibid*.

[27] *Ibid*.

[28] *Ibid*.

[29] *Ibid*.

[30] *Ibid.*

convenient. After all, "if they did not have good enough intelligence, they could be excused for not taking action — and the analysts would get the blame."[31]

CSIS' mandate is to analyze, collect and disseminate information so as to advise the government. The *CSIS Act*, Section 19 (2) states that where it has information that "may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province", CSIS may disclose that information to "a peace 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 in respect of the alleged contravention may be taken."[32] In the context of a potential criminal proceeding, it would appear as though if the RCMP relied on CSIS information to carry out its investigation and the fruits of that investigation must be disclosed to the defence, then all CSIS information relating to that particular case also has to be disclosed to the defence.

CSIS officers are not peace officers, they have no powers of arrest or detention, that is the purview of law enforcement. Intelligence work is often characterized as involving shades of grey, rather than the black and white world often described by law enforcement. "Information is not collected as evidence at trial but as input to the decision-making centres of government."[33] Intelligence is also ". . . . conducted in secret so that peoples' identities and reputations are protected and in order to protect the policy options of the state."[34]

The nature of the terrorist threat posed additional challenges to law enforcement and the RCMP is no exception. In the months following the 9/11 attacks, the RCMP created Integrated National Security Enforcement Teams (INSETs) to "collect, share, analyze information and intelligence that concern threats to the national security and criminal extremism/terrorism."[35] The purpose of the INSETs is "to reduce the threat of terrorist criminal activity in Canada and abroad by preventing, detecting, investigating, and gathering evidence to support the prosecution of those involved in national security-related criminal acts."[36] This is a departure from typical police activity wherein they are reactionary – responding after a crime has been committed. However, as law enforcement has always conducted activities in an attempt to prevent a crime from occurring, or 'catching' the perpetrators in the act to secure a conviction, it is not an entirely new concept. What makes terrorism slightly different is that according to the changes made to the Criminal Code post 9/11, several preparatory activities themselves were described as possible terrorism offences so it made clear that even planning such

---

[31] *Ibid.*

[32] "Canadian Security Intelligence Service Act," laws-lois.justice.gc.ca, April 27, 2023, https://laws-lois.justice.gc.ca/eng/acts/c-23/page-5.html#docCont

[33] Kent Roach, "When Secret Intelligence Becomes Evidence: Some Implications of Khadr and Charkaoui II," *The Supreme Court Law Review* 47 (2009).,162. https://www.canlii.org/en/commentary/doc/2009CanLIIDocs351

[34] *Ibid.*

[35] Leah West, "The Problem of 'Relevance'…".,70.

[36] *Ibid*.

activities could be indictable offences. This placed the RCMP INSET teams squarely in the space of where CSIS typically operates, in the 'before' space.

To muddy the waters even more, in 2015, Bill C-59 was passed which, among other things, gave CSIS the powers to use threat reduction measures – again, another departure from what the McDonald Commission envisioned (threat mitigation and enforcement powers were to remain with the police). So, the current environment has created the expectation for police to be more involved in the 'before' space and for CSIS to be engaged in trying to mitigate national security threats in the 'PoJ space'. The overall result is why we have the situation we have today – more than one agency being tasked to undertake the same activity but for different purposes. It has resulted in further blurring the line and has CSIS information "increasingly drawn into criminal proceedings."[37]

So how do the concerns of CSIS and the right of a government to protect its national security get weighed against the right of an accused to mount a full answer and defence? How do other democratic countries handle this balancing act?

THE FIVE EYES (FVEY) ALLIANCE

As a member of FVEY, it would be natural for the Canadian government to look to its closest allies for possible solutions. While the nature of the threat faced is slightly different for each country, each has found a way to deal with the inherent difficulty in balancing national security interests with the rights of the individual. Perhaps most notable and of importance to Canada are the changes made within the US and the UK; the US because of its geographic proximity to Canada and close working relationships between their intelligence and law enforcement agencies; and the UK due to historical linkages and a closely shared system of government and law.

