Improving the Intelligence to Evidence (I2E) Model in Canada

DAVE MURRAY AND DEREK HUZULAK [*]

ABSTRACT

This chapter examines some of the key issues and challenges of the intelligence to evidence (I2E) process, mainly regarding the exchange of information between the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP). For historical perspective, the authors cite findings from the 1981 McDonald Commission Report, concluding that subsequent events proved McDonald over-optimistic in terms of the expected level of cooperation and sharing of information between the new CSIS and the RCMP. The intervening years between the creation of CSIS in 1984 and the Toronto 18 case saw marginal progress towards improving inter-agency cooperation. Landmark judicial rulings, such as *R v. Stinchcombe*, only served to dampen any incentive to freely share information between the agencies and build an effective I2E operational model. The authors argue that the current I2E model, known as One Vision 2.0, developed in the years following the Toronto 18 case, while representing a notable improvement in the process, nevertheless falls short of achieving a robust framework. More recent improvements stemming from the joint CSIS/RCMP initiative "Midnight Horizon" are helpful but unlikely to move the needle substantially closer to the ideal. Pre-empting terrorist/hate-related attacks requires a more aggressive response than at present, one focused more on eliminating the threat through arrest and prosecution rather than lesser measures aimed at "threat reduction" or "threat containment." To that end, this chapter offers some recommendations. The authors conclude that while CSIS and the RCMP

[*] The authors are former senior operational managers with the Canadian Security Intelligence Service (CSIS). Now retired, their respective careers with CSIS spanned more than 30 years.

have accomplished much towards improving the I2E process, there are clear limits to what they can achieve on their own in the absence of broader government action. Parliament can and must do more to champion needed legislative and policy changes to provide intelligence and law enforcement officials with the additional tools and resources they need to achieve a maximum level of security against terrorist and hate-inspired attacks.

I. INTRODUCTION

The security/intelligence landscape in Canada has undergone considerable change in the past few years with new policy and legislation aimed at providing intelligence and enforcement agencies with additional tools to combat terrorist threats. At the same time, new accountability mechanisms have been introduced to ensure an appropriate balance is maintained with respect to civil and *Charter* rights.

Out of necessity, intelligence agencies conduct most of their investigations in the shadows, away from the public and media spotlights. Often, it is the perceived intelligence failures that make the headlines, while the far greater number of successes in detecting and preventing terrorist attacks, espionage, and foreign-influenced activities go unreported to protect the identities of confidential intelligence assets, methods of operation, and third-party information.

Critics of intelligence agencies and law enforcement sometimes paint a misinformed or exaggerated picture of a national security and public safety regime in crisis or plagued by inefficiencies and inter-agency turf wars.[1] While every country's security and intelligence apparatus labour under some degree of bureaucratic inefficiency and suffer occasional intelligence failures, Canadians can feel confident in having one of the most professional and accountable national security regimes in the world. That does not mean there are no major challenges or room for improvement.

One challenging area is the issue of I2E. This chapter lays out our thoughts as former intelligence insiders and practitioners familiar with the

---

[1] CSIS has many critics, ranging from civil liberties organizations to academics and journalists. While some criticism is based in fact, as validated through formal external review, the criticism often reflects the uneasy tension and balance of perception and values that exist in any democratic society between those who advocate for more effective national security models versus those who see national security more decidedly through the lens of civil liberties.

workings of I2E. We will argue that despite some evident success, the current I2E model has inherent vulnerabilities and that more can, and should, be done to effect model improvements. Other authors within these pages will have touched upon, directly or indirectly, the case-specific strengths and weaknesses of the I2E process as it unfolded during the Toronto 18 prosecutions. Instead, our objective is to broadly assess the currently accepted model that developed over several years following the Toronto 18 case and offer a perspective on how it might be made even stronger going forward. But first, it is important to consider some of the background to the issue in order to better understand the evolutionary factors at play.

