Remarks by Director David Vigneault to the Centre for International Governance Innovation

From: Canadian Security Intelligence Service

Speech

Ottawa - February 9, 2021 - Good afternoon everyone. It's a pleasure to be here with you today. I recognize the challenges of organizing events like this in our new normal and would like to express my sincere gratitude to the Centre for International Governance Innovation for doing so. It's a bit unusual for me today as the tables have turned. You can see me and I cannot see you. Usually, I'm the one on the outside looking in.

I have often commented on the need for a sophisticated dialogue on national security issues - one framed in a Canadian context. These issues are far too important to be left to the agencies alone and that is precisely why we need you to be involved. We need to engage with each other more, break down traditional siloes, and integrate our thinking. I am pleased to see that CIGI has recently launched a research project that will serve to begin addressing this gap in a meaningful way.

There is a lot of uncertainty in our world today, much has changed at such a rapid pace. Undoubtedly, this will continue into the foreseeable future.

The COVID-19 pandemic has had a profound impact on every aspect of our lives. Despite this stress, CSIS remained vigilant of national security threats, both old and new, and carried out its mission to protect Canadians. As all of us adjusted to the new environment, so did threat actors. CSIS pivoted in part by stepping out of the shadows to shine a brighter light on threats to Canada's national security.

The fluid and rapidly evolving environment created by COVID-19 has created a situation ripe for exploitation by threat actors seeking to cause harm or advance their own interests. With many Canadians working from home, threat actors are presented with even more opportunities to conduct malicious online activities.

For instance, we've seen the continued use of online platforms by violent extremists to recruit others and to spread their hateful messaging, anti-authority narratives and conspiracy theories about the pandemic to rationalize and justify violence. We are also seeing an increase in the exploitation of cyber tools to steal sensitive information, conduct ransomware attacks and cause disruption. In addition, we remain aware of the efforts of state adversaries to spread disinformation about pandemic responses in an attempt to discredit government efforts and diminish confidence in vaccine rollout efforts.

With the world becoming ever smaller and more competitive, states are naturally seeking every advantage to position themselves as leaders in the global economy.

As a result of this competitive thirst, hostile state actors seek to leverage all elements of state power to advance their national interests. While not new, this has accelerated during the global pandemic and will continue to do so as we attempt to emerge from an event that has shattered national economies.

From a national security perspective, the threat from hostile activity by state actors in all its forms represents a significant danger to Canada's prosperity and sovereignty.

For instance, espionage can have a profound impact on the security of our research and development, and ultimately, the success of our companies. By subverting our ability to innovate and commercialize research, espionage results in lost jobs and diminished economic growth.

Foreign interference, on the other hand seeks to undermine our institutions, threatens our democratic system and our citizens. Above all, this activity erodes our sovereignty and undercuts our societal norms.

Together, this one – two punch contributes to a complex environment full of other threats.

With that in mind, I would like to turn to providing you with an update about the threats we are currently facing.

Violent extremism continues to represent a deeply concerning threat to public safety, and a significant area of focus for CSIS.

The threat landscape surrounding religiously, politically, or ideologically motivated violent extremism continues to evolve and has increased in complexity. Threat actors who commit violent acts are more often no longer influenced by a singular and definable belief system, but a range of very personal and diverse grievances and narratives.

Today, threat actors leverage a range of readily available communication tools and platforms that enable them to communicate securely with one another. They use these tools to spread and amplify extremist messaging, recruit others, and finance and plan activities all without getting off their living room couch.

For example, we've seen Canadians move from supporting Daesh to violent misogyny within a short period of time.

CSIS is seeing a rise in the threat from ideologically motivated violent extremism or IMVE. Indeed, since 2014, Canadians motivated in whole or in part, by their extreme views in this sphere have killed 21 and wounded 40 on Canadian soil. In 2019, two IMVE groups were added to Canada's list of terrorist entities for the first time, with another four being added just last week.

This issue is broad and complex. It represents a societal problem that will require a holistic approach involving all elements of civil society to address it. As with religiously motivated violent extremism, CSIS plays a key role, alongside intelligence and law enforcement partners, in that broader government response.

While violent extremism remains an ongoing threat to our safety and a significant preoccupation for CSIS, the greatest strategic threat to Canada's national security comes from hostile activities by foreign states. While we focus on protecting our citizens, we bear witness to hostile states leveraging all elements of their state apparatus to advance their national interests at Canada's expense.

Historically, spies were focused on obtaining Canadian political, military and diplomatic secrets. While these secrets are still attractive, today our adversaries are more focused on intellectual property and advanced research held on computer systems in small start-ups, corporate boardrooms, or university labs across the country.

State cyber actors will continue to target sensitive and proprietary data that resides on these networks – some of which remain relatively open and accessible. They will continue to deploy tradecraft that is highly-creative and

deceptive to gain access to data that holds strategic and tactical value.

