HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 148 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, February 6, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, February 6, 2019

● (1530)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Ladies and gentlemen, I call this meeting to order.

First of all, if I could deal with a bit of committee business, the subcommittee agreed that we would call the ministers on February 25.

Could I have a mover of that motion?

Mr. Motz, thank you.

I'll just say to colleagues and witnesses that we're likely to be interrupted, but we will try to maintain as much order as possible. If the lights start flashing and the bells start ringing, etc., I may ask permission for the committee to carry on.

One of our witnesses has flown in all the way from California. We'd like to respect that.

All we have to do is just go upstairs, anyway. I don't want to—

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Should we start with him first?

The Chair: Did Mr. Porter come in as well, from—?

Mr. Christopher Porter (Chief Intelligence Strategist, FireEye, Inc.): Yes, from Washington.

The Chair: Oh, really. Well that hardly counts.

Mr. Christopher Porter: One cold capital to another.

The Chair: Yes. Thank you for that.

I was at the Pentagon in June. I chair the joint board on defence. One year it's in Ottawa, and the next year it's there.

The Washington Capitals had just won the Stanley Cup. My American counterpart thought it was hilarious to present me with a Washington puck. I said to him afterwards, “Yeah, your Russians are pretty good.”

With that, may I call upon Mr. Porter, all the way from Washington, for his 10 minutes, please.

Mr. Christopher Porter: Thank you, Mr. Chair. I appreciate the opportunity to share FireEye's perspective with you on threats to the Canadian financial services sector and to provide an overview of how we as a company and the private sector in general work in partnership with the government to help defend that sector.

As the Chair said, my name is Christopher Porter. I'm the chief intelligence strategist for cybersecurity company FireEye. We have more than 4,000 customers in 67 countries. My testimony today will reflect the lessons we learned from responding to incidents around the world, but also intelligence we gather on threats that are specific to Canada.

In addition to working at FireEye, I am also a non-resident senior fellow at the Atlantic Council and until 2016 I served for nearly nine years at the U.S. Central Intelligence Agency, which included an assignment as the cyber-threat intelligence briefer to the White House National Security Council staff, several years in counter-terrorism operations and brief war zone service.

In addition to the 300-plus security professionals responding to computer intrusions worldwide, FireEye also has over 200 cyber-threat analysts on staff in 18 different countries. They speak over 30 languages. They help us predict and better understand the adversary, often by considering the political and cultural environment of the threat actor. We were born as a technology company, but we have these capabilities, as well. We have an enormous catalogue of threat intelligence and it continues to grow every day alongside the continually increasing attacks on organizations around the world.

We also have deep ties to Canada. FireEye appliances defend Government of Canada email inboxes every day, and we work closely with Canada's public safety institutions to keep Canadians safe by defending their networks and also by supporting investigations.

For today's discussions I will focus not only on the cyber-threats that Canada's banks, investment firms and government financial regulators face today but also the threats that they are likely to face in the near future. We live in a time of rapid change in how cyber operations are deployed, especially by nation-states. What were once spying tools used to carefully, quietly and illicitly acquire information are increasingly in the hands of military officers poised to go on the offensive and do serious damage and disruption.

This is especially true in Canada, which is often one of the first nations targeted for new types of cyber operations. Canada is a country with a high per capita GDP which makes it an attractive target for financially motivated criminal activity. It is a world leader in high-tech development, including in some niche areas of military applicable dual-use technology, so it's going to be a perennial target for foreign intelligence services. As a member of NATO with a large diplomatic and investment presence worldwide, Canada is a natural target for politically motivated retaliation from a number of actors worldwide.

Companies and individuals in Canada are also targeted by a spectrum of threat activity that ranges from deliberate, sophisticated criminal intrusions to commodity malware that spreads worldwide and only incidentally affects Canadians.

For example, in February 2017, multiple major Canadian financial institutions were exposed to risk of state-sponsored cyber-theft from North Korea. At that time, the Polish financial supervision authority took its systems offline after discovering malicious code had been placed on its web server and it was being used to redirect select targets to malicious downloads that gained control of their computer. Notably, those attackers used a white list of IP addresses to designate which individuals would receive the designated payload and multiple Canadian financial institutions appeared prominently on the targeted list. Even though the threat was in Poland, it still came home here in Canada.

