CÉPI CIPS
WORKING PAPER NO. 13 April 2020

Watching the Watchers: The National Security and Intelligence Committee of Parliamentarians in Action

Wesley Wark
Adjunct Professor, Centre on Public Management and Policy
Principal Researcher, Centre for International Policy Studies
University of Ottawa

The National Security and Intelligence Committee of Parliamentarians recently tabled its 2019 reports. NSICOP is a young and unique committee—not a regular committee of parliament but a specially constituted committee of members of both the House and Senate, appointed by the Prime Minister upon recommendations made by opposition parties with official standing. Committee members have high levels of security clearance that allow them as a body, for the first time in Canadian parliamentary history, to receive classified briefings and examine classified documents. NSICOP was established through legislation (Bill C-22) passed in the summer of 2017. It really only got going in early 2018 and has maintained an impressive tempo of meetings and reporting ever since. It submitted its first set of reports in December 2018 and these were published in April 2019.

Now we have a chance to examine the Committee's work at a further stage of maturity.

NSICOP makes its reports public after submission to the Prime Minister in classified form and following a redaction process managed by the Department of Justice to remove any sensitive national security information. The year 2019 was a truncated one for the Committee as it had to rush to complete its reporting for submission to the Prime Minister prior to the election call in September, 2019. Despite the time crunch, NSICOP produced in 2019 a massive annual report comprising 182 pages, and a special report dealing with the military's use of information on Canadians (57 pages). Both were tabled on March 12, 2020.

This report is divided into two parts. Part One examines the Committee's 'framework' reviews on chosen strategic issues affecting the security and intelligence community as a whole. Part Two looks at the more agency-specific ('activity') reviews undertaken by the Committee in 2019.

Part One: Framework Reviews

The two studies reviewed here take the form of what the Committee calls "framework" (or horizontal) reviews, which basically means tackling a strategic issue of concern that effects the working of Canada's security and intelligence community as a whole. The two framework reviews dealt with "Diversity and Inclusion in the Security and Intelligence Community" and "The Government Response to Foreign Interference." Both subjects were new to the Committee and had never before been subject to external study. Both subjects were chosen independently by the Committee through an internal process of deliberation involving the Committee's secretariat and its members. Both were excellent topic choices by the Committee, not least because they point to persistent problems that will need continuing study down the road.

The NSICOP Study of "Diversity and Inclusion in the Security and Intelligence Community" (Chapter 1)

The Committee indicated that its decision to embark on this foundational study was based on a variety of reasons, including the fact that ensuring diversity and inclusion in the make-up of the community is a challenge that persists with goals that remain elusive; a recognition that diversity and inclusion are not only in line with societal norms and goals but actually benefit the performance of the security and intelligence community; and that troubling cases involving harassment and violence within federal government departments and agencies, especially DND/Canadian armed forces, the RCMP and CSIS have become prominent in recent years.

The committee planned this initial study to create a baseline for a follow-on and more systematic assessment in 3-5 years. Although the current study is the first of its kind and exploratory, it is based on

Impressive research setting out the legislative framework for action, number crunching the available data, and providing an overall portrait of persistent deficiencies in reaching diversity goals and ensuring inclusivity. Hitting any kind of sweet spot is inherently difficult, giving the possibility of too aggressive or too under-stated findings and recommendations. It will come as no surprise that the data available suggest that diversity goals for the employment equity groups currently recognized by law such as women, indigenous persons, persons with disabilities, and visible minorities are not currently being fully met. The NSICOP study also recognizes that members of the LGBTQ2+ community are not currently part of the legislative mandate for equity hiring. Progress has been made, but it is unevenly distributed.

The good news is that many officials in the security and intelligence community, from the Prime Minister down, recognize the need for change and improvement. The bad news is that the benefits of supporting diversity and inclusion are not universally accepted within the workforce of the community. Evidence suggests that this might especially be the case within the RCMP and DND/CAF. More education is clearly needed.

There is another kind of bad news and that involves problems around evidence and standards. To achieve desired levels of increased diversity and inclusion it is absolutely essential that we can quantify existing levels of employment and existing experiences with inclusion. But the data itself remain outdated, soft, and subject to many different and uncoordinated methods of collection and analysis. Performance objectives suffer not just from data inadequacies but also from the same phenomenon of lack of uniform and coordinated plans.