Post 9/11, the US government quickly worked to make changes to what it viewed as a flawed intelligence system; a system that was replete with silos, lacking in a coordinated effort. As such, in 2002, Congress passed the *Homeland Security Act* whose aim was "to coordinate national security efforts."[38] In 2004, Congress also passed the *Intelligence Reform and Terrorism Prevention Act* (IRTPA) which created the office of the Director of National Intelligence (DNI). The 9/11 Commission report cited a lack of information sharing to be one of the biggest failures within the American intelligence community and through Congress, it was mandated that "an information-sharing environment, including fusion centers that allow federal, state, local, and tribal agencies to collaborate . . . . [be established] to help correct the communication breakdown between agencies."[39] Of note, this was all mandated through legislation passed by American legislators.

---

[37] *Ibid.,71*.

[38] J Dailey, "The Intelligence Club: A Comparative Look at Five Eyes," *Journal of Political Sciences and Public Affairs* 5, no. 261 (2017), https://www.longdom.org/open-access/the-intelligence-club-a-comparative-look-at-five-eyes-36432.html

[39] *Ibid.*

For the UK, the impetus for substantial, meaningful reform came in the aftermath of the July 7, 2005 attacks in London. Subsequent reviews agreed that "the existing model of siloed anti-terrorism and reactive policing was unworkable"[40]and the UK government set about to integrate its security service and law enforcement agencies. This has resulted in a more integrated model of cooperation in which "MI5 is confident that the courts will protect sensitive information from disclosure based on public interest immunity."[41] Of importance was its government's revision of Part II of the *Criminal Procedure and Investigations Act* (1996) which "sets out the manner in which police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation and which may be relevant to the investigation, and related matters."[42] In addition, a National Security Council (NSC) was established in 2010 in an effort to "consider matters related to national [defence], foreign policy, foreign relations, and intelligence coordination."[43] Of note with regards to this body's creation:

> "The 2010-2011 annual report by the Intelligence and Security Committee of Parliament provided several quotes by the leaders of the UKs intelligence agencies regarding the NSC. The chief of the SIS stated that the NSC was "a valuable step forward" and that a weekly meeting "enabled senior Ministers to have a fuller sense of the intelligence underpinning of the issues that they are addressing."[44]

What About Canada?

It is possible that because 9/11 was perpetrated against the US on American soil and the 7/7 attacks were perpetrated against the UK in London, it spurred lawmakers, be they in the American Congress or the UK Parliament to take it upon themselves to become better informed about the threats facing their respective countries and inform themselves as to how they can best be managed. Prior to 9/11, the Air India bombing "was the worst act of terrorism against the traveling public in world history,"[45] yet it elicited little reaction from either the Canadian government or public-at-large; not the way 9/11 galvanized support. This despite the fact that "the bombing of the Air India flight was the result of a conspiracy conceived, planned, and executed in Canada. Most of its victims were Canadians."[46] It would appear as though "Canadian did not embrace this disaster as their own."[47] Arguably and despite terrorist activity taking place both

---

[40] Dave Murray and Derek Huzulak, "Improving the Intelligence to Evidence…", 192.

[41] *Ibid.*

[42] Ministry of Justice, "Criminal Procedure and Investigations Act 1996 (Section 23(1)) Code of Practice," GOV.UK (Assets Publishing, November 23, 2020), https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-1996-section-231-code-of-practice

[43] J Dailey, "The Intelligence Club. . .".

[44] *Ibid.*

[45] Public Safety Canada, "Lessons to Be Learned," Public Safety Canada, September 20, 2022, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lssns-lrnd/index-en.aspx

[46] *Ibid.*

[47] *Ibid.*

within Canada and its closest allies, the threats facing Canada and its ability to combat them are not well understood within government.

While the Canadian government passed the Anti-terrorism Act in 2004 as a response to 9/11, it was an amending piece of legislation that had four objectives:

> "to prevent terrorists from getting into Canada; to activate tools to identify, prosecute, convict and punish terrorists; to keep the Canada-US border secure and a contributor to economic security; and to work with the international community to bring terrorists to justice and address the root causes of violence."[48]

Band-Aid Solutions

Over the years from both the experience obtained through national security investigations such as the Toronto-18, as well as various inquiries into how CSIS and the RCMP share information, the two organizations created a framework through which they would cooperate called One Vision. This framework relies on both agencies to conduct their own separate, but parallel, investigations. CSIS collects "intelligence under its mandate for advisory purposes . . . . and the police for Criminal Code purposes."[49] In short, this resulting framework solidified that which the McDonald Commission sought to avoid: a duplication of effort.

