A PIVOTAL MOMENT: CSIS STEPS OUT OF THE SHADOWS TO PROTECT CANADA'S BIOPHARMACEUTICAL AND HEALTHCARE SECTORS DURING THE COVID-19 PANDEMIC

Public Service Innovation and Leadership During COVID-19

BY CATHERINE LATHEM

NOV. 23, 2020

PUBLIC POLICY FORUM

ABOUT PPF

Good Policy. Better Canada. The Public Policy Forum builds bridges among diverse participants in the policy-making process and gives them a platform to examine issues, offer new perspectives and feed fresh ideas into critical policy discussions. We believe good policy is critical to making a better Canada—a country that's cohesive, prosperous and secure. We contribute by:

- Conducting research on critical issues
- Convening candid dialogues on research subjects
- Recognizing exceptional leaders

Our approach—called **Inclusion to Conclusion**—brings emerging and established voices to policy conversations, which informs conclusions that identify obstacles to success and pathways forward. PPF is an independent, non-partisan charity whose members are a diverse group of private, public and non-profit organizations.

1400 - 130 Albert Street
Ottawa, ON, Canada, K1P 5G4
613.238.7858

ppforum.ca

@ppforumca

WITH THANKS TO OUR PARTNERS

Canada

The Wilson Foundation

LAWSON FOUNDATION

Microsoft

BY CATHERINE LATHEM

A PIVOTAL MOMENT: CSIS STEPS OUT OF THE SHADOWS TO PROTECT CANADA'S BIOPHARMACEUTICAL AND HEALTHCARE SECTORS DURING THE COVID-19 PANDEMIC

It was a world we had never experienced before. Panic surged. Questions mounted. Death tolls were rising. The killer: invisible, silent and ruthless. The weapon: a pandemic that was sweeping the globe like a tidal wave. The enemy had a name: COVID-19. The health and the economy of a world was at the mercy of this vicious viral villain. The question for governments: How do we stop COVID-19? The answer: a vaccine.

Developing a vaccine, the world was warned, could take months or even years. Health researchers and scientists around the globe began the methodical work of trying to pick apart the complex virus. The public message from world leaders was clear: collaboration was vital and countries needed to work together to fight COVID-19. The reality, though, looked different. This was a race. There was a lot of money at stake to be the government holding the key to a potential cure. Canada was no different.

What happened next would play out like a real-life spy thriller. Canadian companies and universities would be the targets of foreign espionage. Threat actors infiltrating our labs in hopes of stealing our valuable vaccine research. The situation was so dire, it would force Canada's top secret intelligence agency to step out of the shadows and warn those most at risk.

On March 23, the federal government announced the start of major investments in Canadian biopharma companies and researchers to help in the development of a vaccine. It was all part of a more than $1 billion national medical research strategy.

"We are funding nearly 100 research teams focused on rapidly developing effective methods to diagnose, treat, and manage patients with COVID-19," Canada's Health Minister Patty Hajdu said at the time.

The federal government named private-sector companies and research institutes that would share a $275-million dollar investment. AbCellera, a Vancouver-based biotech company, was at the forefront of developing antibody-based drugs to treat and prevent COVID-19. Quebec City-based company Medicago had identified a viable plant-based vaccine candidate. Considered to be one of the most advanced infectious

disease research facilities in the world, the University of Saskatchewan's Vaccine and Infectious Disease Organization — International Vaccine Centre (VIDO-InterVac) received millions to support vaccine development and clinical trial capacity. The National Research Council of Canada received $15 million to upgrade its Montreal facility. BlueDot, a Toronto based digital health firm, received funding to help the government in modelling and monitoring the spread of COVID-19.

Canada's vaccine hopes were placed squarely on the shoulders of these researchers, Prime Minister Justin Trudeau referring to them as some of the "most skilled and brightest" in the world.

There was talent and research here envied around the globe. It soon became clear just how much other countries wanted to get their hands on that Canadian research.

"We were observing this in real time. Gathering the intelligence and seeing activities play out," says Alex, a Senior Intelligence Analyst with the Canadian Security Intelligence Service's (CSIS) Espionage and Economic Security Unit. We can only refer to him and others in this story by first name to protect their identities.

"I saw activity in late March accelerating through April."

That "activity" was believed to be originating from those CSIS considered to be the "usual suspects", China and Russia. The foreign state-sponsored threats ranged from cyber-espionage to more human intelligence-based. In some cases it was foreign spies posing as researchers. The concern was they would gain access to the Canadian vaccine research themselves or try to recruit insiders. If successful, all that groundbreaking research Canadians had been working on would be stolen and used by those foreign governments to reverse engineer the vaccine. Those foreign governments would then be able to bring the product to market first. It would all mean a huge loss for not only Canadian researchers, but also Canada's economy.