In particular the Committee found that achieving better organizational outcomes was inhibited by lack of executive accountability, by inadequate or outdated performance measurements, by the failure to study barriers to diversity and inclusion, and by siloed responses to the problem, treated largely as an HR issue in individual departments and agencies. The Committee also noted that the Department of National Defence was less than forthcoming in supplying it with requested DND internal studies.

One noteworthy initiative was launched by the Prime Minister in December 2016 when he asked the leadership of the security and intelligence community to

create a group of experts to address diversity and inclusion challenge. This led to the formation of a so-called "Tiger Team" which met on a regular basis and had a clear reporting channel to the PCO. But whatever initial good work the Tiger Team may have done was hampered by organizational challenges, and a less than ambitious mandate. Sadly, the tigers seem ultimately to have gone to sleep. The NSICOP report notes that the Tiger Team has not met since July 2018. It is time, perhaps, for the Prime Minister to crack the whip again.

The Committee's recommendations may appear understated, but all are supported strongly by its analysis. It calls for better coordination, better data collection and analysis, stronger executive accountability, and a common performance measurement framework. None of this will be easy to do for departments and agencies with heavy operational burdens and finite resources. Underlying the Committee recommendations are two other themes: the need for real and sustained leadership to achieve diversity and inclusion goals, and the need for a culture shift on the part of the security and intelligence community to fully embrace diversity and inclusion principles. There is, of course, a chicken and egg problem nested here. The importance of diversity and inclusion can easily be set out in theory; the demonstrated benefits can only be fully realized once appropriate levels of diversity and inclusion have been achieved and sustained. For a country like Canada, where available statistics show that immigrants make up two-thirds of population growth, where the indigenous population is growing at four times the rate of non-indigenous peoples, where up to 13% of people self-identify as LGBT and where, by 2031, members of visible minorities will represent one-third of Canadians, we cannot wait for the full experiential proof of the benefits of diversity and inclusion, especially for the security and intelligence community. Hopefully the government will take the Committee's call to action seriously and re-energize the pursuit of diversity and inclusion in the security and intelligence community.

<u>The Government Response to Foreign Interference (Chapter 2)</u>

The National Security and Intelligence Committee of Parliamentarians has sounded the tocsin on the threat posed by foreign interference to Canada and on the inadequacies of the government's response to it. The media sat up on noticed. The NSICOP chapter on foreign interference garnered the most media attention on the report's release, probably because it offered headlines by explicitly naming China and Russia as leading state actors engaged in interference operations in Canada. While calling out China and Russia in broad terms, many passages of the public version of the study were redacted in ways that make it difficult to know the finer details of the Committee's analysis.

The relevance of a study of foreign interference is clear for any democracy and its threat extends well beyond Canada. Our allies and partners globally have been variously targeted, as the Committee report makes clear. Some countries may be out ahead of Canada in understanding and responding to the threat. The NSICOP study is welcome and timely in its effort to paint a picture of the threat to Canada and the government's response and situating this in a comparative context alongside our allies.

The Committee report opens by quoting an excerpt from a very important speech by the CSIS Director, David Vigneault, to the Economic Club of Canada in December 2018, shortly after the Committee decided to take up its study. In that speech, which has to be read as a major effort to change the national security agenda, Vigneault stated:

"*Terrorism has understandably occupied a significant portion of our collective attention for almost two decades.*

Nevertheless, other national security threats – such as foreign interference, cyber threats, and espionage – pose greater strategic challenges and must also be addressed.

Activities by hostile states can have a corrosive effect on our democratic systems and institutions.

Traditional interference by foreign spies remains the greatest danger, but interference using cyber means is a growing concern. [emphasis added]

The scales, speed, range, and impact of foreign interference has grown as a result of the Internet, social media platforms, and the availability of cheaper and more accessible tools.

These include social media bot-nets, "fake news", and advertising campaigns designed to confuse public opinion and influence our political system."

If M. Vigneault was trying to push the national security agenda in a new direction, some confusion nevertheless remains about the use of the phrase "traditional interference by foreign spies […]". The committee's own definition only clearly emerges at the very close of the study when it states its case for focusing on its preferred subject:

"The Committee recognizes that hostile foreign states will engage in both espionage and foreign interference, but it also notes that there is a clear distinction between espionage (i.e. exfiltration or stealing of information) and foreign interference (use of clandestine means or threats to promote a certain position or objective."