One Vision has evolved over the years to the now One Vision 3.0. This model shifts away from criminal prosecution as the gold standard to that of ensuring public safety through other possible means. It also includes a role for the Public Prosecution Service of Canada (PPSC).[50] While done with the best of intentions, the One Vision framework is resource intensive and complicated. It is "also potentially dangerous since they [CSIS and the RCMP] depend on the selective parceling of information from intelligence services to police,"[51] which has been condemned by committee reports since 9/11. In addition, prolific writers in this field, namely Craig Forcese and Kent Roach, note that "while criminal prosecutions are not the proper response to every terrorist threat and will not be possible in every case. . . . they remain the most transparent, fair and likely effective answer to those who are prepared to use violence. . . ."[52] But in Canada's national security environment, achieving a criminal prosecution

---

[48] Department of Justice Government of Canada, "About the Anti-Terrorism Act," Government of Canada, Department of Justice, Electronic Communications, July 7, 2021, https://www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html

[49] Dave Murray and Derek Huzulak, "Improving the Intelligence to Evidence. . .", 187.

[50] Jim Bronskill, "CSIS, RCMP Modelling New Security Collaboration Efforts on British Lessons," nationalpost.com, March 14, 2021, https://nationalpost.com/pmn/news-pmn/canada-news-pmn/csis-rcmp-modelling-new-security-collaboration-efforts-on-british-lessons

[51] Kent Roach and Craig Forcese, "Intelligence to Evidence in Civil and Criminal Proceedings: Response to August Consultation Paper," ssrn.com, September 13, 2017, p.3 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035466

[52] Dave Murray and Derek Huzulak, "Improving the Intelligence to Evidence...", 192.

for terrorism is difficult and is no longer seen as the gold standard by those conducting the investigations.

While efforts will be required to continuously improve the CSIS – RCMP relationship, there is no denying that the Canadian Supreme Court rulings of *Stinchcombe*, *McNeil* and *O'Connor* have had a chilling effect on information sharing between CSIS and the RCMP. Until a legal disclosure regime is better defined for national security, all the changes within the organizations and their relationship with one another will be for not. CSIS and RCMP cannot fix a problem that outside of their jurisdiction / authority to address. The government must now address this specifically. As noted by Kent Roach and Craig Forcese, there is a role for parliamentarians to play in drafting legislation that seeks to clarify the meaning of 'relevance' when "applied to the context of national security investigations."[53] As noted by both, the current standards are extrapolated from several rulings involving multiple cases and as such, are reliant upon "a heavily-lawyered approach"[54]that may cause "doubt and uncertainty."[55]

While looking again at the changes made within the UK system, their strength is the certainty that has been created within the legal framework as to what constitutes disclosure and relevance for national security. This has created

> "a platform on which MI5 and police expectations can be managed, and may have facilitated the movement to blended investigations. . . . it is easier to collect to evidential standards if you have reduced the evidentiary rules to plain text. You do not need to parse several hundred pages of Supreme Court jurisprudence to figure out what the Court had in mind."[56]

[53] Kent Roach and Craig Forcese, "Intelligence to Evidence in Civil and Criminal Proceedings. . .", 8
[54] *Ibid.,*7.
[55]*Ibid.*
[56]*Ibid.,*8.

IMPACT OF GOVERNMENT INACTION VIS-À-VIS LEGISLATIVE REFORM

When comparing Canadian prosecutions for terrorism or other hate-related crimes to other countries, Canada's numbers fall short. "As of November 2017, approximately 60 known foreign terrorist fighters have been permitted to return and live in Canada without criminal consequences."[57] However, in the UK, "between 2015 and 2016 prosecuted 79 people for terrorism related offences, and in 2017 arrested 400 more."[58] Canada has strong anti-terrorism legislation brought in post 9/11 with subsequent additions through the years, so a lack of law is not the reason why. The reason is "believed to be more a result of shortcomings and roadblocks in the I2E model which has tended to discourage authorities in many cases from pursuing a prosecutorial path."[59]