"Spies are no longer wearing trench coats," says CSIS Director General of Academic Outreach and Stakeholder Engagement René Ouellette, "they're wearing lab coats."

Ouellette says some of these foreign state-sponsored companies are also seemingly "above board" investors. The problem is once the Canadian company agrees to take the funding, the investor can then gain access to the company, which means those foreign governments benefit from all that Canadian research.

"Canadian organizations should be aware of the geopolitical situation in the countries in which the companies they do business with are located," Ouellette warns, "companies in Canada want to make sure they can trust the foreign company they are dealing with."

"You want to make sure the fruits of your research are protected and that you benefit from them and that Canada benefits from them. If you're not paying attention to these licensing agreements and the legal and

regulatory environments in which your international partners are operating, you may find yourself no longer able to control your intellectual property."

As CSIS Director David Vigneault says, "CSIS is not a secret organization. We are an organization that keeps secrets." Its job traditionally has always been to protect Canadian military, parliamentary and cabinet secrets. CSIS investigators then collect highly classified intelligence that may be putting our country at risk, and share it with the highest ranking Canadians who have reached the highest security clearance. But over the years CSIS has noticed a shift.

"Traditional spy versus spy stuff still happens, of course, but now if a foreign government is interested in advancing its artificial intelligence to support its military development and research, it's not going to come after the government of Canada, it's going to come after advanced AI researchers working in places like downtown Toronto," says Ouellette.

"The pharma sector has been on our radar for a number of years but in a limited scope," Alex adds. "There has been espionage and foreign influence directed against that sector like almost all of our knowledge-based economy sectors, but this really changed when the pandemic took off. We noticed a significant increase in threat activity at unprecedented levels."

Many of the Canadian researchers being targeted by these foreign spies had no idea they were under potential attack. They needed to be warned. But how could they? Remember all of that threat activity CSIS had picked up was classified intelligence. Revealing the covert information could reveal the source of that information and that could put the source or Canada at risk. The researchers were all in private-sector companies and university labs, they had no security clearance, no commitment to keep the country's secrets. CSIS was in unchartered territory, they had to move fast, these scientists were at risk of losing everything.

"It was a race to get to these companies before our adversaries did," Ouellette recalls.

"Since Mr. Vigneault arrived as Director of CSIS in 2017, one of the things he has been talking about is how to make the service more responsive and modernized so it can build relationships and engage with private-sector, academic and NGO type sectors and be able to talk to them about the new geopolitical threat environment we're living in," Ouellette says.

The CSIS Stakeholder Engagement unit was created in November 2019 and was finding its feet, under the direction of Tricia Geddes, Deputy Director of Policy and Strategic Partnerships. It was a work in progress, when Vigneault approached Ouellette with a direct and immediate task in early 2020.

"In February, he said, you're about to get really busy," Ouellette recalls, "he said we're starting to see a lot of activity and we need to get out there and start warning our scientists and our medical researchers. They need to protect their intellectual property."

Threat activity was increasing. Critical life sciences sectors involved in Canada's COVID-19 response were more and more at risk from foreign interference and espionage. CSIS launched a nation-wide outreach effort, pulling together employees from across the country.

"We were working remotely from home at the time because of the pandemic," Jacqueline says from her Edmonton home. "It was definitely an interesting time to be joining a new team and starting a new program."

Jacqueline was the newest member of the Stakeholder Engagement team. Her job: to identify research entities, university labs and health networks across the country involved in Canada's pandemic response. She would need to assess those at the cutting-edge of vaccine and therapeutics development believed to be the most vulnerable to threats of espionage and foreign interference. CSIS intelligence and liaison officers then began a nationally coordinated effort, on the ground from British Columbia to Newfoundland, to communicate with these entities and to sensitize them to the threat.

"It was a bit of a race for us to try and figure out who all of these companies were that were involved in the area and to get to them before it may be too late."

By late March, these foreign governments were ramping up, using tactics to pilfer Canadian labs of research. Canadian security agencies working with CSIS were taking notice. That's when the Canadian Centre for Cyber Security sent out an alert to warn Canadian health organizations about cyber threats. The statement read in part:

> *"The Cyber Centre assesses that the COVID-19 pandemic presents an elevated level of risk to the cyber security of Canadian health organizations involved in the national response to the pandemic. The Cyber Centre therefore recommends that these organizations remain vigilant and take the time to ensure that they are engaged in cyber defense best practices, including increased monitoring of network logs, reminding employees to practice phishing awareness and ensuring that servers and critical systems are patched for all known security vulnerabilities."*

Enter Alex. As a Senior Intelligence Analyst, Alex usually briefs government officials with top security clearance on classified intelligence collected by CSIS investigators. This would be different.

