The Spy Who Briefed Me:

The benefits and risks of cooperation between the Canadian Intelligence and national security community and its non-traditional partners

Stephanie Carvin,
Norman Paterson School of International Affairs, Carleton University

Thomas Juneau, Graduate School of Public and International Affairs, University of Ottawa

Corresponding Author
Stephanie Carvin
stephaniecarvin@cunet.carleton.ca

TSAS RB 2023-05

TSAS
canadian network for research on terrorism, security and society

Introduction

In recent years, scholarship on the Canadian national security and intelligence community has focused on its structure and functions, (Carvin, Juneau and Forcese 2021; Juneau, Lagassé and Vucetic 2019; Juneau and Carvin 2021), critical scholarship (Crosby and Monaghan 2018; Lyon and Murakami Wood 2020); Nagra and Maurutto 2013), history (Barnes 2020; Kealey 2017; Sethna and Hewitt 2018) and legal issues and reform (Forcese and West 2020; West 2018).

Less attention has been paid to how the Canadian intelligence and national security community has evolved. The intelligence studies literature on change, reform, and adaptation suggests that we should expect evolution in the aftermath of two events. The first is "strategic surprise", or "the sudden realization that one has been operating on the basis of an erroneous threat assessment that results in a failure to anticipate a grave threat to vital national interests" (Handel 1984; Jones and Silberzahn 2013; Lowenthal 2017). The second is "intelligence failure", essentially, failure in the acquisition, analysis, or most likely the appreciation of relevant data by the intelligence community (Betts 1978; Gentry 2008).

However, in our research, we find that there are a number of problems applying these models to Canada. First, this literature is largely focused on the experience of the United States and, to a lesser extent, other countries such as the United Kingdom or Israel (Betts 1978, 1982, 2007; Byman 2005; Dahl 2013; Diamond 2008; Gentry 2008; Honig 2008; Jervis 2010; Kahana 2005; Morrison 2011; Parker and Stern 2005; Wirtz 2017). However, these explanations which link reform to the aftermath of strategic surprise or intelligence failure do not fit the Canadian case. Although there have been controversies in Canada relating to intelligence and national security, the country has generally not experienced intelligence failures or strategic surprises of the type seen in other national contexts.

Therefore, to explain change in the Canadian intelligence and national security community, we use the concept of "shock" to the system, based on a description of a need for a sudden response by one of our project interviewees. A shock consists of three parts – 1) an unforeseen event that 2) creates a sudden shift in threat perception that 3) the intelligence and national security community is initially poorly set up to address by itself and so needs to turn to partners it traditionally has not worked with before ("non-traditional partners"). This produces a requirement for quick adjustment in the community, by building bridges to work with new departments, agencies and organizations within and beyond the federal government. It also calls for internal adjustments, including developing accessible products for new consumers and factoring in intelligence to decision making where it was previously absent. Most importantly, it requires thinking beyond strict institutional mandates and stovepipes, and considering other departments and agencies where previously bureaucratic and cultural barriers may have existed.

In this paper we briefly outline our methodology and findings of our research. We highlight the advantages of closer cooperation between the intelligence and national security committee and its non-traditional partners, but conclude with some risks and challenges that need to be addressed going forward.

Methodology

This research is part of a larger project on understanding the relationship between intelligence and policy making in Canada. Between 2018-2022, we conducted over 70 semi-structured interviews with individuals who either produced or consumed (or both over the course of their career) intelligence products. We selected interviewees based on our contacts, snowball sampling, and cold-call emails. The rank of these individuals ranged from desk officer and analyst through to deputy minister or head of agency level. Some were still in service at the time of the interview, while others were retired. Funding for these interviews was made possible by the Social Sciences and Humanities Research Council (SSHRC) and TSAS.

Four shocks to the system

We distinguish shocks from strategic surprise and intelligence failure in that the former does not have *immediate* negative consequences for the country in which it takes place. However, a realization of potential future negative consequences motivates the need for evolution, notably through enhanced collaboration.