The Committee advances no argument to suggest that "traditional foreign interference" is more harmful to Canadian national security and democratic practices than foreign espionage, which would be a very debatable proposition, only that it is less well known and understood. In choosing to focus on foreign interference the Committee lopped off other significant elements of the problem beyond espionage, including cyber-enabled threats, election interference activities, and economic dimensions (hostile economic activities), which might have led them to a study of the Investment Canada Act. Maybe all these are on the cards for the future.

Despite the Committee's desire to focus in on foreign interference operations, it is important to note that foreign spy services will often be the drivers behind interference operations and that both espionage and interference may rely on the same instruments (including people) and techniques. If you are talking about a threat posed by activities generated by foreign espionage and security agencies, it is difficult to distinguish between their overlapping business lines.

Diaspora groups, or what the Committee calls ethnocultural communities, constitute the most vulnerable targets for foreign interference operations. Their free-speech and free-association activities, protected by the Canadian Charter, might be threatened. Any such efforts by foreign states, whether China, Russia or others (whose identities are redacted in the public report) to interfere with such rights must be vigorously countered and repressed.

Other civil society groups such as the academic sectors, the media, political actors, that are potential targets of foreign interference discussed in the report, arguably possess greater degrees of self-protection and are relatively less vulnerable. But all need to be made equally aware of the nature of the threat, even if the threat does not press equally on all such groups.

What must be avoided is any domestic politicisation of the foreign interference threat, in particular any articulation of the Cold War notion of "agents of influence" lurking within vulnerable civil society groups that is not backed by hard evidence and not handled through appropriate protocols. A model for such protocols might be offered by the system created to deal with concerns about election interference. Inappropriate practices, misguided assessments and public utterances by intelligence community officials could do the devil's work in a multi-cultural society.

The detailed examples provided in the report of foreign interference targeting political actors, the media, and academic institutions are almost entirely redacted, making it difficult to assess the quality of the evidence and judgements brought to bear (predominantly by CSIS) on these matters. The Committee offers no independent judgements on the threat reporting that has been conducted and offers no guidance on how best to bring public attention to such threats. It does indicate that "CSIS devotes considerable resources to investigating and reporting on foreign interference activities." What percentage of effort this represents relative to CSIS other main lines of reporting is redacted.

Other federal departments and agencies are engaged on the foreign interference issue, but here the Committee's report suggests different lenses brought to bear by, for example, the RCMP and Global Affairs Canada. The Committee appears, implicitly, critical of these non-CSIS perspectives. It also notes that the Privy Council Office has recently taken up the task of trying to develop a more government-wide approach to the problem, including through the plethora of senior officials committees now engaged on intelligence issues.

But it is worrying, as the Committee notes, that "security and intelligence organisations do not share a common understanding of the threat, including its gravity in Canada and its most common manifestations." The Committee, rightly, wants to see change in that regard. Not only are there disparate assessments of the nature of the threat but responses to date have usually been *ad hoc* and incident driven. The Committee chastises the government for its limited public engagement on this issue including to key "fundamental institutions" that might be affected. The government, it says, "must do better."

The Committee keeps its recommendations short and (relatively) sweet. The Committee asks the government to commit to the development of a strategic outlook and policy that would embrace all aspects of foreign interference, not just the ones studied by the committee. The commendation includes examining the adequacy of existing legislation, boosting public outreach and guiding cooperation with allies. The Committee also wants greater central leadership, citing the Australian creation of a "National Counter Foreign Interference Coordinator." The Committee presses on with an earlier recommendation for regular briefings to Parliamentarians on the foreign interference threat and beefed up expectations for Ministers regarding steps they are required to take to avoid any taint of foreign interference.

These recommendations are sound, but circumscribed. Even better than creating another siloed strategy for foreign interference, to join existing approaches to terrorism and cyber security, would be a proper, holistic national security strategy, that would include the full range of threats facing Canada and enumerate the responses to those threats. A foreign interference strategy would be a sub-set. Instead of creating a stand-alone foreign interference "czar," not a standard practice in the Canadian security and intelligence community, it might have been more practical to recommend an expanded role for the National Security and Intelligence Adviser and the Privy Council office machinery, with dedicated attention to foreign interference. Parliamentarians do need to be made aware of the work of NSICOP through systemic engagement.

If there are going to be briefings to members of the House and Senate, wouldn't it be better to have full national security briefings, not ones restricted to foreign interference matters alone?

