**John Tait Memorial Lecture - Canadian Association for Security and Intelligence Studies Annual Symposium**

 January 15, 2016   
 Ontario

Speech

*Check against delivery*

**Introduction**

Good morning.

Welcome to Ottawa and to the 2016 CASIS annual symposium. I would like to thank the conference organizers, and Greg Fyffe, President of the CASIS Board of Directors, for the kind invitation to speak to you all today.

I am honoured to have been invited to deliver this year’s John Tait Memorial Lecture. Unlike many past speakers, I was not personally acquainted with John. However, I have been fortunate enough to have found no shortage of people to tell me about him; his impact within the public service and beyond was considerable.

For those of you who are unaware, John was a distinguished scholar, a graduate of Princeton, Oxford and McGill Universities, a Rhodes Scholar and a lawyer. He had a distinguished career, moving between several federal government departments before becoming Deputy Minister of Justice and Deputy Attorney General of Canada in 1988.

In 1994, John became Senior Advisor to the Privy Council Office, to which role he added Coordinator of Security and Intelligence – a precursor to today’s National Security Advisor role – in 1996. It is in honour of his career and, in particular, that ultimate role, that this lecture bears his name.

Apart from his activities in support of security and intelligence development and coordination, however, John was also designated to lead a Deputy Minister Task Force on Public Service Values and Ethics. This year marks the 20-year anniversary of the report of the task force, Strong Foundations, which continues to inform the public service to this day.

While a report about values and ethics may not seem, on its face, as relevant as John’s activities specifically relating to security and intelligence, it occurred to me in preparing for today’s lecture that the opposite is true. Many of the most challenging issues that arise in respect of national security, and national security enforcement, relate in no small way to values and ethics. For example, the Islamic State, the focus of today’s conference, is driven by values that we recognize as anathema to our own, and the ethics of particular law enforcement tools and techniques are often debated.

Also notable within the discussion on values and ethics, and undeniably relevant to police, particularly as we confront the increasingly complex nature of both crime and enforcement, is the professionalism that is required – indeed, demanded – of all those who serve the public in this evolving world. The Strong Foundations report posits that a professional public service implies a body of knowledge, skills and expertise that those outside the profession are unlikely to possess, a set of values and attitudes that determine the culture of the profession, and a set of standards for both of these. I can think of virtually no arena in which these attributes are more important, in terms of keeping pace, doing one’s job well, and building and maintaining public trust, than modern police forces.

I have been striving since my appointment for ever-increasing professionalism in Canada’s national police force, my police force, your police force. This can be understood in a number of ways, depending on who you are, but the reason I think it bears emphasizing is that it is required to confront the particular national security threat environment in which we find ourselves today.

Professionalism, both in appearance and action, is also crucial to a larger issue that colours each and every one of our activities. While I will speak to investigative and enforcement challenges, as I tried to refine those topics I realized that our greatest challenge, and the one with the greatest impact, is more fundamental – trust and confidence in policing. While we, the police, may become occupied in chasing what we believe to be the holy grail – technological, legislative and policy solutions to the challenges we face – it is my view that if we do so exclusively, we are chasing the wrong holy grail.

In order to succeed in discharging our mandate what we ultimately require is the consent, confidence and fundamental trust of Canadians.

That requires that we contribute to an understanding of what is a complex swirl of social and legal issues. This audience – all of you -- are crucial to our ability to do that. Your end of this bargain is to engage with us, to ask questions and be willing to hear the answers, to be constructively critical. We are all, to some extent, in this together.

I will be speaking to you today about the current environment as seen by the RCMP, particularly as it relates to ISIL given the theme of this symposium. I will also outline for you some of our challenges and successes to date, and an approach to moving forward. I hope to leave time for questions at the end of my presentation, and I encourage you to ask them, not only of me but of subsequent presenters, as this symposium presents a unique opportunity for the engagement I’ve described.

**The Current Threat Environment**

The current threat environment is, in the intel lexicon, multi-dimensional and complex, and now includes individually-driven, sudden and unpredictable acts, such as the attack on Parliament on October 22nd. ISIL has become what one might term a “next generation” threat – it is active across a range of theatres, both inside and outside Canada, and has become effectively borderless. As my friend the Director of the FBI puts it, “This is not your parents’ Al Qaeda.” Primarily through the savvy use of technology, the threat is being aggressively marketed and promoted, and adherents are able to connect in increasingly seamless ways that are increasingly undetectable to law enforcement. It is able to be pushed out from an area – Iraq and Syria – that we have little to no visibility on. All of this will come as no surprise to this room.