"Our comfort zone in the Service is providing intelligence and analysis and advice to government clients, from the working level up to cabinet ministers and the PMO," Alex says, "It's a new role for me to step out of the shadows and be so public-facing."

This was a first. A pivotal move for CSIS.

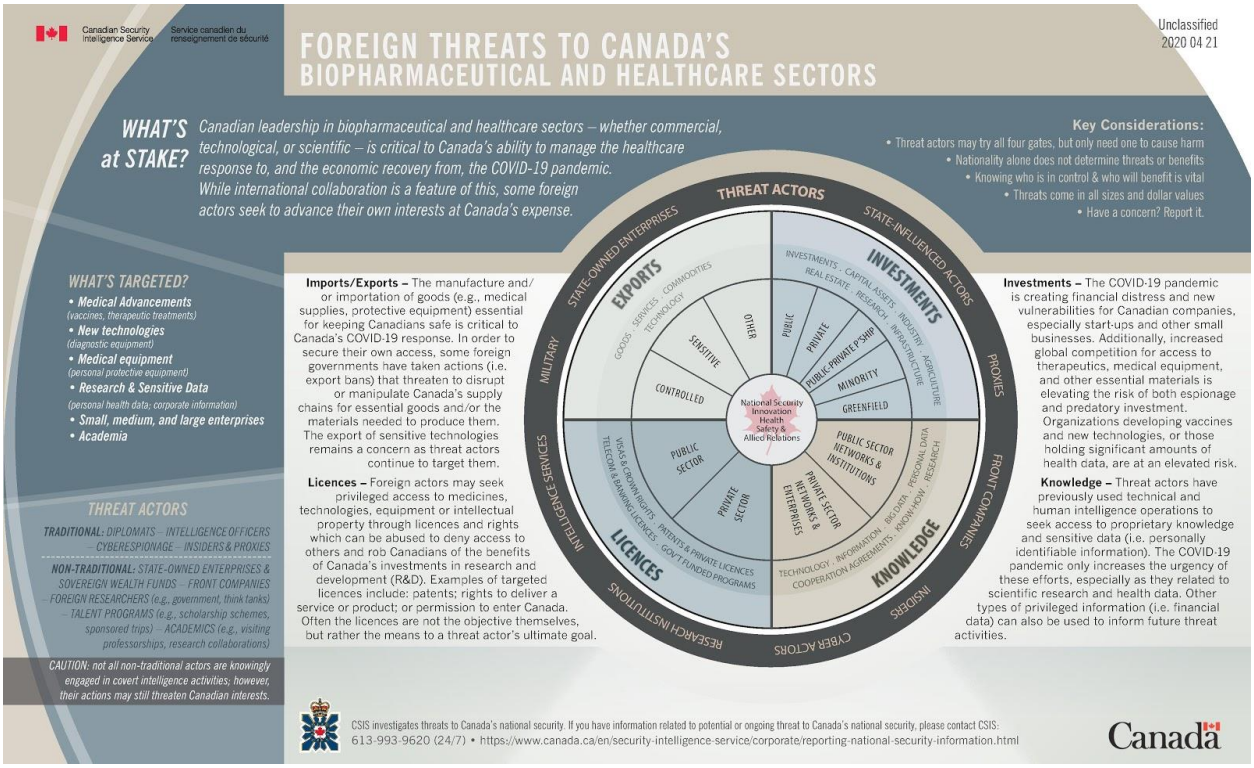
"It's a fundamental change," says Alex. "We realized how important R&D was to Canada and realized that our traditional advice to just the government was not going to cut it. The stakes involved with the lives of Canadians required us to pivot rapidly and to do something that we were not accustomed to doing."

It would mean analysts like Alex and his colleagues would have to take that "classified" information and sanitize it, making it "unclassified", so that company CEO's and lab researchers could view it.

The CSIS Intelligence Assessment Branch developed a framework called the *Four Gates of Economic Security* which highlights the ways these companies and research institutes may be targeted. It includes imports and exports, investments, knowledge and licenses.