II. The McDonald Commission

As part of an examination or study of Canadian national security policy, it is worth taking a step back in time to review the 1981 McDonald Commission Report, which proved wide-ranging in the scope of its inquiry and the foresight of many of its observations and recommendations. The Commission conducted arguably the most in-depth review of the national security framework ever conducted in Canada, before or since, and provided a number of insightful recommendations towards establishing sound, well-balanced national security policy and legislation.

The Commission was conducted in the aftermath of a domestic terrorism-related crisis (October 1970) perpetrated by members of the *Front de libération du Québec* (FLQ) and resulting in illegal or inappropriate activities by the RCMP Security Service. The fundamental question the Commissioners confronted was how to achieve an effective balance between national security and basic civil liberties. While the Commissioners focused on RCMP Security Service wrongdoings, their forward-looking recommendations were designed to create institutions that could effectively deal with the emergence of a more complex and challenging threat environment while adhering to the rule of law.

In the end, the Commissioners recommended the establishment of a new civilian intelligence agency – CSIS – and provided core terms of reference for the *CSIS Act* and subsequent operating policies. In recommending the establishment of a civilian intelligence agency to replace the RCMP Security Service, CSIS would not be granted police powers or a

mandate to deter, prevent, or counter threats.[2] As argued by the Commission, the danger would be that the new organization could "be both judge and executor."[3] Instead, the Commission saw prevention and countering as the role of relevant departments and agencies having enforcement powers, especially the police (specifically the RCMP), acting on CSIS intelligence.[4] CSIS thus became strictly a collection, analysis, advisory, and reporting agency expected to feed various government and law enforcement agencies information for the purposes of countering threats by way of arrest and prosecution, or other means.[5] CSIS would also collect security-related threat information for non-enforcement purposes to keep senior government officials and policymakers informed about major security issues and trends, both domestically and internationally. Additionally, unlike foreign intelligence collection as defined in section 16 of the *CSIS Act*, there was no statutory or geographic limitation or boundaries imposed on CSIS's ability to collect security-related intelligence (i.e., espionage, foreign-influenced, and terrorist-related activities directed against Canada or detrimental to Canadian interests) which can be collected globally through direct means or via established liaison channels with foreign partners.

From the start, the decision to establish separate mandated functions between police work (criminal) and intelligence collection naturally resulted in several hurdles, both anticipated and unanticipated, in efforts to carefully bridge the divide between the collection of intelligence and its use as evidence. As time passed and the threat environment grew more severe, the challenges of migrating intelligence to the enforcement side became more apparent and problematic.

---

2 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security Under the Law*, vol. 1, 2nd Report (Ottawa: Supply and Services Canada, 1981), 613.

3 Commission of Inquiry, *Freedom and Security Under the Law*, 613.

4 Commission of Inquiry, *Freedom and Security Under the Law*, 613.

5 It should be noted that the amended *CSIS Act* under Bill C-51 allows for certain threat reduction activities within strict policy guidelines or judicial approval. The introduction of CSIS's threat reduction powers remains highly controversial and suspect as to their effectiveness in fully neutralizing threats. As a matter of corporate practice and perhaps Ministerial direction, it would be reasonable to expect that threat reduction activities undertaken by CSIS should be used sparingly with caution and not be allowed, over time, to become the default or preferred means of addressing public safety and national security threats or justification by law enforcement in opting not to pursue a criminal investigation leading to arrest and prosecution.