From the interviews we conducted between 2018-2022, we identify four major shocks as case studies:

- ***Foreign investment (2012):*** The purchase of NEXEN Inc. by the Chinese National Overseas Oil Corporation (CNOOC)
  Traditional and non-traditional partners: The Canadian Security Intelligence Service (CSIS) and Innovation, Science and Economic Development Canada (ISED)
  In response to this event, the Harper government introduces enhanced scrutiny of foreign investment by foreign and state-owned enterprises, requiring enhanced collaboration between the national security and intelligence community, notably CSIS, and ISED, with the former providing enhanced advice to the latter.
- ***Extremist travellers (2013):*** The realization that large numbers of Canadian extremist travellers (foreign fighters) were travelling overseas.
  Traditional and non-traditional partners: RCMP and Passport Canada
  Following attacks by Canadians at the In Amenas refinery in Algeria, Bugas Airport in Bulgaria in 2013, and increase in the number of Canadian extremist travellers to Syria, a need to track and prevent Canadian extremist travellers from going overseas.
- ***Threats to democratic institutions (2016):*** The realization of foreign interference in the 2016 US election.
  Traditional and non-traditional partners: Communications Security Establishment (CSE) and Elections Canada
  Concern that foreign adversaries will interfere in the Canadian election in the way Russia interfered in the US election in 2016 and in other countries such as France in 2017 requires the community, including CSE, to work with Elections Canada on developing a

plan to respond and notify Canadians if a similar incident occurs. It also leads to the creation of the Security and Intelligence Threats to Elections (SITE) Task Force

- ***COVID-19 pandemic (2020):*** Unprecedented public health emergency
  Traditional and non-traditional partners: Canada Border Services Agency (CBSA) and Public Health Agency of Canada (PHAC)
  Following the outbreak of COVID-19, CBSA worked with PHAC to prevent fraudulent COVID-19-related materials (such as testing kits, personal protective equipment). PHAC provided insight on how to recognize this contraband. Work was also done to secure the safe delivery of COIVD-19 vaccines to Canada.

In our view, these four shocks over the last ten years represent, collectively, one of the most significant drivers of change in the Canadian intelligence and national security community. Importantly, the requirement to work together does not mean that such collaboration was easy or natural. Media reporting suggests, for example, that CSIS and ISED found it difficult to cooperate over issues such as 5G. Nevertheless, we assess that there have been three significant impacts from this evolution.

First, this period led to significant increases in the exchange of information between Canadian policy makers and their intelligence and national security counterparts. While Canada continues to lack a centralized intelligence and national security body (like the UK's Joint Intelligence Committee or the US National Security Council), intelligence is increasingly playing a role in decision making in Canada.

Second, and concomitantly, there has been an increase in the number of people that have access to classified information and briefings, growing the size of the intelligence and national security community.

Third, increased demand has encouraged the intelligence community to develop shorter and more accessible products for busy policy makers. This includes more oral briefings, the use of one page "placemats" which explain issues in a more graphical way, increased use of open-source information in products to lower the classification and make products available to a greater number of individuals (Juneau and Carvin 2021: 111-119).

Risks and Challenges Ahead

The development of formal and informal ties between the core intelligence and national security agencies and departments with non-traditional partners is, overall, a very positive trend, albeit an incomplete one. Indeed, it is necessary to counter today's threats. However, it does raise several questions and challenges that both intelligence leaders and policy makers (and their critics) should be aware of.

Governance

Individual departments and agencies in the Canadian national security and intelligence community have learned to better work together in recent years, but there remains scope for improvement: our research shows that despite the increased desire for collaboration, the community continues to work far too much in silos, and the centre. As noted above, the Privy Council Office, under the leadership of the National Security and Intelligence Adviser to the prime Minister – is too weak to play a strong, community-wide leadership and coordination role. The intelligence "community", in this sense, continues to be one more in name than in reality.

This problem is inevitably compounded by the broadening of the actors involved in addressing the diversifying range of threats that Canada faces. This raises several technical issues. Non-traditional partners, for example, often do not have many officials with high security clearances (in a context where the granting of new clearances suffers from massive backlogs), or do not have easy access to highly classified information systems. Legal and regulatory frameworks governing the sharing of intelligence are often outdated or too rigid, further constraining coordination.

Moreover, the development of relations between intelligence agencies and non-traditional partners raises the still vexing question of their ability to understanding each other, what we refer to in our research as their respective policy and intelligence literacy (Juneau and Carvin 2021: 81-89). Our interviews found that policy literacy in the intelligence community – the overall understanding of how the policy world works, and more specifically of how it could use intelligence – has undoubtedly improved over the past couple decades, but that it remains low. Conversely, intelligence literacy – how policy makers in the political and senior bureaucratic realms understand what intelligence can, and cannot, do for them – has similarly improved but remains low. This paradox is only intensified when non-traditional partners are brought in.