Imports and Exports	**Investments**	**Knowledge**	**Licenses**
Foreign governments have taken actions (i.e. export bans) that threaten to disrupt or manipulate Canada's supply chains for essential goods and/or the materials needed to produce them.	Increased global competition for access to therapeutics, medical equipment, and other essential materials is elevating the risk of both espionage and predatory investment.	Threat actors use technical and human intelligence operations to seek access to proprietary knowledge, sensitive data, scientific research and health data.	Foreign actors may seek privileged access to medicines, technologies, equipment or intellectual property through licences and rights, which can be abused to deny access to others and rob Canadians of the benefits of Canada's investments in research and development (R&D).

CSIS then took those four gates and developed a "placemat" with all the information CSIS could safely share in an unclassified format to educate the private-sector targets.



Now that the Intelligence Assessments Branch and Stakeholder Engagement had translated the threats into an unclassified format and identified the biopharma companies and labs that were most at risk, they needed to alert them of those vulnerabilities. The challenge was, there were dozens of them fanned out across the country. CSIS would need to coordinate and leverage its considerable talent in regional offices spread out across Canada. CSIS employees from British Columbia, the Prairies, Ontario, Quebec and Atlantic Canada stepped in with urgent warnings to these universities and companies. They made phone calls, set up virtual briefings and knocked on doors to spread the message.

"We knew there were companies here working on things related to virology and biopharm for COVID," says Jeff, who is a Supervisor with CSIS' Atlantic Region office in Halifax. "We were pretty sure that some of these healthcare sectors and hi-tech companies would be in the crosshairs of these countries."

Jeff and his team are responsible for counter-intelligence, counter-proliferation and cyber security for Nova Scotia and Prince Edward Island. His team knew this work would be different and the threat was imminent.

"We did up a spreadsheet of all the different companies and we just started splitting them up."

Jeff says his office contacted about 20 companies and institutions in all. His counterparts in regional offices across the country were doing the same. But he says it wasn't easy. We were of course in the midst of a world-wide pandemic. They were CSIS investigators, working from home, cold calling and trying to track down unsuspecting company CEOs and university researchers, many of whom were also working from home at the time and never expected a call from CSIS.

"There was a lot of phone tag," Jeff laughs, "and then when you track them down you have to try to be able to convince them that you are who you say you are. Which in 2020 is a little harder than it was maybe 10 years ago."

Jeff says there was another obstacle, one that would force a major change on how CSIS would deliver this threat information.

"A lot of these organizations had about 20 people we would have liked to have had in these presentations. But we weren't able to present it personally because of COVID. So what we had to do, which was something really new for CSIS, was have these sort of 'digital conferences'."

Those webinars would soon become a key plank of CSIS' outreach to these vulnerable health sectors. In a time when the face-to-face meetings were impossible because of the pandemic, there were benefits and risks. The webinars, often done in partnership with the Canadian Centre for Cyber Security, would be a more widespread means of getting the message out to multiple companies, labs, researchers and stakeholders faster, but they would also live on forever over the internet.

"That was a bit of a watershed moment for us," Ouellette admits. "We quickly moved from being an organization that had more discreet conversations one-on-one, to now having larger ones, 100 to 200 participants on a webinar, and then record it and post it to YouTube. That is something new for us. We moved from a to z in the space of about three weeks."

Ouellette says that avenue to spread information also became a learning tool.

"Having the webinar on YouTube has allowed all of our investigators to know exactly what they can say when they go out and meet people and how far they can go when talking about threats facing the biopharma and life science research sectors. More importantly, it allowed the dissemination of this crucial information to as many researchers as possible."

Not only were the webinars new, so too were the social media warnings. The CSIS communications unit crafted a series of tweets aimed at the health-care sector and business community, in hopes of reaching any entities investigators may have missed.

“Our investigators in the field could point to the Twitter feed to say, look what’s already out there,” Ouellette says, “these companies aren’t spies, they’re not military, they’re scientists and researchers. Being able to point to the public communications that we were doing helped to get doors opened and phone calls returned.”

“That certainly was a game-changer for us,” Jacqueline adds. “A lot of novel approaches were taken on this with pretty significant pay off.”

These threats weren’t hollow. According to CSIS, they were concrete. They had evidence. On July 16, Canada, the United States and United Kingdom took another bold move, issuing a joint public statement about Russian threat activity.

Canada’s Communications Security Establishment (CSE) and the Canadian Centre for Cyber Security said they had technical information that Russian Hackers APT29, also known as “the Dukes” or “Cozy Bear” operating “almost certainly” as part of the Russian Intelligence Services, was responsible for malicious cyber activity targeting vaccine research entities. It’s the same group responsible for the hack that took place in the lead up to the 2016 U.S. election. This time, intelligence agencies believed the group was working to steal information and intellectual property relating to the development and testing of COVID-19 vaccines in Canada, the U.S. and U.K.