III. Intelligence to Evidence (I2E) – A Work in Progress

Although the mandates would be separate, the McDonald Commission foresaw a close working relationship between the new CSIS and law enforcement. The Commission Report references joint operations with the police, liaison officers embedded in respective RCMP and CSIS offices to facilitate and control the exchange of information, and a resulting "mutual dependency" between CSIS intelligence collection and police enforcement.[6] The Commission anticipated that CSIS and the police would liaise and cooperate in a way that would "avoid duplication."[7] In the years immediately after the 1985 Air India bombings, liaison was taken to the level wherein RCMP and CSIS liaison officers were embedded in each other's major offices, with RCMP liaison officers having the authority to review "all" CSIS terrorist-related reporting. It should come as no surprise that CSIS produced a disproportionate amount of the combined terrorist-related reporting between the agencies. RCMP liaison officers were routinely copied on all CSIS terrorist-related reports and were free to request formal disclosure of any information contained therein. CSIS, in turn, was free to approve or reject disclosure, the latter without an obligation to provide detailed justification. Although CSIS retained ultimate control over the disclosure of its information, in many ways the CSIS/RCMP liaison program, discontinued shortly after 9/11, gave the RCMP an unprecedented right of review and potential access to a daily stream of CSIS counterterrorist reporting, a level of access, albeit indirect, never before or since enjoyed.

Much has changed in the legal landscape since the McDonald Commission report, primarily because of *Charter*-based decisions by the courts. Of particular importance was the Supreme Court of Canada's decision in *R v. Stinchcombe*,[8] which reinforced full and fair disclosure to the accused. This had a profound impact on terrorism cases brought before the courts. It also had an additional chilling effect on the level of information sharing between CSIS and the RCMP. On the one hand, CSIS became increasingly concerned about disclosing information to the RCMP for fear that broader disclosure obligations to the defence post-*Stinchcombe* might

---

6 Commission of Inquiry, *Freedom and Security Under the Law*, 772.

7 Commission of Inquiry, *Freedom and Security Under the Law*, 423.

8 R v. Stinchcombe, [1991] 3 S.C.R. 326, 68 C.C.C. (3d) 1.

endanger and reveal sensitive sources and methods of operation. This fear was somewhat understandable given that "Canadian disclosure obligations are broader than equivalents in the United States and United Kingdom."[9]

On the other hand, the RCMP was more reluctant to rely too heavily on CSIS information in any potential criminal proceedings for fear that CSIS might at some point initiate an objection to disclosure under the *Canada Evidence Act*,[10] potentially resulting in a stay of proceedings. While the impact of *Stinchcombe* in creating a more demanding disclosure regime is real, it remains the case that if sensitive information was ever at jeopardy of being disclosed during court proceedings, the government could always invoke an objection under section 38 of the *Canada Evidence Act* "using what is known as an Attorney-General's certificate."[11] While certainly not the preferred outcome, the AG certificate does provide an important layer of protection against the risks associated with disclosure.

---

9 Craig Forcese, "Staying Left of Bang: Reforming Canada's Approach to Anti-terrorism Investigations," *Criminal Law Quarterly* 64 (2017): 493. This point is reinforced by Leah West in her comparative assessment of U.K. and Canadian disclosure regimes. As West argues, in addition to the material on which they have based their case, British prosecutors are only obligated to disclose information "which might reasonably be considered capable of undermining the case against the accused, or of assisting the case for the accused." This contrasts with the more demanding Canadian model under Stinchcombe which provides that "[u]nless the information is clearly irrelevant, privileged, or its disclosure is otherwise governed by law, the Crown must disclose to the accused all material in its possession." This plays out on numerous levels but is particularly relevant on the issue of British Security Service intelligence used to initiate a police investigation. West illustrates this by considering:

> [A] scenario where MI5 has human source intelligence that gives them reason to believe that a target of investigation is planning to detonate a bomb at a tube station one particular morning in London. This intelligence is passed from MI5 to the Metropolitan police who attend at the tube station. The police identify the subject, find explosives in his possession and arrest him. How the police knew to look for the accused in the station on that date is not subject to disclosure unless the prosecution concludes that something about the human source or the information they provided would undermine the Crown's case.

See Leah West, "The Problem of 'Relevance: Intelligence to Evidence Lessons from UK Terrorism Prosecutions," *Manitoba Law Journal* 41, no. 4 (2018): 76, 81, 93. This would be not the case in Canada under Stinchcombe, with the initial CSIS role being subject to disclosure and raising concern about the protection of source identities, which is critical to CSIS longer term investigative efforts.