Commodity campaigns, such as ransomware, crypto jacking and especially credential theft malware constitute a significant threat to Canadians. Card-related fraud is a serious concern. FireEye routinely uncovers major underground fora that sell thousands of stolen credit cards at a time, sometimes from major financial institutions, but just as often targeting customer accounts at smaller banks and credit unions.

Canada is also often one of the first targets for new malware campaigns. A Canadian bank was one of the first five financial institutions worldwide to be targeted by TrickBot malware and since then we've observed additional financial institutions added to TrickBot's configuration files that have a presence in or are based in Canada. Notably, Canadian URLs appeared in all TrickBot campaign IDs and several of those organizations were either credit unions or smaller banks. In August 2017 we also observed a PandaBot configuration file that revealed targeting specifically of 15 major Canadian financial institutions.

● (1535)

At least a half dozen organized crime groups also conduct financial crime operations targeting companies and people in Canada, and their sophistication is on par with what previously we would have said was reserved only for nation-states. One group in particular, which FireEye calls Fin10, has been focused specifically on Canada since 2013, carrying out numerous intrusions against gambling and mining organizations, exfiltrating business data and extorting victims.

With ongoing intrusion operations, active underground threat activity, substantial targeting by commodity malware campaigns and homegrown threat actors, Canada will likely continue to face a complex and challenging criminal threat landscape in the short- to medium-term future.

The cyber espionage threat to Canada is moderate, but could be on the rise. We have observed 10 separate cyber espionage groups from China, Russia and Iran targeting Canada in recent years. Organizations in the government, defence, high-tech, non-profit, transportation, energy, telecommunications, education, and media sectors, among others, have all been impacted, much like they have been in many western countries.

Many Chinese cyber-threat groups have renewed their attention to the theft of military applicable technologies since mid-2017 and are likely to intensify those efforts as trade-related conflicts with Canada and its allies emerge. This greatly increases the risk to Canadian commercial firms in all industries, but especially those that develop cutting-edge technologies or that directly compete with Chinese companies internationally.

Aside from intellectual property theft, Chinese-origin operations continue to heavily target competitive business intelligence from Canadian companies, especially those making foreign direct investments globally.

Looking forward, I am gravely concerned about the militarization of cyber operations. As NATO members continue to share capability in training, the major cyber powers outside the alliance are likely to do the same. This proliferation of cutting-edge offensive cyber power, combined with an increasing willingness to use it, with minimal blowback and spiralling distrust, has set the stage for more disruptive and destabilizing cyber events possibly in the near future.

In the past, some countries would have responded to western sanctions with increases in denial of service attacks on finance sector websites, but in the future, they may just as well respond with destructive attacks that are aimed at permanently disabling financial services or altering data in ways that undermine trust in the global financial system. For example, they could delay or impair the trustworthy settlement of collateralized government debt.

For countries sufficiently sanctioned, and therefore increasingly outside the financial system anyway, there is little incentive not to do so during a confrontation. Efforts to undermine foreign governments may increasingly be met with disruptive cyber campaigns, such as those that target elections infrastructure and individual candidates, where Canada is especially vulnerable.

I urge the Government of Canada to work with its allies in the United States and Europe to find peaceful, diplomatic arrangements with potential rivals and adversaries in cyberspace. Attribution, while difficult, has not proven to be the barrier that many predicted to enforcing such diplomatic arrangements, and many of Canada's likely antagonists share similar concerns about cyber-threats to their own financial sector, government stability and a desire to protect their people.

Diplomatic agreements that focus on ensuring the sovereignty of signatories and that avoid destabilizing operations while protecting human dignity can be reached. They can be enforced, and they would be mutually beneficial. But they may require the west to curtail some of its own cyber activities. While not sufficient on their own to protect Canadians, diplomatic agreements restricting certain classes of cyber operations will prove necessary alongside private sector technology and services to protect Canadian citizens and businesses in the long term.

Thank you, Mr. Chair, for the opportunity to participate in today's discussions. I look forward to answering any questions you may have.

● (1540)

The Chair: Thank you, Mr. Porter.

Mr. Reiber, you have 10 minutes, please.