The Committee argued in its report that "foreign interference in Canada has received minimal media and academic coverage and is not part of the wider public discourse." According to the Committee, "this has resulted in an assumption that foreign interference is not a significant problem in Canada." The evidence for this assertion is thin (there are redactions on this point in the report) and contradicted by the fairly extensive attention that has been paid in Canada to forms of Chinese interference in particular. Fear of the Chinese state's reach, for example, has been very prominent in public discussions on the issue of Huawei and its presence in 5G telecommunications systems. The problem is not minimal coverage of foreign interference but the absence of the necessary nuanced and strategic discussion. The Committee has made an important contribution to raising Canada's game in that regard. It has opportunities in future, by expanding the scope of its foreign interference study to include foreign espionage and cyber-enabled threats, by moving from the "traditional" to the "new," to make a much greater contribution still. Should it expand its study it would add weight to the recommendation that the government commit to a broad-based strategic outlook and policy covering all aspects of foreign interference in the Canadian democratic system.

Part Two: Agency-specific Reviews

The National Security and Intelligence Committee of Parliamentarians undertook two agency-specific (or what it calls "activity") reviews during 2019. One was a study of the national security and intelligence activities of the Canada Border Services Agency (CBSA), incorporated as chapter 3 of the annual report. The other was a stand-alone special report on the use of Canadians' communications by the Department of National Defence/Canadian Armed Forces. These agency-specific studies are important for what they reveal of activities undertaken by individual elements of the Canadian security and intelligence system which

have never before been subject to independent, external review. They are also a test of the ability of the Committee to engage not just on strategic issues affecting the community as a whole, but to dive deeper and review the operations of individual departments. With the coming into force of new national security legislation in 2019 (Bill C59), the future role of the Committee of Parliamentarians in conducting agency-specific review will have to be rethought. There is now, thanks to Bill C59, a National Security and Intelligence Review Agency (NSIRA) with a mandate precisely focused on agency specific review, with an emphasis on CSIS and CSE, but potentially embracing all elements of the Canadian security and intelligence system. The committee of parliamentarians will have to make a case that they need to continue agency-specific reviews in future, that they can do them well, and that they can avoid duplication, and work in harmony with the new NSIRA. In an ideal world it might be helpful for two review bodies to have a look at the same agency; in practice this would be wasteful of review resources and pose an unnecessary burden on the operational departments and agencies that are under the microscope.

The Committee should understand that the strategic (framework) reviews are their bread and butter. Perhaps agency-specific review can be considered as a necessary contribution to effective study of the more strategic environment of Canadian security and intelligence. But that case will have to be made and demonstrated, or the Committee will ultimately have to abandon its agency specific reviews. On the basis of the valuable work the Committee has done to date, that might be a pity.

The Canada Border Services Agency's National Security and Intelligence Activities (Chapter 3)

The Committee has conducted a milestone review—the first independent, external study of the Canada Border Services Agency. CBSA is a large federal department, with an annual budget of $1.87 billion for 2019-2020 and a workforce of 14,000 people. It was created in December 2003, driven by a post 9/11 security environment, through an amalgamation of elements of what was then called Citizenship and Immigration Canada (now Immigration, Refugees and Citizenship Canada), the Canada Customs and Revenue Agency (now Canada Revenue Agency), and the Canadian Food Inspection Agency. It faced a difficult and protracted birth, having to blend different work cultures into one organisation, focused on protecting and facilitating the functioning of Canada's borders.

CBSA is not a major intelligence collector, though it does run some independent collection programs. It is a major user of intelligence, which is critical to its ability to risk manage the border to allow for the essential movement of low risk people and goods, and to interdict high risk traffic. In this sense CBSA has a niche function in national security and intelligence but also has to be considered a core member of Canada's security and intelligence community. A key word that animates all of CBSA's work is admissibility. CBSA has legislative authority as the enforcement, intelligence and investigative arm of the Immigration and Refugees Protection Act (IRPA). To make proper determinations about the admissibility of people and goods, CBSA must have a strong intelligence capability.

The Committee's rationale for studying CBSA is clearly set out, as is its focus. It wanted to bring greater understanding of CBSA in the national security environment by defining its place in the security and intelligence community, identifying the proper authorities under which it operated, studying its governance, its conduct of sensitive national security and intelligence activities and its relations with key federal partners, such as IRCC, the RCMP and CSIS. All of this suggests two preoccupations—one concerning machinery of government, the other concerning the potential risks posed by CBSA's activities to Canadians' privacy and civil liberties. These are relevant and important preoccupations, but they don't necessarily fully answer the central question—whether or not CBSA has a strong intelligence capacity and uses intelligence well in its decision-making on admissibility. There are pieces of an answer in the Committee's look at some high-risk intelligence operations engaged in by CBSA, discussed below, but no overall assessment is provided. Future probes of CBSA either by the Committee or by the National Security and Intelligence Review Agency, need to probe this issue.