This raises the issue of the bureaucratic governance of the national security and intelligence community. In the past two decades, our research has shown that governance in the national security and intelligence realms has improved: it has become more institutionalized, in particular, as deputy minister committees responsible for policy, operations, and assessments have been stood up and have matured. The broadening of the set of actors involved in national security, however, has taxed a system that, despite these recent improvements, remains flawed. Looking forward, the main actors involved, led by the NSIA, will need to figure out the right balance between involving these non-traditional partners in the governance of national security, while not taxing them with too much of a burden that is in addition to their many non-intelligence responsibilities.

Review, oversight, and transparency

Canada's national security and intelligence architecture has gone through the most significant changes to its governance and architecture in decades over the past few years. The creation of

the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the National Security and Intelligence Review Agency (NSIRA), in particular, have completely overhauled what was until then an inadequate and underdeveloped review and oversight mechanism (West 2021: 257-273.

This is, overall, a positive and much-needed development: strong review and oversight of intelligence is essential to democratic health and, by shining light on weaknesses and mistakes, is already providing an impetus for positive changes. Moreover, these changes have created a system whereby the review of intelligence activities are no longer stove-piped or linked to specific departments and agencies. Instead, review agencies now have the mandate to follow how intelligence and intelligence products are used across the federal government. This is very important for the legitimacy and social license of increased intelligence sharing.

Paradoxically in our research as well as in frequent informal conversations with officials in both the intelligence and political realm, we have frequently heard individuals expressing concerns – sometimes in an abstract way, but in other instances in reference to specific cases – that the greater transparency and scrutiny that comes with enhanced review and oversight risks increasing the opportunities for the politicization of intelligence. For example, concerns have been raised about Parliamentary review of intelligence documents related to the National Microbiology Lab and Canada's chaotic exit from Afghanistan in 2021. The Liberal government was accused of obfuscation in seeking to use intelligence review bodies to review an issue. For their part Conservatives were being accused of seeking to circumvent these bodies in order to politicize national security for partisan ends (West, Carvin, Juneau 2022). If the review and review bodies themselves become controversial, particularly where non-traditional national security partners are involved, the work and legitimacy of these bodies and their investigations may become compromised.

Politicization

The growing ties between core intelligence agencies and non-traditional partners also has the potential to reshape broader interactions between the intelligence and political realms in Canada.[1] In our research, we found no evidence of cases of the hard politicization of intelligence analysis in Canada. This conclusion can be contrasted with occasional media reports of such politicization in the US and UK. This is a good thing: intelligence analysis should, ideally, be unbiased and non-partisan; to optimally contribute to policy making, it should be, and be perceived as, fiercely independent.

There is a risk, however, that these growing relations with non-traditional partners could change the incentive structure: as intelligence analysis is used by a growing number of politicians and their staff to inform an expanding range of decisions and policies, there will be more opportunities to politicize it. As with the issue of review and oversight above, this should not be perceived as a call to slow or even roll back the normalization of intelligence throughout the

[1] This is a point we develop in a forthcoming article with *Intelligence and National Security*.

federal government machinery. To the contrary: this trend needs to continue and even intensify. It does, however, again imply that even if the net benefits are clearly positive, there are growing risks that need to be acknowledged and mitigated.

Conclusions

In an ideal scenario, intelligence products help provide a decision advantage to policy makers. The former help inform the latter through the provision of timely information that can help shape a problem and evaluate policy solutions. At the same time, policy makers should provide the context and requirements of what information they need to do their jobs to intelligence collection agencies.

We know, however, that this is difficult to do in practice – especially in a country where national security issues have traditionally taken a back seat to more pressing domestic ones. Moreover, bureaucratic fiefdoms, personality conflicts, stove-piped information flows and even a lack of secure infrastructure has hampered efforts at information sharing within the national security context.

Our research suggests that there has been significant progress in cooperation and information sharing not just between the different departments and agencies that comprise the intelligence and national security, but also with its non-traditional partners such as ISED, Passport Canada, Elections Canada and PHAC. Importantly, this widening of the community has not been centrally planned or coordinated, nor is cooperation automatic or easy. The intelligence world still struggles to understand the policy-world, and vice-versa. The scope for improvement of this otherwise positive development remains significant. Additionally, as we note above, while information sharing is good, it risks politicization, while the governance and review of such activities still needs to be developed.

Bibliography

Barnes, A. (2020). “Getting it Right: Canadian Intelligence Assessments on Iraq, 2002-2003” *Intelligence and National Security,* 35(7): 925-953.