Mr. Jonathan Reiber (Head, Cybersecurity Strategy, Illumio): Mr. Chairman and Vice-Chairman, thank you for the invitation to testify before your committee today. It is an honour to represent my company, Illumio, and to offer my thinking about the future of cybersecurity and national security policy planning.

I'm the head of cybersecurity strategy at Illumio, which provides microsegmentation capabilities for cyber-resilience, and the former head of cyber-strategy in the Pentagon, where I was speech writer to the deputy secretary of defense during the Obama administration.

If I may first beg your indulgence, I'd like to open my statement by honouring the memory of a great Canadian national security leader with whom I worked in the Obama administration and who died last year. We worked on cybersecurity together. I'd like to inform you about him briefly and register his name into the Canadian record.

Shawn Brimley's life has been celebrated across his adoptive home in the United States, including through a letter from former president Barack Obama and moving eulogies in our national press, but for his family and for our two countries, I'd like to enter this statement into the permanent record of the House of Commons.

Shawn Brimley was born in Mississauga, Ontario, served in the Canadian army and was educated at Queen's University. He later settled in Washington, D.C. with his wife, Marjorie Clark Brimley, and achieved more in his 40 years than most do in a lifetime of service. He went from serving in the Pentagon to the White House to running one of Washington's premier think tanks, the Center for a New American Security. He wrote the 2010 Quadrennial Defense Review, helped shape the U.S. pivot to Asia, ran crisis response and strategic planning initiatives out of the White House and was a leading thinker behind the third offset strategy for long-term U.S. defence innovation.

A loving husband and father, a great friend and a mentor, Shawn Brimley made all of us safer and more secure. For that, this House and this country, as well as mine, can be proud.

As he testified before the U.S. Congress in 2015, it is an honour to testify in front of this House today, especially on an issue that he and I started working on nine years ago.

In the years since I first entered the Pentagon, the cyber-threats have become a top-tier challenge to international security. Three trends make it so: the vulnerability of the networks and data of cyberspace; the overarching digital transformation of society; and, a lack of sufficient investment by organizations in the people, processes and technologies required to deter, defend against and recover from cyber-attacks. Governments and organizations have taken steps to improve their cybersecurity posture by building teams, developing options and adopting technologies, but progress has been too slow to keep pace with the threat.

Nation-states and non-state attackers steal, destroy and manipulate data in and through cyberspace. Adversaries flourish in what could be called the “grey space” below the level of outright conflict, and they appear undeterred in pursuing their goals in that way. To name just a few, consider China's continuing campaign to steal U.S. intellectual property, including the data of the joint strike fighter; North Korea's 2015 theft of $81 million from the Bangladesh central bank and the U.S. Federal Reserve; China's theft of 21.5 million personnel records from the U.S. Office of Personnel Management; and, Russia's disruptive attacks on the Ukrainian electric grid in 2015 and 2016.

Nation-states present the greatest threat because they have the resources to put hackers on salary. These people can go to the gym; they can work diligently over time to try to penetrate a target. In recent years, they have shifted their focus from theft and destruction to the data manipulation of political and media targets.

The Russian attack on the 2016 U.S. presidential election is the most notable example. As you're familiar with, on the express direction of Russian President Vladimir Putin, Russian military intelligence hacked into the networks of U.S. political organizations and political leaders and exploited vulnerabilities in social media business practices to spread propaganda and foment mistrust in the American population.

The Russian operation hit at three parts of the American “centre of gravity” during a period of acute political transition: the American people, the political leadership and the key technology companies. Other countries have since taken similar steps, including China's reported penetration of Cambodia's electoral system in 2018, which affords it the opportunity to manipulate the outcome of those elections.

Why is this problem so severe right now? There are three points, I would say. The first is increased urbanization. The second is the proliferation of dual-use technologies. The third is the interconnected nature of the world economy. This means that smaller groups of individuals can have an impact significantly disproportionate to their size. This is the high-consequence risk nature of modernity, which is what Anthony Giddens called it.

Examples include the 9/11 attacks by al Qaeda, the actions of the subprime lenders and their impact on the mortgage market and, most recently, Russia's cyberspace operation against the U.S. election. Just like the September 11 attacks when 19 men slipped past the security establishment and turned airplanes into missiles, a small group of Russian operatives found a seam in American security to conduct a high-risk asymmetric attack.

