The John Tait Memorial Lecture
CASIS Conference
15 October 2004

CSE's Post-9/11 Transformation

Thank you Tony.

Let me begin by saying I was honored to be asked to deliver the John Tait Memorial Lecture this year.

For me, as for most public servants of my generation, John's name is synonymous with the highest standards of public service. I got to know him when he and I worked at the Privy Council Office in the mid-1990s. He was a person who had an extraordinary intellectual capacity and a deep understanding of this country, its federal system of government, and the Canadians whose lives are dedicated to public service. His wisdom and leadership are greatly missed.

Following his time as Deputy Minister of Justice, John moved to the Privy Council Office where, as the Government's Security and Intelligence Coordinator, he was the Deputy Minister responsible for CSE's policy and operations. In this capacity, he worked closely with CSE and helped prepare the organization for the future in many important ways.

It was under John's direction, for example, that CSE began work to formally and comprehensively analyze its mandate, authorities and policy structure – work that laid a critical foundation for the development of the legislation for CSE following 9/11. And it was under John's watchful eye that CSE initially established its critically important professional relationship with the then newly-appointed CSE Commissioner and his Office.

One of the strongest connections that CSE has with John, and one that will endure, is our values framework.

As many of you know, John led the federal government task force on public service values and ethics, which issued a landmark report in 1996, entitled "A Strong Foundation".

Shortly thereafter, CSE adopted its own values framework. While the organization was fully engaged in developing a CSE-specific framework based on the work of the task force, it was because of John's leadership and support that the result was a framework that is now an integral part of CSE's organizational culture. Needless to say, given John's involvement, lawfulness is at the top of the CSE values list –and a value that is absolutely critical as we

implement new authorities and programs in this post 9/11 environment.

All of this to say that John had an enormous positive influence on CSE, as well as on the broader public service, and it is a privilege to deliver, as CSE's current Chief, this lecture in memory of him.

However, before accepting the invitation to speak, I had to do some serious thinking about whether I could say enough about CSE to make this meaningful for you.

As you know, throughout our history, which now spans nearly 60 years, CSE has generally been portrayed as an "ultra secret" organization and, until recently, not much was said about it in public. Indeed, as Margaret Bloodworth pointed out to this Conference two years ago, when she spoke as Deputy Minister of National Defence after I had chaired one of the panels and had made some introductory remarks about CSE, it was not very long ago that even an appearance by the Chief of CSE in this type of public venue would have been out of the question. And to have the Chief not only appear, but actually say something, was a strong sign of rather fundamental change!

The new equation for CSE is, in my mind, quite simple. To be effective as an organization, CSE needs the right authority structure. By that I mean, to do our work effectively in the current security environment, CSE needs a clear legal and policy framework that enables us to deliver on our mandate with the right level of accountability.

This is only possible in the current context if CSE has the support of parliamentarians and Canadians – which requires us to share more information about CSE than we have shared in the past. This is the path we have been on for the past three years, and my acceptance of the invitation to speak with you today is, in my mind, simply another step in this direction.

That said, as I know this audience will appreciate, there are limits to what can be said publicly about an organization like CSE. Generally speaking, over the past three years, we have shared a great deal more information with parliamentarians, and other interested Canadians, about what we do and why. But an organization such as CSE simply cannot say much publicly about how we do what we do, because revealing our capabilities and methods would very quickly render us less effective.

So I am hopeful today that this audience, which is obviously a sophisticated one, will understand that I will be speaking within certain parameters as I provide you with my views on how CSE had to change, and has changed, to meet the realities of the post 9/11 world.

It is important for you to understand at the outset that CSE's mission has two complementary dimensions – to provide and to protect information through leading-edge capability.

For almost 60 years, CSE has been doing this by maintaining cutting-edge expertise in cryptography, or code making, and cryptanalysis, or code breaking. Together these two related disciplines are called cryptology, so CSE is Canada's national cryptologic agency.

Esoteric words aside, the simple point I wish to make is that CSE is structured and organized to both collect and protect information. In offensive mode, our job is to go out into the global information infrastructure and collect information relevant to the Government's foreign intelligence priorities. In defensive mode, our job is to help protect the government's communications and information systems, with top priority placed on those that are most critical to safeguarding our national security.

Reflecting this, CSE has two business lines – Foreign Signals Intelligence (or SIGINT) and Information Technology Security (or IT Security).

Let me start with IT Security. In this area, CSE's mandate is "to provide advice, guidance and services to help ensure the protection of electronic information and information infrastructures".

