Canadian Security Intelligence Activities: A Necessary Intrusion, A Legal Challenge

©Reid Morden
Laurier Centre for Economic Research and Policy Analysis
International Symposium on Aviation Security
May 8, 2014

Canadian Security Intelligence Activities:
A Necessary Intrusion, A Legal Challenge

What we have been talking about this morning and will continue to talk about for the remainder of the Symposium are technologies and techniques which surround what is the most visibly and physically intrusive experience most people will encounter – the process we now all go through to get on an aircraft. There have also been the extensively reported instances of governments' accessing the personal information of their citizens and, from time to time, the citizens of other countries (just ask Chancellor Merkel). Why are we now so inundated with government-sponsored intrusiveness? Many would immediately say – 9/11. Maybe, but I think that while 9/11 may have brought this heightened level of intrusiveness to our doors faster, it simply accelerated a trend.

What brought this on? To start with, there has been a fundamental shift in the definition of national security itself. When Sir Francis Walsingham was running intelligence operations for Elizabeth I, national security was about the protection of the state and its vital interests from attack by other states. Fast forward 400 years, the concept has broadened to cover the responsibility of government to tackle a range of threats to individual citizens, families and businesses.

Today, there are public expectations – quite possibly unrealistic expectations - that government will be able to provide threat warnings and advise on how risks to individuals and businesses can be minimized. The terrain is unfortunately littered with terrorist operations, sometimes successful or partially so, sometimes anticipated and successfully thwarted. We should therefore not be surprised that public opinion demands inquiries of the intelligence community, into what they knew, and what they might have been expected to know that could have allowed the attack to be anticipated. In short, taxpayers want to know if they are getting their money's worth. And what you are discussing here today is part of that calculation because aviation security is obviously an expensive business.

Expensive or not, sustainable or not by bloodless economic analysis, I doubt that any government would base its security spending plans without reckoning the human and political costs of putting its citizens in danger of injury or death. And thus, the security overlay to which we are all subjected, is pretty much a permanent thing.

Nowhere is this more obvious than in movements of people, goods, and services across our border with the United States. For Canada, getting the security of the North American perimeter right outdoes everything else on our security radar. To bring this home we need do no more than calculate the impact on Canada when that border was shut down following 9/11. This is a border through which passes some 75% of Canada's exports, exports which fuel 40% of our economy. Somewhere around $ 2 Billion worth of goods cross that border each day, touching on not only Canada's biggest corporations but also the vast majority of the one million small and medium-sized businesses across Canada.

Our actions to manage the border take place against a background drumbeat of American political and media criticism of Canada' s attitude on security. While this criticism may not be well-founded, it exists and continues to have an important impact on Americans, in and out of government. There continues to be a serious, unending, and expensive job of building and maintaining the trust and confidence of not only the American Administration the American Congress but also American public opinion.
Against this backdrop, where should we find the balance, where should we draw the line between the security needs of the state and the rights of individual citizens?[1] What are we talking about? Within Canada intelligence is usually taken to mean security intelligence which is designed to be preventive. Whether it is countering espionage, subversion, or terrorism, the structures, equipment and activities of intelligence organizations should be geared to meet an agreed threat.

After 120 years of an interlocked security intelligence service and federal police force, it was only in 1984, by establishing the civilian Canadian Security Intelligence Service (CSIS) and the disbanding of the RCMP Security Service that Parliament recognized the differences between security intelligence activities and law enforcement work.

In providing a legislative basis for the new security service, the government recognized that intelligence cannot effectively operate by applying the often restrictive norms of the criminal law. Let me share a brief quote from Stanley Cohen, Senior General Counsel at the Federal Department of Justice which sums up the differences very neatly:

> **"*The divide between the investigative powers necessary for law enforcement and those necessary to protect national security is not an obvious one. However, while both of these spheres of official activity are carried out under the umbrella of the rule of law, they are quite distinct from one another and their needs and requirements differ substantially"[2].***

In other words, security issues often demand deep and intrusive probing if the security of Canada is to be adequately protected.

The need for these greater powers is balanced in the CSIS Act by a significantly higher level of third-party scrutiny than would have been feasible or appropriate for law enforcement. That balance is particularly reflected in the CSIS Act[3], in the creation of the Security Intelligence Review Committee (SIRC). SIRC's powers and mandate were largely borrowed in creating the Office of the Commissioner of the CSEC some twelve years later. A question today is whether such a degree of scrutiny should be applied to other institutions operating within the intelligence or security framework, such as certain aspects of the RCMP, the CBSA or the activities of CATSA.

---

[1] See Charkaoui v. Canada (Citizenship and Immigration), 2007 SCC 9 at para. 77.
[2] Stanley A. Cohen, Privacy, Crime and Terror, Legal Rights in a Time of Peril, LexisNexis Butterworth's, Dec. 2005, pg. 52
[3] CSIS Act, R.S.C. 1985

Until 9/11, our experience with terrorism was almost exclusively focused on those who brought their homeland issues onto our soil, whether it involved Armenians and Turks, members of the Provisional Irish Republican Army (PIRA), or Sikh extremists seeking a separate Khalistan or a regrettably long list of others.