10 R.S.C. 1985, c. C-5.

11 Forcese, "Staying Left of Bang," 503.

In order to limit sensitive CSIS intelligence and methodologies from being revealed in court proceedings, CSIS and the RCMP have developed the "One Vision" framework in which CSIS and the police conduct separate but parallel investigations against the same individual(s). One Vision was developed and formalized in the years following the Toronto 18 case and was directly informed by the procedures followed during the investigation by the RCMP and CSIS and related judicial rulings. The courts have generally accepted this framework, with CSIS collecting intelligence under its mandate for advisory purposes (and possibly threat reduction purposes) and the police for *Criminal Code* purposes. The model allows for strategic case management discussions at senior levels between CSIS and the RCMP, but disclosure to police investigative teams at the division level, formal or otherwise is, by design**,** limited to lessen the exposure of CSIS information during judicial proceedings. The result is the exact opposite of the McDonald Commission's views that close cooperation and liaison would help to "avoid duplication." Instead, One Vision rests heavily on duplicating investigations, with the police attempting to re-establish, through their own separate inquiries, things that CSIS may already know but cannot formally disclose to support court processes.[12] Even discussions at the senior levels of CSIS and the RCMP are routinely conducted in a manner so as to limit exposure of CSIS intelligence and focus only on what is strictly necessary for deconfliction and case management purposes.

Rather than increasing disclosure of CSIS intelligence, the focus, especially post-*Stinchcombe* and even more so after 9/11, has been on minimizing disclosure of CSIS information to the RCMP under what is termed the "less is more" approach. The guiding principle here is that CSIS provides the RCMP only the bare minimum amount of information it possesses in the form of a "disclosure letter" (versus an "advisory letter," which authorizes the use of CSIS information in court proceedings) directly linked to the elements of a criminal offence, sufficient in content to support the RCMP initiating their own criminal investigation, thus limiting the exposure of CSIS information. While the "less is more" approach is

---

[12] For an additional perspective on One Vision, see commentary by then-Director Richard Fadden at a February 11, 2013 session of the Standing Senate Committee on National Security and Defence: Ottawa, Senate, *Proceedings of the Standing Senate Committee on National Security and Defence*, 41-1, No. 12 (11 February 2013) (Richard Fadden).

attractive in theory, it has not always achieved the desired outcome in practice. Moreover, limiting the amount of CSIS information in the form of a disclosure letter does not necessarily guarantee an impenetrable shield around CSIS's information.

As the Air India Inquiry, chaired by former Supreme Court Justice John Major, concluded:

> There is a lack of institutionalized coordination and direction in national security matters. Canadian agencies have developed a culture of managing information in a manner designed to protect their individual institutional interests.
>
> The current practice of attempting to limit the information CSIS provides to the RCMP in order to prevent its disclosure in criminal proceedings is misguided... The result of such efforts to deny intelligence to the police is an impoverished response to terrorist threats.
>
> The processes and procedures by which decisions are made as to what information should be passed/exchanged between the intelligence and law enforcement communities are seriously flawed and require substantial revision.[13]

For the McDonald Commission, in recommending the establishment of CSIS, separation of the security intelligence function from the RCMP was the blueprint for moving forward by preventing any further illegal activities or dirty tricks and establishing a robust accountability regime and independent oversight of CSIS's activities. The McDonald Commission, while acutely aware of the risks of non-cooperation, appeared over-optimistic that inter-agency goodwill would ultimately prevail and lead to seamless cooperation. In fact, what developed was an initial period of organizational friction that hindered early efforts to achieve an effective model of cooperation. While the Commission proved insightful in most of its predictions and recommendations, this was perhaps its single and most consequential miscalculation. The *Stinchcombe* decision merely added an additional issue to what was already a relationship defined, more often than not in the early years, by inter-agency friction and institutional self-interest.