On CBSA's place in Canada's security and intelligence community the Committee recognises both its niche function and its core membership, without commenting on whether any tensions can arise in these disparate definitions. It allows that while CBSA has no specific legislative authority for conducting its national security and intelligence activities, these activities do flow organically from its various enabling pieces of legislation. The Committee finds CBSA to be well-governed with regard to its security functions, even while noting significant changes to its governance structure in April 2019 and concluding that it was too soon to make any "definitive assessment" of these changes. While CBSA told the Committee that the governance change was rooted in a desire to achieve greater clarity around internal roles and responsibilities and increase efficiency, the scale of problems that triggered this change are not addressed.

The Committee's study of CBSA's most sensitive intelligence and security operations is at the heart of the report. It looked at five areas:

Scenario-based targeting
Surveillance
Use of confidential human sources
"Lookouts"
Joint force operations

The methodology employed by the Committee was to assess the risks to Canadians' rights and to understand the ways these risks were handled and mitigated by CBSA in the course of its operations. It presents its findings in very handy tabular form even if the more revealing statistics are redacted.

All of these sensitive activities are meant to inform CBSA's admissibility decision-making. The Committee gives them all a thumbs up, to the extent of finding that CBSA has awareness of the risks involved and mitigation measures in place. Readers of its report will be in no position to second-guess its findings because of the sparsity of evidence provided (most is redacted). But the Committee has determined that activities such as scenario-based targeting (which is algorithm dependent) and CBSA's contribution to the RCMP-led National Security Joint Operations Centre, set up in 2014 as a fusion centre to deal with high risk travellers (including returned foreign fighters), show that CBSA is functioning effectively.

Yet at the same time the Committee notes in its conclusions and findings that "internal CBSA reporting on its sensitive national security and intelligence activities is piecemeal and lacks a cumulative assessment of risks and outcomes." In other words, the CBSA has a system for managing its national security and intelligence activities but no real capacity to know how well it is functioning overall.

This finding circles back to what I believe is the central issue—how capable is CBSA to use the intelligence at its disposal in decision-making on admissibility? The committee stuck to a fairly high-level overview of CBSA and does not appear to have conducted any in-depth case studies of its own that might have provided further elucidation. The only exception is a reference made in the report to a detailed examination of a singular case in which CBSA admitted it had erroneously granted permanent resident status to a foreign national of "national security concern" in August 2017. This story reached the media's attention in January 2019, although there are no references to media reporting in the Committee's brief mention of this episode. The Committee reaches no independent findings about this case, and contents itself with noting that "CBSA and IRCC have put in place measures to prevent similar cases in future." What those measures might be is not described.

The Committee also did not address issues around data management and information systems, at CBSA, a matter of long-standing concern.

When CBSA was created its leadership was deeply concerned about ensuring a culture shift within the new organisation to enable it to perform an intelligence collection, processing and analytical function to assist in border security admissibility decisions. What progress CBSA has made in the past decade and a half goes largely unanalysed in the Committee's report.

Two good things do emerge from the Committee's study of CBSA. One is a recommendation to ensure stronger Ministerial accountability for CBSA's national security and intelligence activities, through requirements for specific Ministerial directives to CBSA and CBSA annual reporting to the Minister

(the Minister of Public Safety). The other is the welcome news that CBSA has put a strong team together on its end to serve as liaison to the review bodies and that the CBSA team worked well to meet all of the Committee's requests for information in a timely and efficient manner.

Appreciating that the Committee has conducted a first-ever, but high-level look at CBSA, its work has to get high marks. The question remains of whether agency-specific studies are likely to be an element of the Committee's work going forward. The jury has to be out on this for now, in the sense that the Committee has demonstrated an ability to conduct a useful overview study of an agency, but has not shown an ability to conduct a more granular review that would probe deeper and deploy case study-style examinations. Should the new National Security and Intelligence Review Agency proceed with its own plans to examine CBSA, we might have an answer as to which body is best suited to conduct agency-specific studies. Back-to-back studies might also suggest the ways in which there can be a hand-off between the two review bodies from high level agency-specific studies conducted by NSICOP to more granular deep-dives conducted by NSIRA or indeed other independent agencies such as the Office of the Privacy Commissioner, where its mandate might be engaged.