These actors are able to leverage emerging technologies such as bulk data collection or AI-powered analytics to their advantage. With full integration, they pull from common data pools to identify threats and vulnerabilities. Without strong defences to protect our citizen's data, it is easily accessed and can be used to drive the further development of AI capabilities.

For instance, in 2020, global news sources revealed that Zhenhua Data Technology which primarily serves China's military and intelligence services had been gathering sensitive data on 2.4 million individuals for several years. Approximately 20% of this data was not publically available and likely accessed via cyber-espionage.

Canadian companies, in almost all sectors of our economy, have been targeted. They have been compromised and have suffered losses from human and cyber enabled threats. CSIS has observed persistent and sophisticated state-sponsored threat activity for many years now and we continue to see a rise in the frequency and sophistication of this threat activity. CSIS actively investigates this daily, from coast to coast to coast and abroad.

In particular, I would cite Canada's biopharma and health sector; artificial intelligence; quantum computing; ocean technology; and aerospace sectors as facing particularly severe threat activity.

Emerging technologies in these sectors are also among the most vulnerable to state-sponsored espionage given that they are largely developed within academia and small start-ups. They're attractive targets because they may have less security awareness or protections in place. They are also more likely to pursue financial and collaboration opportunities, which can, and sadly are, exploited by other countries.

Our investigations reveal that this threat has unfortunately caused significant harm to Canadian companies. Collectively, it jeopardizes Canada's knowledge-based economy. When our most innovative technology and know-how is lost, it is our country's future that is being stolen.

Our adversaries do not play by globally-accepted rules.

Some countries do not reciprocate Canada's openness and support for a level playing field and others are aggressively advancing their own economic, intelligence and military state interests, at our expense. This is no longer traditional private commerce.

This is state capitalism and it creates a skewed playing field in which our private sector is always at a disadvantage.

Employees, former employees, students, professors, contractors, business associates, or any individual with inside knowledge of – or access to – an organization's systems can be targeted by hostile intelligence services to wittingly or unwittingly steal sensitive information.

An insider acting at the behest of a threat actor can compromise a system and cause damage, or open a backdoor to allow access from across the street or across the ocean. They can steal information outright, and walk it out the door on a flash drive.

It is no secret that we are most concerned about the actions by the governments of countries like Russia and China. But we should also not discount that threat activity evolves and can originate from anywhere in the world.

China is an important actor on the world stage and a partner for Canada on some important fronts. Canada and Canadians have benefited for decades from relationships with Chinese researchers, scholars, artists, business people,

and others; and our cultural mosaic is all the richer because of the presence of Chinese-Canadians across Canada, in large cities and in small towns dotting every corner of this country.

To be clear, the threat does not come from the Chinese people, but rather the Government of China that is pursuing a strategy for geopolitical advantage on all fronts – economic, technological, political, and military – and using all elements of state power to carry out activities that are a direct threat to our national security and sovereignty. We all must strengthen our defences.

I will now focus on the threat of foreign interference.

Foreign interference has always been present in Canada, but its scale, speed, range, and impact have grown as a result of globalization and technology. We are increasingly seeing social media being leveraged to spread disinformation or run influence campaigns designed to confuse or divide public opinion, interfere in healthy public debate and political discourse, and ultimately create social tensions.

Efforts by foreign states to target politicians, political parties, and electoral processes in order to covertly influence Canadian public policy, public opinion and ultimately undermine our democracy and democratic processes represent some of the most paramount concerns. Our electoral system has been shown to be resilient, but we must also work hard to keep it that way. Vigilance is the best defence.

A number of foreign states engage in hostile actions that routinely threaten and intimidate individuals in Canada to instill fear, silence dissent, and pressure political opponents. One notable example of this is the Government of China's covert global operation, known as Operation Fox Hunt which claims to target corruption but is also believed to have been used to target and quiet dissidents to the regime.

Those threatened often lack the resources to defend themselves or are unaware that they can report these activities to Canadian authorities, including us. Moreover, these activities are different from the norms of diplomatic activity because they cross the line by attempting to undermine our democratic processes or threaten our citizens in a covert and clandestine manner.

Today, I felt it was important to provide you with this update on the threat environment, given the significance of the changes. The world has changed significantly and so have the threats, in short order.

What has not changed, and must not, is how innovative and dedicated CSIS employees are. The high quality of our investigations, our analysis, the advice we provide and our decisiveness around taking action to address the threats has not changed.

However, we need to ensure that CSIS authorities continue to evolve so that they are able to address the challenges of the significantly more complex environment around us. Today's threats manifest themselves in vastly different ways than they did in 1984, when the CSIS Act was enacted.