The worry from CSIS is that its "targets, sources, means and methods may be disclosed to the defence (and public) in a prosecution, should CSIS share its intelligence with the police."[60] This thereby creates the silos that were often referred to in the post 9/11 reports of several countries, including those also found from the Air India Inquiry in Canada. "Silos are anathema in a dynamic security environment."[61]

An MI5 officer, while serving in Ottawa gave testimony that "the key difference between operations of the UK and Canada was that CSIS and the RCMP lacked the institutional framework to share information extensively and also protect themselves from disclosure in criminal proceedings."[62] What is often not well understood is the nature of security intelligence collection. For CSIS, its intelligence collection has both domestic and foreign elements that need to be considered. "The threat actors, influences, consequences and theatres of operation demand liaison and information sharing with foreign and domestic partners. . . . often under the demand for secrecy."[63] Within this context, it should be easier to understand "maintaining strong relationships of trust with these partners is vital to [CSIS'] success."[64]

Without amending legislation that defines relevance in the context of national security, CSIS' information will continue to be sought for disclosure in public, This will cause CSIS to either reconsider what information it shares with the RCMP or it will have to engage in lengthy trails to determine relevance and disclosure of its information. These lengthy trials take an economic toll on all parties involved (state and individual), and often run counter to an accused's right to have a speedy trial.

---

[57] Leah West, "The Problem of 'Relevance'. . .", 58.

[58] *Ibid.*

[59] Dave Murray and Derek Huzulak, "Improving the Intelligence to Evidence (I2E) Model . . .",196.

[60] Craig Forcese, "Threading the Needle: Structural Reform & Canada's Intelligence to Evidence Dilemma," *Manitoba Law Journal* 42, no. 4 (2019): pp. 131-187, https://tinyurl.com/mp92b8px p.132.

[61] *Ibid.,* 133.

[62] Leah West, "The Problem of 'Relevance': Intelligence to Evidence Lessons from UK . . .", 64.

[63] *Ibid.,* 60.

[64] *Ibid.*

While much of the government's efforts to-date have focused on how CSIS and the RCMP can improve their information-sharing and ensuring there are enough oversight bodies for those involved in national security, a fundamental key aspect is missing: a Cabinet-level body responsible for national security matters. A half step measure was created in 2017 with the passing of the *National Security and Intelligence Committee of Parliamentarians Act*. Its mandate:

> "to review the legislative, regulatory, policy, administrative and financial framework for national security and intelligence; any activity carried out by a department that relates to national security or intelligence. . . .; and any matter relating to national security or intelligence that a minister of the Crown refers to the Committee."[65]

In its Special Report on the National Security and Intelligence Activities of Global Affairs Canada (GAC) submitted June 2022, several findings were directly linked to the I2E problem. One of the key findings was when considering the threat posed by foreign interference in Canada, GAC's response, despite the tools it has to use to counter this threat at its disposal, have largely been ignored. In fact, the committee ". . . . expressed concern that GAC's leadership role in responding to foreign interference meant that foreign policy considerations often take precedence over considerations of domestic harms."[66] In addition, the committee noted that because up until now, GAC has not had any reporting requirement to the Minister of Foreign Affairs "on the full spectrum of its national security and intelligence activities. This gap raises concerns about the Minister's awareness of the risk associated with the Department's most sensitive activities . . . . and undermines the Minister's accountability for those activities."[67]

The I2E problem is largely focused on the information sharing between CSIS and the RCMP, despite other government departments having key roles to play in the collection and sharing of information on national security. If GAC is meant to be a coordinating department and it is falling well short per the committee's report, what are the parliamentarians prepared to do about it? At what point will parliamentarians take action and legislate the changes they wish to see as Congress did in the US and Parliament did in the UK? A cohesive strategy on national security is required; Canada's allies have positive comments to say about the impact it is having in their respective countries, yet Canadian parliamentarians continue to drag their feet. "Parliamentarians tasked with national security responsibilities have an obligation to

---

[65] Legislative Services Branch, "Consolidated Federal Laws of Canada, National Security and Intelligence Committee of Parliamentarians Act," National Security and Intelligence Committee of Parliamentarians Act, April 27, 2023, https://laws-lois.justice.gc.ca/eng/annualstatutes/2017_15/page-1.html

[66] "Special Report on the National Security and Intelligence Activities of Global Affairs Canada," nsicop.opsnr.ca, June 27, 2022, https://www.nsicop-cpsnr.ca/reports/rp-2022-11-04/special-report-global-affairs.pdf p. 5.