The initial years of organizational friction between CSIS and the RCMP have long since given way to a genuinely productive partnership and much closer cooperation in the greater public interest. CSIS and the RCMP have sought to adapt to legal realities through One Vision and, more recently,

---

13 "John Major's Air India Inquiry's Key Findings on Relationship between Intelligence and Evidence," *Georgia Straight*, December 11, 2012, www.straight.com/article-329962/Vancouver/john-majors-air-india-inquirys-key-findings-relationship-between-intelligence-and-evidence.

One Vision 2.0.[14] The One Vision initiative, while a credit to both organizations' commitment to building a closer working partnership and more effectively co-manage threats, also seeks the seemingly opposite goal of maintaining "an appropriate degree of separation between (their) respective (or parallel) investigations." Furthermore, in addressing the "triggers" for CSIS initiating discussions with the RCMP, One Vision 2.0 states: "CSIS has discretion with respect to why and when it chooses to disclose information to the RCMP. An assessment is undertaken by CSIS to determine whether to initiate Strategic Case Management discussions with, and possibly disclose information to, the RCMP."[15] While One Vision is a step in the right direction, we believe a more effective model is attainable, one that would further reduce the risk to public safety through greater sharing of information and the establishment of an integrated (also sometimes referred to as blended) model of investigation rather than continuing to conduct separate or parallel tracks of investigation.

It is difficult to conclude that a model based on duplication and paralleling of investigative activity, with a narrow range of interaction between the primary investigative bodies, strengthens national security. Questions must therefore be asked. First, is the current intelligence to evidence model better described as the institutions making the best out of a very difficult and complex legal disclosure regime? The answer, in our judgement, is yes. Secondly, does it create a greater risk than we should accept in the current heightened threat environment? Again, the answer is yes. Finally, while front-line agencies may be doing their best to successfully navigate around the challenges posed by I2E, is the legal framework now in place adequate for Canada's needs? The answer is no. The current legal framework around disclosure places unnecessary and unreasonable pressures and requirements on agencies like CSIS and the RCMP, often creating roadblocks to arrest and prosecution of serious threats.

To date, front-line agencies have made considerable progress towards improving collaboration, co-managing threats, and tailoring information exchanges through One Vision and other initiatives. What is missing and

---

[14] Colin Freeze, "Concerns over Bill C-51 Prompt CSIS to Brief Other Agencies on Operations," *Globe and Mail*, September 8, 2016, www.theglobeandmail.com/news/national/concerns-over-bill-c-51-prompts-csis-to-brief-other-agencies-on-operations/article31788063/.

[15] "CSIS-RCMP Framework for Cooperation: One Vision 2.0," Secret Law Gazette, November 10, 2015, secretlaw.omeka.net/items/show/21.

what is additionally needed is action by lawmakers to introduce new legislation and/or amend existing legislation that would better protect sensitive information from disclosure in court proceedings without negatively impacting an accused's right to a fair trial. The McDonald Commission cautioned: "Indeed, we consider a potential lack of cooperation between the Force (RCMP) and a separate civilian security intelligence agency as the greatest risk involved in the structural change we are proposing."[16] With that in mind, and despite much-improved cooperation as of late, in today's heightened threat environment, we should not underestimate the risk of failure of an intelligence to evidence model that creates challenges to exchange and disclosure, and that requires complex adaptations by front-line agencies charged with protecting national security. Intelligence enabling enforcement should become the driving force for change and the basis of future I2E model enhancements.