This pivot for CSIS to go public with this information to private-sector companies, Ouellette says, has paid off. He says many of the researchers had no idea they’d be targets of foreign espionage. The information, Ouellette believes, could have prevented devastating losses.

“That’s been the most rewarding part of this effort. For the most part, many of these companies and researchers were surprised to receive a call from us. These folks would say ‘I’m not a national security person, I’m a scientist, I study vaccines. What does that have to do with geopolitics with Russia and China?’ but as we started going through these discussions you could start to see the light bulb go off.”

It forced these companies and research institutes to act swiftly. They increased cyber security measures and analyzed networks and servers for vulnerabilities to protect themselves from malicious attacks. They also became more vigilant, by improving vetting processes when it came to hiring new researchers and developing investment partnerships. When a threat was suspected, these researchers, scientists and biopharma executives then started calling their CSIS contacts. The result, Alex says, was the building of relationships.

“As we established that trust, as we established that relationship, businesses started to open up. They would say ‘you know what, I actually did see something really curious last week, or we saw this unusual cyber activity’. That kind of discussion is very helpful; it allows us to investigate those threats to the security of Canada.”

“This is a fairly significant leap for CSIS,” says the former head of the Intelligence Assessment Secretariat and Privy Council Office, Greg Fyffe, “where CSIS obviously is, is knowing that they have to do this because otherwise the interests of Canada are at risk.”

Fyffe says CSIS would have been forced to analyze the critical decision to step out of the shadows, and know the dangers.

“Was there another way of warning these companies? Who are we dealing with?” Fyffe says, “Just because a company has valuable public information that another country wants doesn’t mean that the head of that company or the people working for that company are Canadian citizens or are not security risks or would be able to get a security clearance if they were up for the chance. In a sense, you are dealing with an unknown population who could include people who say, ‘well, I know some people who would really like to have this information and they might even be prepared to buy it,’ so they would have had to look at all those risks.”

“It’s easy to lock stuff up because it’s on a need-to-know basis, it’s hard to know when to release that material. The intention is to reach as many people as possible, even people you don’t know could be of help to you. You have to try and figure out how you draw any bounds around that. How do you sanitise it down to a level where the information is still compelling for people who receive it, but you haven’t given away anything that would be dangerous for the wrong people to know?”

Fyffe says this “public face” of CSIS will now be seen more in the future.

“There are more and more threats coming from foreign actors. The stealing of intellectual property, disinformation, stealing stuff that is civilian and that’s military and that’s government. There is no sign of that letting up. It follows that the agencies that are responsible for security have to keep building these bridges into organizations in the private sector that are under attack.”

Ouellette and his team admit there were challenges and learning curves in embracing this change and launching the Academic Outreach and Stakeholder Engagement Branch.

“We’ve all been doing this together from across the country, in different time zones and without ever seeing each other in-person, so that’s been interesting,” Ouellette says. “I think it’s important that our presence be increasingly known and seen in all parts of the country across a wide range of sectors of the economy and society, which also provides us with new perspectives that we may not otherwise see.”

“There is a lot of ironing out that has to happen in terms of making sure everybody still knows where their lanes are and how best to coordinate efforts,” he adds. “We’re kind of building a plane in mid-air right now but we are getting it done.”

“We’ve learned the importance of collaboration,” says Alex. “We’re going to build on this and we’re going to get better at it. I think we could even amplify our impact further if we work with the rest of government, who are all in their own mandate and within their own capacity, considering how to reach out to the public on these kinds of issues. I think we’ll be stronger as a government if we work together.”

CSIS has considered this pivot a success.

“I think we made a difference,” says Jeff.

They believe by notifying companies and research agencies, they’ve thwarted attacks. This shift isn’t over; their work is not done in protecting the health-care sector and Canadians in this ongoing pandemic.

“That’s where we’re going next,” says Jacqueline, “the supply chain, distribution, manufacturing and logistics, because we know that as fruits of the research start to be ready to come to market and be distributed to Canadians, we want to make sure that all those folks involved in that chain are aware of the risks, vulnerabilities and threats along the way. We just want to make sure there is no interference in the supply chain or tampering or cyber threats. We want to make sure that vaccines get distributed.”

“I think it was a change born out of necessity based on what we were seeing and threat activity during the pandemic but this will become business as usual for us,” adds Alex. “I think that this is the future of CSIS.”


PUBLIC
POLICY
FORUM