[67] *Ibid.,* 93.

ensure they fully understand the current model, why it has been shaped this way, and where legislative changes are required."[68]

A FINAL PLEA FOR CHANGE

Canada's current legal system and subsequent interpretations of the key cases has resulted in "[introducing] a structural impediment to the use of criminal law in national security matters where the criminal law is the most appropriate state tool."[69] CSIS and the RCMP

> ". . . . continue to operate in a challenging legal and operational environment. Relative to its close peers, Canadian national security law is a remarkably staid area, with often dated statutes setting parameters for state conduct in a world dramatically different from that anticipated by their drafters. Old statutory authorities are sometimes construed and reconstrued, producing awkward outcomes and occasional scandals. Occasional adjustments to national security laws, ... focus (mostly) on real issues, but fail to resolve old problems while creating new ones."[70]

In addition, Canada's bifurcation system creates lengthy and complicated trials with vast resources being expended not on determining guilt or innocence, but on what information can be disclosed. "Trial judges specialized in terrorism cases might reasonably be expected to handle both the trial and the disclosure issues, ideally in association with specialized prosecutorial teams."[71] By eliminating the bifurcation system, prosecutions could once again become the gold standard.

Finally, while the vast majority of emphasis for change in national security maters to-date have come from terrorist threats; recent events like the war in Ukraine and foreign interference in Canadian elections has demonstrated that "Canada remains unprepared to confront a rapidly shifting security environment. . . ."[72] As noted earlier in this paper, the Canadian government "does not have a permanent cabinet-level body focused on national security, a striking contrast to allies such as the United States"[73] and the UK. In addition, because

---

[68] Dave Murray and Derek Huzulak, "Improving the Intelligence to Evidence (I2E) Model . . .".,194.

[69] Jay Pelletier and Craig Forcese, "Curing Complexity: Moving Forward from the Toronto 18 on Intelligence to Evidence," *Manitboa Law Journal*, 2019, pp. 155-179, B. Evidentiary Intelligence and the Warrant Process | Chapter 7 – Curing Complexity: Moving Forward from the Toronto 18 on Intelligence-to-Evidence | CanLII

[70] Craig Forcese, "Staying Left of Bang: Reforming Canada's Approach to Anti-Terrorism Investigations," papers.ssrn.com, June 1, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2976441, 1-2.

[71] *Ibid, 19-20.*

[72] Jack Burnam, "Canada's National Security Institutions Have Fallen Woefully Behind," Policy Options, November 7, 2022, https://policyoptions.irpp.org/magazines/november-2022/canada-national-security-challenges/

[73] *Ibid.*

> ". . . . we have no equivalent of a US or UK National Security Council. . . . nor . . . . an 'intelligence czar,' . . . . the national security and intelligence advisor faces a challenging task of coordination with no formal powers beyond persuasion and a closeness to the prime minister."[74]

Canadian national security currently exists in a decentralized format with ". . . . a diffuse governance model, of unknown and unmeasured performance."[75] The system has not kept pace with the types of threats facing the government. "The new threat environment also places even greater emphasis on Canada's ability to work closely with allies. An overly decentralized national security system is now a deep liability, ..."[76] and limits Canada's ability to coordinate efforts with its partners.

In hindsight, there have been several instances in which intelligence agencies failed to uncover possible threats and 9/11 made clear what the repercussions could be if officials wait for 'actionable intelligence'. The US "had good information about the training camps in Afghanistan, and there were strong signs that al Qaeda was behind the 1998 bombings of two U.S. embassies in East Africa and the 1999 attack on the USS Cole in Yemen."[77] The real problem for US government officials was that they never believed the required threshold had been met "to trigger action against al Qaeda networks or training camps."[78] So, while intelligence agencies could have been better at sharing information and anticipating the 9/11 attacks, "it was the search for intelligence concrete enough to be used as evidence — . . . . — that led to intelligence failures that were, in part, really policy failures."[79] In short, intelligence alone should not decide what policy makers or law enforcement decide to do because there is often 'no smoking gun' in intelligence work. Rather, "elected officials will have to perform the job they are paid to do: Judge. Decide. Lead."[80]

---

[74] Wesley Wark, "A Case for Better Governance of Canadian National Security," Centre for International Governance Innovation, March 29, 2021, https://www.cigionline.org/articles/case-better-governance-canadian-national-security/.