Our niche is at the highest end of technology. We maintain the highest level of technical expertise in the Government and in the country. We provide, for example, the highest grades of cryptography – the codes that protect the Government's most sensitive communications including, for example, military communications.

The simple fact is that we now live in an age in which our security and prosperity have become increasingly dependent on the secure movement and storage of information. Effective protection of critical information and infrastructures is now essential to the nation's security.

In recognition of these new realities, the National Security Policy released in April 2004 commits the federal government to strengthening its approach to cyber-security. As the policy points out, the threat of cyber-attacks is real, and the consequences can be severe.

To achieve a more proactive approach and to keep pace with the efforts of key allies, the Government is thus strengthening its capacity to predict and prevent cyber-attacks by making substantial improvements in the quality of its threat and vulnerability analyses. It is also strengthening its ability to defend its systems and respond to incidents and attacks.

CSE's IT Security program will provide the leading-edge technical expertise required to accomplish these policy objectives. To help us do this, we have recently received significant additional resources from the funding allocated to address national security issues in Budget 2004.

As a result, CSE's IT Security business line is now in a growth phase and positioning to meet the cyber-security challenges of the future. This is a significant component of our organizational focus right now and, in my view, CSE's role here is absolutely critical –

to both the successful implementation of the new National Security Policy and the longer-term security of our nation.

I would like to stress here that much of our critical infrastructure – power grids, hospitals, businesses, key economic institutions and the like – now relies on cyber capabilities. Since the private sector and other levels of government own most of this infrastructure, the national security implications in this area certainly cannot be effectively addressed by the federal government acting alone.

It is precisely for this reason that, as announced in the National Security Policy, the federal government will "convene a high-level national task force, with public and private representation, to develop a National Cyber-security Strategy to reduce Canada's vulnerability to cyber-attacks and cyber-accidents". Public Safety and Emergency Preparedness Canada is now making preparations for this exercise, and the task force will be launched in the coming months.

Some of our key international partners, most notably the United States with which we share much common infrastructure, have already conducted national exercises like this, and have developed national strategies to secure cyberspace and protect their own

critical infrastructure. From my perspective, it is essential that we take this step as well.

As we move into our cyberspace future, I would hope that future CASIS events would find a more prominent place on the agenda for discussions about cyber-security issues. As I say to my colleagues, this aspect of our national security is far too serious to be left to technical conferences alone. It needs strategic-level dialogue too, and I believe that CASIS can make a very important contribution in this area as it has in many others.

Let me now turn to CSE's SIGINT business line and the way it has evolved since 9/11.

CSE was created shortly after WWII and, for the next four and a half decades, its SIGINT culture and capabilities were Cold War oriented. Its SIGINT efforts were directed primarily against the Soviet Union, a target that was large, slow moving and fairly predictable with a familiar hierarchical organization, a worldwide diplomatic presence and a stable cast of allies and supporters.

The greatest challenge during this Cold War period was cryptography. Sensitive Soviet communications were layered with

sophisticated cryptography or codes, and it was hard to get at content even with the most sophisticated techniques.

Following the end of the Cold War, CSE began to shift its focus. Over the next ten years, the organization produced a more diverse range of intelligence products, serving a broader base of Government organizations.

This post-Cold War evolution allowed CSE to sustain its highly skilled and professional workforce, as well as its solid relationships with key allied agencies abroad but, when the events of 9/11 took place, CSE was nevertheless facing a tough scenario.

Simply put, in a kind of perfect storm situation, the 1990s saw the global revolution in communications technologies, resource shortages and the lack of an updated authority framework combine to create a serious erosion of CSE's SIGINT capabilities.

Let me first explain how the legal environment had become problematic for CSE.

Many of you will know that Part 6 of the Criminal Code protects "private communications", a term whose definition includes any

communication that would have a reasonable expectation of privacy and that originates or terminates in Canada. This provision affected CSE in two ways.

The first impact was obvious. CSE could not intercept a communication that an intelligence target abroad sent to or received from Canada. In the context of security intelligence, where the communications of a terrorist or a terrorist group located abroad were targeted, this restriction meant that CSE could not provide intelligence in a situation that could pose a very serious threat to this country – a known terrorist group abroad communicating with a member or accomplice in Canada.

For example, if a known member of al Qaeda operating abroad communicated with someone in Canada, even if the person in Canada was a foreign operative of al Qaeda, Part 6 of the criminal code prohibited CSE from intercepting the communication.