Betts, R. (1978). “Analysis, War, and Decision: Why Intelligence Failures Are inevitable”, *World Politics,* 31(1): 61-89.

Richard Betts (1982). *Surprise Attack: Lessons for Defense Planning*. The Brookings Institution Press.

Betts, R. (2007). *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.

Byman, D. (2005). “Strategic Surprise and the September 11 Attacks”, *Annual Review of Political Science*, 8(1): 145-170

Carvin, S., Juneau, T., and Forcese, C., eds. (2021). *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*. Toronto: Toronto University Press.

Crosby, A. C., and Monaghan, J. (2018). *Policing Indigenous Movements: Dissent and the Security State*. Winnipeg: Fernwood Publishing.

Dahl, E. (2013). *Intelligence and Surprise Attack: Failure and Success from Pearl Harbour to 9/11 and Beyond*, Washington, DC: Georgetown University Press.

Diamond, J. (2008). *The CIA and the Culture of Failure: U.S. Intelligence from the End of the Cold War to the Invasion of Iraq*. Stanford: Stanford University Press.

Forcese, C. and West, L. (2021) *National Security Law*. Toronto: Irwin Law.

Gentry, J. (2008). “Intelligence Failure Reframed”, *Political Science Quarterly*, 123(2): 247-270.

Handel, M. (1984). “Intelligence and the problem of strategic surprise”, *The Journal of Strategic Studies*, 7(3): 229-281.

Honig, O. (2008). “Surprise Attacks—Are They Inevitable? Moving Beyond the Orthodox–Revisionist Dichotomy”, *Security Studies*, 17:1, 72-106

Jervis, R. (2010). *Why Intelligence Fails: Lessons from the Iranian Revolution and Iraq War*. Ithaca: Cornell University Press.

Jones, M., and Silberzahn, P. (2013). *Constructing Cassandra: Reframing Intelligence Failure at the CIA, 1947-2001.* Stanford: Stanford University Press.

Juneau, T., Lagassé, P., and Vucetic, S., eds. (2019). *Canadian Defence Policy in Theory and Practice*, Cham: Palgrave Macmillan.

Juneau, T., and Carvin, S. (2021), Intelligence Analysis and Policy Making: The Canadian Experience. Stanford: Stanford University Press.

Kahana, E. (2005). “Analyzing Israel's Intelligence Failures”*, International Journal of Intelligence and CounterIntelligence*, 18(2): 262-279.

Kealey, G. (2017). *The Royal Canadian Mounted Police Security Service and the Origins of the Long Cold War*, Toronto: University of Toronto Press.

Lowenthal, M. (2017). *Intelligence: From the Secrets to Policy*. Thousand Oaks: CQ Press.

Lyon, D., and Murakami Wood, D. (2020). *Big Data Surveillance and Security Intelligence: The Canadian Case*. Vancouver: UBC Press.

Morrison, J. (2011). "British Intelligence Failures in Iraq", *Intelligence and National Security*, 26(4): 509-520.

Nagra, B., and Maurutto, P. (2023). "Anti-Muslim Surveillance: Canadian Muslims' Experiences with CSIS", *Sociology of Race and Ethnicity*, (OnlineFirst) https://doi.org/10.1177/2332649223115158

Parker, C., and Stern, E. (2005). "Bolt from the Blue or Avoidable Failure? Revisiting September 11 and the Origins of Strategic Surprise", *Foreign Policy Analysis*, 1(3): 301–331.

Sethna, C., and Hewitt, S. (2018). *Just Watch Us: RCMP Surveillance of the Women's Liberation Movement in Cold War Canada*. Montreal & Kingston: McGill-Queen's University Press.

West, L. (2016). "Cyber Force: The International Legal Implications of the Communication Security Establishment's Expanded Mandate under Bill C-59", *Canadian Journal of Law and Technology*, 16(2): 381-415.

West, L., Carvin, S., and Juneau (2022). "National security can't become a tool of partisan feuding", *Globe and Mail*, 12 January https://www.theglobeandmail.com/opinion/article-national-security-cant-become-a-tool-of-partisan-feuding/

West, L. (2021). "Review and Oversight of National Security in Canada", in Carvin, S., Juneau, T. and Forcese, C. *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community.* Toronto: Toronto University Press: 257-273.

James Wirtz (2017). *Strategic Denial and Deception: The Twenty-First Century Challenge*. Routledge.