[75] *Ibid.*

[76] *Ibid*.

[77] Bruce Berkowitz, "The Big Difference Between Intelligence and Evidence, . . .".

[78] *Ibid.*

[79] *Ibid.*

[80] *Ibid*.

BIBLIOGRAPHY

Berkowitz, Bruce. “The Big Difference Between Intelligence and Evidence.” rand.org. RAND, February 2, 2003. https://www.rand.org/blog/2003/02/the-big-difference-between-intelligence-and-evidence.html.

Bowal, Peter. “Stinchcombe: Crown Disclosure of Criminal Evidence.” LawNow Magazine. Centre for Public Legal Education Alberta, February 26, 2021. https://www.lawnow.org/stinchcombe-and-crown-disclosure-of-criminal-evidence-2/.

Branch, Legislative Services. “Consolidated Federal Laws of Canada, National Security and Intelligence Committee of Parliamentarians Act.” National Security and Intelligence Committee of Parliamentarians Act, April 27, 2023. https://laws-lois.justice.gc.ca/eng/annualstatutes/2017_15/page-1.html.

Bronskill, Jim. “CSIS, RCMP Modelling New Security Collaboration Efforts on British Lessons.” nationalpost.com, March 14, 2021. https://nationalpost.com/pmn/news-pmn/canada-news-pmn/csis-rcmp-modelling-new-security-collaboration-efforts-on-british-lessons.

Burnam, Jack. “Canada's National Security Institutions Have Fallen Woefully Behind.” Policy Options, November 7, 2022. https://policyoptions.irpp.org/magazines/november-2022/canada-national-security-challenges/.

Canada, Public Safety. “Lessons to Be Learned.” Public Safety Canada, September 20, 2022. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lssns-lrnd/index-en.aspx.

Canada, Public Safety. “National Security and Intelligence Review and Oversight Framework.” Public Safety Canada, March 18, 2020. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/036/index-en.aspx.

Canada, Public Safety. “Remarks by Director David Vigneault to the Centre for International Governance Innovation.” Public Safety Canada, August 20, 2021. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-en.aspx.

“Canadian Security Intelligence Service Act.” laws-lois.justice.gc.ca, April 27, 2023. https://laws-lois.justice.gc.ca/eng/acts/c-23/page-5.html#docCont.

“The CSIS-RCMP Relationship in _____Through the Lens of an Ongoing Investigation.” nsira-ossnr.gc.ca. Accessed May 5, 2023. https://nsira-ossnr.gc.ca/wp-content/uploads/Redacted-Regional-NSIRA-Review-e-Updated.pdf.

Dailey, J. “The Intelligence Club: A Comparative Look at Five Eyes.” *Journal of Political Sciences and Public Affairs* 5, no. 261 (2017). https://www.longdom.org/open-access/the-intelligence-club-a-comparative-look-at-five-eyes-36432.html.

Forcese, Craig. “Threading the Needle: Structural Reform & Canada's Intelligence to Evidence Dilemma.” *Manitoba Law Journal* 42, no. 4 (2019): 131–87. https://www.canlii.org/en/commentary/doc/2019CanLIIDocs2805

Forcese, Craig. “Staying Left of Bang: Reforming Canada's Approach to Anti-Terrorism Investigations.” papers.ssrn.com, June 1, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2976441.

Government of Canada, Department of Justice. “About the Anti-Terrorism Act.” Government of Canada, Department of Justice, Electronic Communications, July 7, 2021. https://www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html.

Government of Canada, Department of Justice. “National Security.” PPSC, July 20, 2021. https://www.ppsc-sppc.gc.ca/eng/pub/fpsd-sfpg/fps-sfp/tpd/p5/ch01.html.