IV. DISCLOSURE AND THE FEDERAL COURT

Related to the question of I2E is the role of the Federal Court in ruling on disclosure of national security intelligence in court proceedings. Public discussion has centred on the issue of whether rulings on disclosure of sensitive security intelligence should be made by the trial judge, not the Federal Court as is the current practice. Concern has been raised that the existing bifurcated court model creates a "cumbersome" system wherein the Federal Court rules on disclosure and the trial judge must then accept the decision and determine whether a fair trial can then be held.[17] Although the Air India Commission "recommended that Canadian trial judges, like trial judges in Australia, the United Kingdom, and the United States, should be able to make – and if necessary, revise – non-disclosure orders during the course of terrorism trials... the federal government rejected these recommendations without any public explanation."[18] Ultimately, the matter was referred to the Supreme Court on appeal following a decision "by one of the judges in the Toronto 18 prosecution (who) held that the system was unconstitutional because it denied trial judges the right to control their own

16 Commission of Inquiry, *Freedom and Security Under the Law*, 771.

17 Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-Terrorism* (Toronto: Irwin Law, 2015), 305–08.

18 Forcese and Roach, *False Security*, 306–07.

trial."[19] The Supreme Court disagreed, deciding in favour of the government.[20] Despite the Supreme Court ruling, in our view, it only stands to reason that doing away with a bifurcated court system in favour of having the trial judge determine all matters related to disclosure would contribute greatly to a more efficient and just model. The constitutional and legal arguments may have been settled for now, but future governments interested in introducing substantive prosecutorial reforms to the national security area would be well advised to revisit the issue and bring this part of the legal system in line with that of some of our closest allies.

V. Lessons From Our Friends

In seeking to improve upon the current I2E model, much can be learned from some of our closest allies and how they have adapted to the contemporary terrorist reality. For example, in the United Kingdom (U.K.), the accepted practice is that all terrorism-related intelligence obtained by the police is provided to MI5, which sets the overall counterterrorism requirements and priorities for the country.[21] The U.K. model is based on some very hard lessons learned from security intelligence and law enforcement failures in a challenging counter terrorism environment.

Decades of living under a serious threat environment in which there have been dozens of mass-casualty terrorist attacks have focused the minds of authorities (police, intelligence, judicial, and government) on developing a relatively transparent and seamless model of cooperation, supported by a secure means of migrating intelligence to evidence. Given the high number of terrorist plots that have been detected and foiled in the U.K., particularly over the past several years, it is reasonable to conclude that the number of successful terrorist attacks in the U.K. would have been more numerous and deadlier absent the current model. As noted by the Director-General of MI5 in 2018: "Since the Westminster attack in March 2017, with the police we have thwarted a further 12 Islamist terror plots – 12 occasions where we have good reason to believe a terrorist attack would otherwise have taken

---

19 Forcese and Roach, *False Security*, 307.

20 Forcese and Roach, *False Security*, 307.

21 Frank Foley, *Countering Terrorism in Britain and France: Institutions, Norms and the Shadow of the Past* (Cambridge: Cambridge University Press, 2013), 131–32.

place. That brings the total number of disrupted attacks in the U.K. since 2013 to 25."[22]

Following the 7/7 attacks in 2005, U.K. intelligence and law enforcement concluded that the existing model of "siloed anti-terrorism" and "reactive policing" was "unworkable." A collective effort was undertaken to better integrate resources and investigations with "MI5 and police investigative units (now) co-located and (their personnel) embedded." The more integrated model must still pay attention to "careful management of disclosure issues," but the traditional fears and constraints surrounding disclosure are relaxed, and each other's mandates and roles are clearly understood and respected. For their part, MI5 is "confident" that the courts will protect "sensitive information" from disclosure based on "public interest immunity." While the U.K. system is not perfect, it has successfully overcome some of the major "dilemmas that bedevil Canadian anti-terrorism."[23]

VI. THE WAY FORWARD

I2E is but one challenge – albeit a major one – in building a more robust and effective counterterrorism response. The nature of the terrorist threat today in which groups like Al Qaida (AQ) and the Islamic State in Iraq and Syria (ISIS) and their sympathizers are prepared to engage in the indiscriminate mass killing of innocent civilians, including using suicide operatives, demands a firm response. We should also not exclude the growing threat of right-wing extremists who are equally prepared to commit serious acts of racially motivated or anti-government violence. As Craig Forcese and Kent Roach have correctly noted, 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 to achieve political, religious or ideological objectives."[24] Today's most dangerous terrorists are

---

22 "Director General Andrew Parker Speech to BFV Symposium," MI5 Security Service, May 14, 2018, https://www.mi5.gov.uk/news/director-general-andrew-parker-speech-to-bfv-symposium.