The RCMP response to the current national security threat has several dimensions.

Our prevention activities are grounded in our crime prevention mandate and exist in the pre-criminal and criminal space. We strive to lay a proper foundation through bias-free, fair and inclusive policing. We also conduct engagement outreach sessions with many communities and deliver training to first responders. The RCMP works among a variety of governmental and non-governmental partners.

In terms of criminal investigation activities, our Integrated National Security Enforcement Teams – INSETS – and National Security Enforcement Sections – NSES – are able to quickly respond to investigative and operational aspects of incidents and investigations. We also leverage key partners in the security and intelligence community, and work closely with foreign law enforcement counterparts.

**Challenges**

However, the detection and enforcement of criminal offences related to threats to national security is subject to several significant challenges, which I will outline for you in the hope not of imposing any particular vision of the world I may have, but of encouraging continuing public dialogue and the search for solutions moving forward.

First among these are the challenges posed by the very technology that allows ISIL and like groups to enjoy the reach that they do. I have been spending a great deal of time trying to raise awareness of this topic lately, as you may have heard or read.

Ours is an information based business.

We need to know who the next crop of teenaged burglars are; which kids are being abused; who is walking the streets at three in the morning slashing tires or carrying pry-bars and screwdrivers; and, who is sitting in a basement reading jihadist propaganda.

Good information is gold in my business and it doesn’t just fall in your lap. We need people to give it to us, and if they can’t or won’t, we need a way to get it when certain conditions are met.

What has proven difficult is the ability for us, for lawmakers, for society, to reconcile the need to have a robustly Charter-compliant way to access information with the safeguarding of a right to privacy which occupies a place of paramountcy. Today we will abide nothing that can remotely be seen or understood to threaten our freedom, including our privacy. Privacy has become the crusade of those who would have us live in their textbooks. Privacy is an essential component of our freedom, no question, but I argue our privacy must be thoughtfully balanced against the very communal dimension and nature of our existence. We need to consider to what degree privacy is meant to equal anonymity.

It’s a very difficult proposition to bring traditional criminal justice strategies to bear in a place where anonymity is protected. Thinking back to my days as a general duty police officer in Chilliwack, I couldn’t keep the people of my community safe and do my role as a police officer if I didn’t and couldn’t know who they were – if they went about their business in the community of Chilliwack, day-in-day-out, with masks on, or wrapped up in sheets, or driving vehicles without license plates, or their plates were covered up, or using phone numbers that could never be looked up or living in houses that didn’t have addresses, on streets without names – I couldn’t do the job of policing in that context. But this proposition becomes infinitely more difficult for society to accept when it comes to the internet.

Communication, as you are all aware, is able to become increasingly inscrutable through, for example, encryption. This is commonly referred to by law enforcement as the “going dark” problem. This is not a new problem.

I used to chase bikers out on the West Coast, the Hells Angels in particular, they were very difficult to catch, because they had, for all intents and purposes, themselves gone dark. Not technologically; they had gone dark in their behaviours. They wouldn’t talk on the phone, they wouldn’t write criminally relevant communications to one another on their computers, they wouldn’t write criminally relevant communications on paper. When they would go and talk dirty business, they would go off into a field and whisper into each other’s ears. So effectively they’d gone dark on us.

The solution couldn’t have been to make them use their phones. That’s not going to work. We’re not going to create a law that says, ok, if you are organized crime, you must use your communication devices so that the police can intercept them. We had to change our thinking, and we had to engage key partners in communities with regulatory powers, with other powers to be able to bring the full weight of organized society to bear on criminal conduct that was going unchecked. And in the end, we were able to bring some successful and meaningful prosecutions against them.

A similar approach needs to be brought to the challenges posed by the going dark phenomenon. That phenomenon transcends technology, and the solution to the problems posed by it rest not only in finding new technological tools to see beyond the veil, but by encouraging the partnerships and trust that need to exist to surmount the issue.

Beyond going dark, though, exists the more basic problem of acquiring the information we would, in the example above, have acquired through querying uncovered license plates, or checking the phone book to see who was registered to a particular number. That basic name and address info is also made more difficult to achieve through adherence to the protection of anonymity. In that respect, we also, and perhaps more urgently, need new tools, to be able to enforce the criminal law quickly and efficiently, in a way consistent with Canadian values and the Charter of Rights and Freedoms. So I encourage conversation, particularly among groups like the one here today, in this respect.

Another investigative challenge that becomes particularly acute with the geographical breadth of ISIL and ISIL-inspired individuals is that of evidence collection abroad. While we continue to leverage our personnel and excellent partnerships with foreign law enforcement and intelligence services, collecting evidence against individuals in states which are often either failed or failing is a significant challenge. It is often difficult to build criminal cases against high-risk travellers based on their foreign activities.