An Act better suited for the threats of the Cold War era greatly impedes our ability to use modern tools, and assess data and information. We need laws that enable these types of data driven investigations, carefully constructed to reflect the values we share in our democracy, including assurances of robust privacy protections.

Our Act enables advice to government but limits our ability to provide relevant advice to key partners, including many of you listening today. Our Act sets technological limitations on intelligence collection that were not foreseen by the drafters of the legislation in 1984 and unduly limit our investigations in a modern era.

These are simply a few examples of the challenges of our authorities. At CSIS, we take our social license with Canadians very seriously.

Contrary to many of our adversaries, CSIS operates in a democracy governed by the rule of law, not by the law of the rulers. We strive for the best in accountability and see a healthy discussion on the expectations that Canadians have of their national security agencies, and whether the laws have kept pace, as a meaningful contribution to that accountability. We need your help as advocates and partners in this effort.

I would like to take this opportunity to elaborate further on that need for strong partnerships.

Whether we're talking violent extremism, espionage, or foreign interference, no single government department or agency can deal with these threats alone. If we want to be effective in countering modern threats, we must build strategic partnerships – within and outside government. Partnerships facilitate information sharing, consultation, the pooling of resources or expertise, and joint actions.

I'm seeing this happen in real-time with the pandemic. By sharing what we know about a number of related issues, CSIS has increased and deepened its cooperation with partners like the Public Health Agency of Canada. We're also working closely with partners like Innovation, Science and Economic Development Canada to raise awareness of foreign investments that could impact our national security. We are doing as much as we can to harden the target.

I talked about how we stepped out of the shadows during the pandemic. Immediately, we saw that Canadian universities, medical research institutes, pharmaceutical companies, and others involved in the national response to

the pandemic were facing an elevated level of risk to their cyber security. CSIS worked closely with its partners in universities, alongside the Canadian Centre for Cyber Security, to respond accordingly.

The need for partnerships also extends outside our borders, especially among the Five Eyes, the G-7 and other like-minded liberal democracies. It's only through the mobilization of like-minded partners that we can raise the cost to hostile states.

Keeping Canada safe requires a national security-literate population. By this I mean a citizenry that understands the key dilemmas Canada faces, and recognizes the need to adapt and respond in a thoughtful, meaningful, and timely way.

I encourage you to consider CSIS a partner and to contact us for information, advice, or support as your companies, universities, and associations navigate increasingly complex geopolitical waters.

You may think to yourself: "I'm not a national security person. I'm a scientist, a business person, an academic and so on. I'm not interested in geopolitics."

Well, I can say with some confidence that geopolitics is interested in you.

And it's important that you know how you can be at risk and how you can protect your interests.

When you reach out to us, you'll appreciate the expertise and dedication of CSIS employees. As Director of the Service, I take the greatest pride in the quality of our workforce. People truly are CSIS's most valuable resource.

As Canada's security and intelligence service, CSIS must reflect the society it protects. Just like the people of Canada, we're a diverse and inclusive workforce. Our diversity allows us to better understand communities and

helps us maintain the bond of confidence and trust that needs to exist between civil society and intelligence agencies. In exchange for the trust that Canadians place in us, we commit to high standards of accountability.

My remarks today have painted a picture of the key threats we all need to be aware of and have a role in countering.

I can assure you that CSIS, along with Government of Canada and international partners, are actively investigating, monitoring and, disrupting harmful threat actors when our lawful mandates allow.

This builds on active efforts undertaken by the Government of Canada to protect Canadians and their interests; for example, we have increased scrutiny of all foreign direct investments under the national security provision of the *Investment Canada Act* and there is ongoing work of the Security and Intelligence Threats to Elections Task Force to counter foreign interference against threats to elections. Moreover, we have sought to identify new sectors for focused outreach to private companies, associations and academics to help them understand how to protect their intellectual property.

I would like to conclude today, by asking some questions that I would like all of you to consider.

For instance, what are the national security implications of Canada's economic recovery post-pandemic?

What expectations do citizens have regarding how Canadian authorities should use powerful data driven technologies for the public good?

How do we prevent our data and research from inadvertently advancing hostile foreign military, intelligence and commercial interests?

These are just a few questions that we're slowly coming to ask of ourselves and of Canadians.

There is no greater responsibility for a government than the protection of its citizens. In today's dynamic threat environment, government, civil society and the private sector must work together to harden the targets and protect our national interests. I ask all of you to work with CSIS in advancing this call to action to protect the security of Canadians and the health of our economy for our future and that of our children. I'm an optimist. I know we can do it. We must!

Thank you Aaron, and everybody online for listening. I'll stop here, and I'll be pleased to take questions.

Contacts

Information
Media Relations
(613) 231-0100
media-medias@smtp.gc.ca

Search for related information by keyword: Security intelligence | Canadian Security Intelligence Service | Canada | National security | general public | speeches

Date modified:
2021-02-09