Now, however, our own foreign policy leads us into areas of ideological and religious conflict where violence is often seen as the means of resolution. We are no longer simply a refuge for those seeking escape from hatred and strife in their homelands. Nor just a parking spot for those few who abuse Canada's hospitality and bring those homeland problems to our door. Now our own policies and actions motivate those who disagree with them, to retaliate on Canadian soil.[4] Closely related is the disturbing rise of domestic, home-grown terrorism among young people, fuelled in part by persistent economic disadvantage.

Let me change gears. The explosion of information means that policy officials will be more, not less reliant on information brokers. If collection is easier, ***selection*** is harder.
Now, as opposed to the days of the Cold War, intelligence is in the information business, not just the secrets business; a sea-change for the profession. Key questions, mysteries in effect, such as where and how terrorists will next attack, are more abundant now. To solve or even illuminate these mysteries, analysts certainly need access to secrets, but their crucial partnerships are with colleagues outside intelligence and outside government, in the academy and think-tank world, in non-governmental organizations and in private business. Intelligence needs to be opened wide, not closeted in secret compartments. We must recognize that intelligence business is about information, not secrets. I remain concerned that the intelligence community has not embraced this change.

And this leads us into yet another labyrinth. Modern intelligence systems have to be able to access in a timely, accurate, proportionate and legal way, information about individuals and their movements and activities that resides in data bases subject to Data Protection or Privacy legislation, or which may be held by other Governments or global commercial organizations such as airlines or banks.

I am not just referring to traditional police inquiries after the fact to examine the records of an individual identified as a suspect. Effective pre-emptive intelligence may, for example, depend upon data mining techniques applied to records in bulk form. Such techniques inevitably involve trawling through the records of the innocent as well as the suspect to identify patterns of interest for further investigation. Obtaining international agreement on the sharing of such data also becomes very important to ensure future access to these vital sources. In these remarks, I am not even going to touch on the issues surrounding our capabilities for electronic vacuuming.

Now that we have this vast stew of information, and have tried to make some sense of it by analysis, what do we do with it? Well, in the intelligence cycle, we disseminate it. In so doing the trend is to shift away from the highly restrictive "need to know' to what some have called "responsibility to provide", a phrase that expresses it well. In the modern world, we need to think of dissemination as both outward, including to partners and allies overseas, and

[4] Reid Morden, Globe and Mail Comment, July 30, 2005

downwards, where first, front-line or early responders must assimilate it with their own local knowledge and context.

Secondly, although the traditional written intelligence report will remain the staple, the requirement now is also for maps, pictures, biometrics, video and data of all kinds. A supporting infrastructure of secure broadband communications stretching out into the customers' space therefore becomes essential.

The goal in the end is not for analysts to make themselves smarter but to make policy better, make military decisions better and now enable improvement for law enforcement too. As I put it earlier, the key feature of 21st century intelligence is the pressure to use it for anticipatory purposes to protect the citizen.

Moreover, the pressure on the intelligence community to allow its knowledge to be used, including in court, can only increase. The pressure to allow pre-emptive action will increase. The requirement to be able to integrate multiple sources of intelligence in real time to support operations, whether at home or in far off theatres, will increase. The risk management judgments between longer-term exploitation and short term public protection will become harder.

In a book entitled "Diplomacy in the Digital Age"[5], Andrew Cohen, a veteran journalist now teaching at Carleton University, contributed an essay which caught my attention. It dealt, in part, with the impact of the WikiLeaks phenomenon on diplomacy and Cohen concluded that "nothing is secure anymore".[6] He posits, probably quite realistically, that less data will be committed to paper, that diplomatic exchanges will become less frank and open, and that, overall "the end of secrecy will diminish the currency of diplomacy"[7].

And is this relevant to the world of intelligence? You bet. In fact, anytime Cohen used the word "diplomacy", you could substitute "intelligence" and the meaning would remain quite *a propos.*

And this raises a crucial question for the intelligence world. Traditionally, it has gathered data through secret intelligence collection. If Cohen is right, and I think he is, those traditions are in the process of being trashed by the WikiLeaks phenomenon and the exponentially growing availability of open source information.

In fact, the security and intelligence community would be doing itself a favour, and get ahead of the wave, by rethinking the bare, unassailable basics which must, at all costs, be protected. Put an effective barrier around those few elements, and worry less about lesser issues.

In the security domain, there is an unprecedented onus on the courts to ensure that security legislation and police and security powers fit within Canada's constitution. And that they play

[5] Diplomacy in the Digital Age, ed. by Janice Gross Stein, McClelland & Stewart, 2011
[6] Andrew Cohen, Of Satraps and Supplicants: The Diplomatic Diary as the Last Safe Haven, p 232, ibid
[7] Andrew Cohen, p 233, ibid

an important role in delineating that crucial balance between the rights of citizens and the security of the state.

Unfamiliar as many of the factors which lead to security/terrorism cases before the bench will be, I urge that judges meet this new set of challenges directly. One important reason to do so lies with the court's role in protecting the rights of individuals. This is a role both prophylactic and remedial. It is also one which cannot be left solely to the discretion and disposal of the executive or legislative arms of government.

What all this comes down to is the need for recognition from the Canadian public that there is a threat and that it is every citizen's responsibility to help minimize that danger. We also need sustained government leadership which levels with Canadians on the dangers and deals firmly with elements of any community supporting or advocating violent acts, no matter the cause.