Equally challenging in this respect is the need to be aware of, and aggressively question, the justice systems in states in which evidence may be located to ensure the proper respect for human rights that is enshrined in our Canadian system.

Finally, for today’s purposes, we are faced with challenges in proceeding with charges against individuals due to the difficulty, if not impossibility, of using intelligence provided to us as evidence in a criminal proceeding.

Again, this is not a new phenomenon. Intel evidence has long been seen as a thorn in the paw of the security and intelligence operations. At the risk of being labelled a bit of a Judas, though, let me say this: it's not as bad as some would have us believe. Recent successful prosecutions have demonstrated our ability to overcome many of the challenges, and those that remain, significant though they may be, are best overcome by a change in practice, not necessarily a change in law.

**Moving Forward**

Turning back to the particular issue of ISIL, we cannot lose sight of the fact that opportunities exist and are being leveraged to counter the threat. Notwithstanding the challenges I’ve set out, the security and intelligence community has embraced collaboration and collective action as the best practice for managing threat. The whole-of-government approach has met with substantial success and continues to evolve. Government agencies and departments coordinate operationally as never before, without any formally prescribed structure for collaboration.

The speed at which national security threats evolve today means that it is increasingly necessary to act before a threat becomes a crisis and before harm is realized. Canadians expect as much. Certainly, some changes in authorities could be and have been beneficial. But what is even more necessary is continually increasing coordination, even earlier in the threat identification process, and a more open and horizontal approach to strategy development and action. In this way we enable the Government to make better decisions on managing threats, with a high degree of confidence, employing all of the elements of Canadian power.

Ultimately, our goal is to manage threats effectively, efficiently, and in a manner consistent with Canadian values.

Threat management is owned collectively and therefore must be practiced collectively.

Working together, the community can develop a broad array of response options to manage a salient threat at any stage of development. This spectrum of response can become greater than the sum of its parts – that is, some options only become available through cooperation, such as joint operations.

Domestic counter-terrorism investigations have been the most prominent beneficiary of the whole-of-government approach to date. Certainly, de-confliction and operational coordination with CSIS, CSEC and other national security partners has become standard practice for the RCMP’s national security investigations. The challenge remains how to effectively extend that to other threats to the security of Canada, and to other, non-security agencies. Leveraging the niche capacities of key agencies to manage threats is something the community does today, but can do better.

Increased coordination requires increased openness and earliness from all actors. Recent initiatives, such as the multi-agency National Security Joint Operations Centre, demonstrate this ability to collectively assess the threat, and then, collectively act towards the greater good.

This truth should create an imperative on all to share early, widely and robustly, within established legislative frameworks. No agency should independently collect, evaluate and formulate a response to intelligence when a major threat to public safety or national security is at stake. The community is increasingly recognizing that a whole-of-government response ensures that there is a rigorous and careful approach to managing threats. This is not just about how to address threats, but also when.

No one agency, including the RCMP, should be responsible for the Government’s approach. Indeed, not only should the Government and its agencies be responsible for the approach: the private sector has a part to play as well. Academia participates by sharing ideas and contributing to solutions; private industry contributes by being alert to threat cues and participating in initiatives that help in stopping criminals from being able to resource their criminal activities.

**Conclusion**

While challenges and room for improvement remain, Canada’s approach to security and to the threat posed by ISIL is sound. The mechanisms and machinery of its approach are built from the common law and set out in specific statutes, policies and practices. Commissions of Inquiry and other review bodies have consistently recommended supporting and extending existing practices.

A criticism sometimes made in respect of the current approach is that we, as a community, suspect a threat may exist but do not act on it. This is likely valid but it is not a negative – just the opposite. The community’s inability – or lack of willingness – to move against a distal threats is, in fact, key to who we are as a society. It is vital that assessments of threats, including the assumptions on which they are based, be challenged before action is taken, to ensure that they are as comprehensive and objective as possible.

The security and intelligence community’s powers are invasive and their use, in many instances, has a significant impact on a person’s ability to enjoy life, liberty and the security of their person. These powers understandably attract considerable demands for oversight and review from Canadians. Their use must be principled. That is to say, proportionate, reasonable, consistent and transparent enough to allow people to explain their actions.

The community, and the RCMP, have come a long way in developing approaches to threat management. The right next step is to build on the progress to date, reinforce the system and implement continuous improvements that will keep Canada safe and uphold the rights of all Canadians.

Thank you.

–30–