In the meantime, Canadians have some reassurance that CBSA is well managed and that it is careful about the risks to Canadians' rights in the conduct of its national security and intelligence activities. What we don't have is any full assurance that CBSA has achieved the status of an effective user of intelligence in its border security mission.

Special Report on the "Collection, Use, Retention and Dissemination of Information on Canadians in the Context of the Department of National Defence and Canadian Armed Forces Defence Intelligence Activities"

This special report follows on directly from a study undertaken in 2018, during the Committee's first year of existence, into the defence intelligence activities of the Department of National Defence/Canadian Armed Forces. That study resulted in a recommendation, disliked in some DND circles, that the government should consider providing the military with clear statutory authority for the conduct of its defence intelligence activities, which have expanded considerably since 9/11, rather than allow these activities to rest on the uncertain constitutional framework of Crown prerogative.

This might look like a strictly legal argument, except that it isn't. Canadian military operations are evolving in a complex technological environment and often involve coalition partners. The possibility of defence intelligence scooping up Canadians' communications, and sharing it with coalition partners is real, as is the possibility of Canadians being engaged by our forces as enemy combatants in overseas missions, thanks to the emergence of the foreign fighter phenomenon in international terrorist groups.

To be clear, the Committee is not interested in hobbling Canadian military operations conducted under appropriate authority, and is not interested in denying the Canadian military the chance to exploit defence intelligence fully. They just want to be sure that any such activities are conducted under a clear and clearly lawful basis. They want that basis to be articulable, more in keeping with democratic principles, more credible than the doctrine of Crown prerogative, and able to provide the military with "social licence" for its activities.

They made this point in their 2018 report, but towards the very end of their first review they were presented with a late surprise. That surprise was a directive issued by the Chief of Defence Intelligence that was meant to provide guidance to his operators regarding the collection of Canadian information. The directive was promulgated in August 2018, in the midst of the Committee's initial review, but was only provided to the Committee in late October. It came into their hands too late to be incorporated into their 2018 study, but its nature underscored existing Committee concerns, so they decided to make this new Directive the focus of a special report written in 2019.

If the defence intelligence directive was meant to be a quick fix, it failed. The Committee, in its 2019 Special Report, found the directive to be inadequate, both in terms of its application in practice only to counter-intelligence activities and to activities conducted under the authority of another department, but also because the directive also

suggests a potentially broader authority which could be used to direct defence intelligence at Canadians. There is no smoking gun here, no suggestion that the military has hidden a program of spying targeting Canadians. The Committee instead harbours a future-leaning concern that ambiguity underlying the lawful basis for needed defence intelligence activities could be a problem cutting two ways—reducing defence intelligence operations unnecessarily, or opening up a wide vista with potential for abuse of Canadians' charter and privacy rights.

We now know that the government shares this concern and accepts the Committee's recommendations. The Prime Minister's mandate letter for the Minister of National Defence enjoins Minister Sajjan:

"With the support of the Minister of Public Safety and Emergency Preparedness, [to] introduce a new framework governing how Canada gathers, manages and uses defence intelligence, as recommended by the National Security and Intelligence Committee of Parliamentarians."

This is an important signal that the Committee's concerns about putting defence intelligence on a solid foundation will be acted on, though the "new framework" has not yet been revealed.

The Committee has done ground-breaking work to date in conducting independent review of the Department of National Defence/Canadian Armed Forces. The evidence is that it has not always found a willing dance partner at DND. Any atmosphere of distrust and friction that might have been generated in the first two years of the Committee's work will have to be managed and resolved in future. But the relationship could not have been helped by the fact that DND was unable to provide the Committee with either a rationale for the promulgation of the Defence Intelligence directive or any paper trail explaining its origins. Nor did the committee hear directly from either the Chief of Defence Intelligence, Rear Admiral Bishop, who signed off on the directive in August 2018, or the Director General of Intelligence Policy and Partnerships, who is responsible for its implementation. This looks like stone-walling and that will need to stop.

The experience in the Canadian system of review, dating back to the creation of the Security Intelligence Review Committee for CSIS in 1984, is that, sooner or later, departments and agencies that find themselves under the lens of external independent review come to accept this and appreciate its benefits. The sooner, rather than later, that DND joins the bandwagon, the better.