The second impact was less obvious, but more sweeping. In the new technological environment, the variety, velocity and volume of communications was expanding exponentially and communications were moving from place to place in a myriad of unpredictable ways.

Yet CSE could intercept a communication only when it could actually demonstrate that neither end originated or terminated in Canada. In other words, CSE had to be able to demonstrate, before it acquired a communication, that both ends of the communication would be foreign.

Further, in the new environment, communications were moving in complex bundles that had to be mapped and analyzed before acquisition was even possible.

Yet, based on in-depth legal analysis by the Department of Justice, the Criminal Code prohibited CSE from doing initial analysis on bundles or systems where there was any chance that these might contain the communications of a person in Canada.

In this context, the bottom line for CSE was that, in the new communications and security environments, its collection efforts were becoming much less effective.

I should point out here that our key international SIGINT partners – the United States, the United Kingdom, Australia and New Zealand – had already found ways to deal with this issue to ensure

the longer-term effectiveness of their SIGINT enterprises while still protecting the fundamental right to privacy of their citizens.

When the events of 9/11 took place, resolving this issue thus became the crucial one for CSE as we looked to fully engage in the global war on terrorism with our international partners.

In the years leading up to 9/11, another key part of the reality for CSE was that the technological revolution had moved into very high gear.

CSE's foreign intelligence mandate, under executive direction before 9/11 and now under the National Defence Act, is "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence in accordance with Government of Canada intelligence priorities".

"Global information infrastructure" can accurately be thought of as the whole of the modern communications landscape, where communications move over every possible platform and medium in the electromagnetic spectrum to get from one point to another.

Some of you will have heard or may even have used the "vacuum cleaner" analogy to describe how SIGINT agencies operate – we are reported to suck up all communications. But that is not how the business works today.

What we really do is use our brainpower and the latest in technology to selectively hunt for what we are looking for within virtually endless communications haystacks and electronic highways, all of which are in continuous flux.

With respect to brainpower, CSE has always had an incredibly talented workforce that thrives on challenge. We have computer scientists, engineers, mathematicians and other technical experts who live at the cutting edge of changing technologies. We have analysts who can track down difficult communications and analyze meaning and nuance.

Our workforce is technologically savvy, linguistically savvy and national security savvy. Simply put, it has always been our greatest asset.

With respect to technology, CSE's success has always been based on its ability to adapt to the changing environment by applying the

latest research and technology. Since everything is changing at such a staggering pace these days, this requires the constant upgrading of our inventory of hardware, software and other equipment.

By late 2001, as we faced the implications of 9/11, the resources needed to keep up – human as well as technical – were in too short supply at CSE. Our workforce was thinly spread and we were hurting in terms of keeping pace with changing technologies. We needed financial investment to move ahead.

CSE had given visibility to its financial issues in the budgetary process in 2000 and 2001. As a result, the need for long-term investment in SIGINT was already recognized.

However, the list of competing priorities was long and, while CSE did receive some additional program integrity funding through the budget process for fiscal years 2000-2001 and 2001-2002, it was only a portion of what was needed to sustain our capabilities; and the prospects for longer-term investment were uncertain.

Taking all of this into account, the scenario we were facing in September 2001 was a tough one. We had talented people with the

skills required to meet the demands of the 21st century, but we did not have enough of them. And we did not have the authority structure or financial resources needed to respond effectively to the events of 9/11.

Immediately after these events, there was never any doubt in my mind that this event was a transformational one that would change global politics, US foreign policy and Canada-US relations in some rather fundamental ways. What also became certain to me, within a very short period of time, was 9/11 would also result very quickly in a fundamental change to the basic scenario for CSE.

In retrospect, it is clear that nothing could have cast a harsher light on the limits of CSE's authorities and resources than 9/11. In this context, the Government moved very quickly, taking some decisive steps to make it possible for CSE to move forward, and to effectively engage the global campaign against terrorism.

With respect to CSE's authorities, the vehicle for change was Bill C-36, the Anti-Terrorism Act. As part of this initiative, the National Defence Act was amended to include legislation that put CSE on a statutory footing and allowed it to more effectively access the global information infrastructure in the current

technological environment, while also establishing clear limitations to protect the Charter right to privacy of Canadians and persons in Canada.

Under the legislation, as previously, CSE may target only foreign entities abroad. But the legislation takes account of the reality that, if it is to be effective in the current environment at acquiring the communications of foreign targets abroad, CSE may incidentally intercept a small volume of communications with one end in Canada.