23 Forcese, "Staying Left of Bang," 502. Readers are encouraged to directly reference Forcese's detailed description of the U.K. model.

24 Kent Roach and Craig Forcese, "Intelligence to Evidence in Civil and Criminal Proceedings: Response to August Consultation Paper," *SSRN Electronic Journal* (2017): 3, http://dx.doi.org/10.2139/ssrn.3035466.

determined to inflict the maximum number of casualties and widespread damage. Authorities need to work together more closely and demonstrate an equal determination in response to such threats by making arrest and prosecution the preferred outcome at the outset of every terrorist investigation. The response in most cases should not be limited to "threat reduction" or "threat containment" but should instead focus on "threat elimination" through arrest, prosecution, and incarceration. Canada's terrorism offences "introduced since 9/11 are almost all strongly pre-emptive."[25] This provides law enforcement, acting on intelligence, ample opportunities to prosecute terrorist activities under a wide range of related criminal offences.

Policymakers need to think holistically about a national security model that achieves a maximum level of protection and security while respecting civil and *Charter* rights. More than three decades ago, the McDonald Commission understood that an effective national security model must be framed around a bold and comprehensive vision that connects all the parts. In our view, the way forward should include:

1. Addressing overall deficiencies in the I2E model. Toward this end, Canada can learn much from the British experience. It is indeed encouraging that efforts in this regard are reportedly already underway via "Midnight Horizon," a joint CSIS/RCMP initiative launched in 2018 and focused in part on a review of the U.K.'s Counter-Terrorism model with the goal of identifying best practices adaptable to the Canadian model that would result in more "robust information sharing… while protecting methods and sources."[26] Of the changes publicly acknowledged to date, one in particular merits specific mention: "An effort known as the Leads Pilot to assess incoming national security information, which CSIS and the RCMP say has already reduced duplication of effort."[27] This is a welcome and important change. Efforts to identify best practices among foreign allies

---

25 Forcese, "Staying Left of Bang," 489.

26 Jim Bronskill, "CSIS, RCMP Modelling New Security Collaboration Efforts on British Lessons," *Canadian Press*, March 14, 2021, https://www.cbc.ca/news/politics/csis-rcmp-collaboration-effort-1.5949531.

27 Bronskill, "New Security Collaboration."

need not, and should not, be limited to the U.K. Other close foreign intelligence and law enforcement partners may have proven processes and practices they are willing to share that might improve upon and be adaptable to the Canadian model. In our view, however, the main pillars of the U.K. model offer the best prospect of solving the I2E conundrum in Canada.

2. Members of Parliament must take a more active and determined role in identifying and seriously addressing weaknesses in the I2E process and making recommendations for legislative and mandate changes. Standing Parliamentary Committees having oversight of the issue in both the House and Senate have recently acknowledged that I2E continues to face legal, policy, operational, and organizational challenges and hurdles that merit formal review.[28] It is important to emphasize that the improvements achieved through One Vision and the adjustments arrived at via Midnight Horizon represent efforts to work around the elephant in the room: the need to conduct parallel investigations under the current legal framework wherein intelligence flows are restricted to the barest of minimums between CSIS and RCMP investigations. To reiterate, the current model remains one built on duplication, exactly what the McDonald Commission sought to avoid. What we see are efforts by institutions to do their best to work within a challenging disclosure regime by building in points of interaction to better coordinate their efforts. Despite improvements, this model will likely remain fraught with challenges and risks in managing disclosure through these narrow windows of engagement. Parliamentarians tasked with national security responsibilities have an obligation to ensure they fully understand the current model, why it has been shaped this way, and where legislative changes are required.