Jack Burnham. Originally published on Policy Options November 3, 2022. “Canada's National Security Institutions Have Fallen Woefully Behind.” Policy Options, November 7, 2022. https://policyoptions.irpp.org/magazines/november-2022/canada-national-security-challenges/.

Ministry of Justice. “Criminal Procedure and Investigations Act 1996 (Section 23(1)) Code of Practice.” GOV.UK. Assets Publishing, November 23, 2020. https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-1996-section-231-code-of-practice.

Murray, Dave, and Derek Huzulak. “Improving the Intelligence to Evidence (I2E) Model in Canada.” *Manitoba Law Journal* 44, no. 1 (2021): 181–96. https://www.canlii.org/en/commentary/doc/2021CanLIIDocs1642

Nesbitt, Michael, and Dana Haag. “An Empirical Study of Terrorism Prosecutions in Canada.” *Alberta Law Review* 57, no. 3 (2020): 595–648. https://albertalawreview.com/index.php/ALR/article/view/2590/2551.

Pelletier, Jay, and Craig Forcese. “Curing Complexity: Moving Forward from the Toronto 18 on Intelligence to Evidence.” *Manitboa Law Journal*, 2019, 155–79. B. Evidentiary Intelligence and the Warrant Process | Chapter 7 – Curing Complexity: Moving Forward from the Toronto 18 on Intelligence-to-Evidence | CanLII.

“Protecting Canadians and Their Rights: A New Road Map for Canada’s National Security.” ourcommons.ca. Library of Parliament, May 2017.

https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP8874869/securp09/securp09-e.pdf.

"R v O'Connor [1995]." West Coast LEAF, November 25, 2014. https://www.westcoastleaf.org/our-work/r-v-oconnor-1995/.

Roach, Kent, and Craig Forcese. "Intelligence to Evidence in Civil and Criminal Proceedings: Response to August Consultation Paper." ssrn.com, September 13, 2017. https://tinyurl.com/5n8buxc3.

Roach, Kent. "Ensuring Democracy While Protecting Canadian National Security." Centre for International Governance Innovation, October 4, 2021. https://www.cigionline.org/publications/ensuring-democracy-while-protecting-canadian-national-security/.

Roach, Kent. "When Secret Intelligence Becomes Evidence: Some Implications of Khadr and Charkaoui II." *The Supreme Court Law Review* 47 (2009): 147–208. https://www.canlii.org/en/commentary/doc/2009CanLIIDocs351.

"Royal Canadian Mounted Police." RCMP.ca. / Gendarmerie royale du Canada, March 26, 2023. https://www.rcmp-grc.gc.ca/corporate-organisation/history-histoire/rcmp-origin-story-histoire-origine-grc-eng.htm.

"Special Report on the National Security and Intelligence Activities of Global Affairs Canada." nsicop.opsnr.ca, June 27, 2022. https://www.nsicop-cpsnr.ca/reports/rp-2022-11-04/special-report-global-affairs.pdf?trk=public_post_comment-text.

Tunney, Catharine, and Peter Zimonjic. "'Intelligence Is Not Truth': Why Prosecuting Foreign Election Interference Is Rare ." CBC.ca. CBC/Radio Canada, March 2, 2023. https://www.cbc.ca/news/politics/fadden-vigneault-intelligence-bar-evidence-1.6765673.

Tunney, Catharine. "Poor Communication between CSIS and RCMP Stalling Investigations, Says Watchdog | CBC News." CBCnews. CBC/Radio Canada, November 16, 2021. https://www.cbc.ca/news/politics/csis-rcmp-communication-1.6250560.

Wark, Wesley. "A Case for Better Governance of Canadian National Security." Centre for International Governance Innovation, March 29, 2021. https://www.cigionline.org/articles/case-better-governance-canadian-national-security/.

Warkentin, Jakki. "R v Mcneil: The Duty to Disclose Police Misconduct Records." canliiconnects.org, March 5, 2015. https://canliiconnects.org/en/commentaries/36168.

West, Leah. “The Problem of ‘Relevance’: Intelligence to Evidence Lessons from UK Terrorism Prosecutors.” *Manitoba Law Journal* 41, no. 4 (January 1, 2018): 57–112. https://tinyurl.com/mr2kpxra.