At the core of the legislation is the judgment that, if a legitimate foreign intelligence target communicates with someone in Canada, then the privacy rights of the person in Canada, while they need to be respected under very strict rules, should not automatically be allowed to prevent the Government from collecting vital intelligence.

The legislation operationalizes this approach through a specific mechanism that allows CSE, in the course of intercepting the communications of legitimate foreign targets abroad, to acquire incidental private communications as defined in the Criminal

Code. That mechanism is an authorization by the Minister accountable for CSE, the Minister of National Defence.

To be crystal clear on this, the legislation never allows CSE to direct its activities at individuals located within the 12-mile limit that defines Canadian territory, whether these individuals are Canadians or foreigners. Nor does it allow CSE to target Canadians abroad, defined in the legislation as Canadian citizens or permanent residents. But the legislation does allow CSE, in circumstances specifically authorized by the Minister in writing, to intercept foreign communications in situations where private communications may incidentally be acquired as well.

The key conditions that must be satisfied before the Minister issues an authorization are that all interceptions must be directed at foreign entities located outside Canada, that the expected foreign intelligence value justifies the effort, and that satisfactory measures are in place to protect the privacy of Canadians and to ensure any private communication acquired by CSE is used or retained only if it is essential to international affairs, defence or security.

Specific measures are now in place to make sure CSE complies with these conditions, and has robust procedures in place to protect the privacy of Canadians and persons in Canada.

- First, a legal team assigned from the Department of Justice works closely with our senior executive team, policy group and front-line managers and staff to ensure that our procedures satisfy all legislated requirements.

- Second, we provide extensive direction to employees in all areas so that they are well equipped to act in a way that respects the legal framework; and we have internal processes in place, including active monitoring, to ensure that any weakness in procedures, or in their application, are detected right away.

- Third, the CSE Commissioner reviews CSE's activities including, specifically, those under ministerial authorization, and he does so with full access to our staff and our databases.

- And finally, we are subject to review, and indeed have been reviewed on two occasions, including once since our new legislation came into effect, by the Privacy Commissioner.

CSE is very focused on operating within its legal framework for two reasons. The first one relates to our values. Consistent with the values framework I spoke about at the beginning of my remarks, the value of lawfulness is deeply instilled in our workforce.

The second reason is pragmatic. CSE knows that doing anything outside our legal framework would have a devastating effect in terms of undermining the confidence of our Minister, of Parliament and of Canadians, confidence that is essential to our success.

Beyond these adjustments to its authority structure, CSE has received significant resources for SIGINT to help deal with the current technological environment and address the new security agenda.

In the first wave of post-9/11 investment, we were provided with substantial in-year investment for technology and further investment in the December 2001 Budget to build longer-term capabilities, as part of the broad package of initiatives and investments to strengthen the security and intelligence community.

Over the course of the following two years, as we strengthened our capacity to provide intelligence that contributed to Canada's national security, including intelligence about terrorist organizations and the proliferation of weapons of mass destruction, we developed a much better understanding of what it would take to be successful.

As a result, we were able to put forward specific proposals with detailed resource analysis in the context of Budget 2004 and the development of the National Security Policy.

Consistent with the commitments made in this policy to strengthen intelligence collection and to place greater emphasis on security intelligence, CSE has recently received a second wave of additional investment for SIGINT from the funds set aside in Budget 2004 to address security issues. CSE's SIGINT business line, like its IT Security business line, is thus still in a growth phase and positioning for the future.

Of course, the new investments in SIGINT and IT Security require serious management to ensure CSE delivers well in terms of value for money as well as effectiveness. To this end, we have put in place all of the pillars of the Government's modern

comptrollership program, including financial processes, performance measurement and risk management.

As we implement our new scenario and continue to place greater emphasis on the national security agenda, it is vital that we continue to strengthen the effectiveness of our relationships with key partners, both domestic and foreign. In my mind, in the current context, nothing less than perfect collaboration is acceptable.

Two relationships that CSE has worked particularly hard on over the past couple of years have been our partnerships with the Canadian Forces and CSIS. CSE and elements of the Canadian Forces have worked together quite well for decades but, over the last year, we have developed a new operational model to more closely integrate all of our SIGINT operations under CSE management and direction.

This model is now being implemented, and will ensure CSE can better support Canadian Forces' activities in the field and, at the same time, can draw on the capabilities of the Canadian Forces for national purposes.