---

28 House of Commons, *National Security and Intelligence Committee of Parliamentarians, 2019 Annual Report* (March 2020) (Chair: Honourable David McGuinty); Jim Bronskill, "Canadian Senator Calls for Study of Hurdles to Using Secret Intelligence in Court," *The Associated Press*, January 23, 2021, https://globalnews.ca/news/7595278/secret-intelligence-court-cases/.

3. Give serious consideration to a model based on closer CSIS and RCMP integration, facilitating more seamless cooperation and information sharing aimed at identifying and countering terrorist threats and hate-related crimes. To be truly effective, any such model would likely require legislative changes given the impact of *Stinchcombe* as well as changes to agency core mandates. Collaborative approaches could range from operationally embedded employees in respective offices to potentially creating fully integrated CSIS-RCMP counterterrorism teams. At a minimum, co-location of personnel at the regional level, and specialized training of such staff in all facets of intelligence work and related enforcement operations, would mark a major leap forward in the evolution of I2E.[29] Such a model could even take on the characteristics of a permanent counterterrorism task force with members from both organizations seconded full-time to units for a minimum of several years or longer. Existing Integrated National Security Enforcement Teams (INSETs), created shortly after 9/11, could possibly provide a foundational basis for the establishment of such teams. That, however, would require re-defining the role and mandate of INSETs, restructuring of their current operational model, and a substantial increase in the commitment of personnel and level of information sharing by participating agencies.

VII. Final Thoughts

CSIS and the RCMP should be commended for their work in improving upon the I2E model which has resulted in a number of successful arrests and prosecutions. These successes alone have undoubtedly saved countless lives from terrorist attacks. The significant progress made, however, should not be viewed as the best that can be achieved. We believe the next step should be to address the limitations of the One Vision framework, principally by replacing separate, parallel investigations with a

---

[29] Counterintelligence cases would continue to be investigated initially by CSIS and separate from the blended integrated model due to their sensitivity and "non-threat-to-life" nature. See also fn 9 in reference to the greater flexibility built into the U.K. model, which helps facilitate greater ease of interaction between the British Security Service and the police.

more integrated model where information/intelligence is more freely shared among CSIS and RCMP counterterrorism experts and where prosecution becomes the overarching objective from the outset of all terrorist-related investigations. To date, terrorism and hate-related offences resulting in prosecutions have been few in number in Canada when compared to many other countries. This is clearly not explainable by a lack of *Criminal Code* offences and anti-terror laws under which to charge individuals, particularly post-9/11, but is believed to be more a result of shortcomings and roadblocks in the I2E model which have tended to discourage authorities in many cases from pursuing a prosecutorial path. The Federal Government's recent decision to establish a new office of Director of Terrorism Prosecutions is a positive development that will hopefully result in more terrorist-related and hate-inspired prosecutions in the future and provide an incentive for changes at the investigative/operational level in line with what we are proposing.

The changes we propose may be viewed by some as unnecessary in light of enhancements to the One Vision framework, most recently those resulting from the Midnight Horizon initiative. Fair enough. But the ultimate goal of every terrorist or hate-inspired investigation should be to reduce the risk and element of chance to an absolute minimum in detecting and preventing violence as part of a zero-tolerance policy. Any model built on narrow and restricted points of engagement between separate but parallel investigations will likely continue to fall short of that ideal, with risks relating to both issues of disclosure and for the potential for things to be missed or fall through the cracks. On this, there is only so much CSIS and the RCMP can achieve on their own. Unless and until Parliament considers the various shortcomings of the I2E model and recommends meaningful legislative and policy fixes beyond what front-line agencies can achieve working together independently, the ability to aggressively deal with threats through prosecutorial means will remain, inherently, an area of concern and vulnerability.