CSE has also worked more closely with CSIS since 9/11. We now maintain a much stronger shared focus on terrorism and other security challenges, and we collaborate more closely on many levels. I expect this relationship will continue to strengthen in the years ahead as our two organizations continue to implement a more collaborative culture in which active teaming in pursuit of common objectives is the default position.

More broadly, CSE also works far more closely with a number of other Government departments and agencies in support of national security priorities, including the Privy Council Office, Foreign Affairs and the new Department of Public Safety and Emergency Preparedness.

Internationally CSE has had, for decades, particularly close operational relationships with its counterpart agencies in the U.S., the UK, Australia and New Zealand. Our agencies share not just intelligence, but also technologies and expertise that are key to collecting, processing and analyzing foreign communications to derive intelligence. We exchange personnel and engage in joint operations built on collective efforts.

Of particular importance is our relationship with our American counterpart agency, the National Security Agency or NSA. At all levels this cooperation is close and productive.

CSE and NSA share intelligence, tackle common problems posed by changing technology and track threats to our collective security. This partnership provides Canada with invaluable access to American intelligence and technology.

While CSE is, by far, the smaller partner in this relationship, both sides derive significant benefit from it. Indeed, at this juncture, the sharing of some of CSE's unique represents a significant element of Canada's contribution to the global war on terrorism.

Finally, I would like to comment on another relationship that is critically important to CSE – our relationship with the CSE Commissioner. The Right Honourable Antonio Lamer, former Chief Justice of the Supreme Court of Canada, was appointed as CSE's second commissioner in June 2003.

The mandate of the Commissioner under the National Defence Act is to review CSE's activities to ensure that they are in compliance with the law; to inform the Minister of National Defence and the

Attorney General of any activity that he believes is not in compliance with the law; and, in response to complaints, to conduct any investigation he considers necessary.

The Commissioner reports annually on his activities and findings to the Minister of National Defence, who makes this report available to Parliament. To date, the Commissioner has issued eight public reports in which he has stated that the activities of CSE he has reviewed during the year were conducted lawfully and were not directed at Canadians or any person in Canada.

In addition to his public reports, the CSE Commissioner also submits classified reports to the Minister on a variety of issues of the Commissioner's choosing. To date approximately 30 of these reports, covering both SIGINT and IT Security activities, have been delivered, all based on detailed analysis of CSE programs and activities. Again, none of these reports have identified unlawful conduct on the part of CSE.

The highly professional relationship that has been established between CSE and the Commissioner's office helps facilitate this independent review. By law, the Commissioner has full access to the information, documents and databases he requires to conduct

comprehensive reviews of CSE's activities. In support, CSE provides the Commissioner and his staff with detailed briefings, and makes its workforce available to respond to questions.

Over the years, the Commissioner's staff has developed a detailed understanding of CSE's mandate and operations. When the Commissioner reports to the Minister, he therefore does so on the basis of a very solid base of information about what CSE is doing and how it is doing it.

I want to stress here, once again, that the results of all of the Commissioner's reviews are critical since, to be successful, CSE needs the trust and confidence of the Minister of National Defence, as well as trust and confidence of Parliament and Canadians. So operating within exactly the right parameters is something CSE cares about every day.

Similar considerations will, of course, apply with respect to the National Security Committee of Parliamentarians once it is set up. Since 9/11, CSE has appeared before several Parliamentary Committees and has hosted two of them at CSE. Obviously, a more in-depth dialogue with parliamentarians will be possible with

the new committee once it is set up to receive highly sensitive information.

CSE looks forward to engaging the new committee, and I am confident that this engagement will translate into further comfort on the part of both parliamentarians and Canadians that things are on track at CSE.

Adding all of this up, I believe it is fair to say that CSE has had a lot on its plate over the past three years, and still does. We are now under more pressure to deliver our SIGINT and IT Security products and services than at any time in our history, and we are delivering them at the same time that we are growing and changing. More has been given to us and more is expected of us. And we have a clear and important place at center stage in helping to deliver on the Government's National Security Policy.

While some of this is daunting and much of the transformation journey still lies ahead of us, I have to say I am proud of how my organization has responded over these past three years since 9/11 – the SIGINTers, the IT Security personnel and those who support them. Simply put, having started at CSE only 5 weeks before 9/11, it has been a privilege for me to lead such a talented group of

Canadians who are building the kind of operational capabilities and organizational strength that will be needed to help Canada face the national security challenges ahead of us.

Thank you for the opportunity to speak to you today. And good luck with the remainder of the conference.