● (1545)

The Internet grew from zero to just under four billion users in the 35-plus years since its founding and access increased without a commensurate understanding of risk. Whether from the vulnerabilities of code or the impact of social media on political identity formation, network status and cloud environments are vulnerable to breach, and society is vulnerable to manipulation.

As a matter of priority, countries should focus on deterring nation-state attacks. Deterrence is a function of perception, and it works by convincing a potential adversary that the costs of conducting an attack will outweigh the benefit. Effective deterrence requires the ability to impose costs on an attacker through sanctions or military means; defensive tools to repel an incoming attack, like firewalls; and, in the event that a hacker gets through the perimeter defence, resiliency capabilities to limit impact, like microsegmentation.

Two propositions arise from recent history to inform your inquiry. First, adversaries have escalated in cyberspace, despite the U.S. government's efforts at deterrence. The United States and other countries must therefore take a more aggressive stance to deter aggression. In 2018, the U.S. government embraced this position, notably through the defense department's doctrine of defending forward in cyberspace.

As my colleague pointed out, adversaries have escalated, and the United States chose to indict or sanction as punitive measures. These actions, while reasonable, did not set a precedent or effectively deter escalation. For example, even after sanctioning Russia for its actions in the 2016 election, Russia reportedly continued to implant malware on the U.S. electric grid through 2018.

What does it mean to defend forward in cyberspace? If it has indications and warning of an impending attack, the United States must be able to push back against an adversary. This means penetrating the cyberspace infrastructure to conduct counter-offence hacking to blunt an incoming attack. Nation-states have the right to defend themselves in cyberspace, just as they do in other domains. To maintain peace and stability however, any operation must be conducted under the law of armed conflict.

The need for a more forceful deterrence posture is the first takeaway from the last 10 years of cybersecurity policy development in the United States. The second is the need to assume breach and plan for adversaries to penetrate your internal defences and gain access to your most vulnerable data.

What does it mean to assume breach? Most organizations focus on the perimeter defence, and they lack an internal security system to prevent servers from communicating with one another once an attacker has broken in. Once an attacker has penetrated a network, they can spend up to an average of six months inside a data centre or cloud environment, moving around unencumbered, implanting malware for whatever purpose they choose. An organization's crown jewel applications, like its key databases, are open game in that instance.

In the Chinese attack on OPM, for example, no rules existed to govern how applications and servers would interact internally. Thus, when the Chinese made their way inside, they could easily make their way to the database that held 21.5 million records.

Microsegmentation prevents breaches from spreading. At its most basic level, it puts walls around vital applications to segment them away from the rest of the cloud environment and data centres. An intruder may be able to get three servers, but not 3,000. In this way it's a deep foundation for cyber resilience and the last line of defence. For critical infrastructure sectors like the financial sector, if you have this kind of capability installed, it provides an element of resilience not just for the sector itself, but for the nation as a whole.

It is not a question of if but when a breach will occur. Countries need to proactively defend themselves against aggressors to achieve deterrence, but they also need to assume breach and implement defence in-depth strategies to withstand cyber-attacks. Leadership enables success against all parts of the cybersecurity project.

In his seminal essay, “The Challenge of Change”, historian Arthur M. Schlesinger said, “Science and technology revolutionize our lives, but memory, tradition and myth frame our response”. That is true. Our ability to manage technological change depends ultimately on the success of the leader and his or her ability to tell a story to make change. We have a crop of strong security leaders who have come up in Canada and the United States in the last 10 years. Technology's momentum and evolution may never end, but good leaders help society adapt and manage change, from the rise of aviation to the dawn of the nuclear age. Cybersecurity is simply the latest chapter in our story.

Ultimately, leadership is underpinned by analysis, and that's what makes this committee's work so important.

Thank you for having me. I welcome your questions.

● (1550)

The Chair: Thank you, Mr. Reiber.

Thank you for your statement about Shawn Brimley. That was a kind and thoughtful gesture, and appreciated by us all.

Ms. Damoff or Mr. Spengemann.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Chair, I'm going to start and then I'll turn it over to my colleague.

I have a very quick question, Mr. Porter. You mentioned something about the Canadian election infrastructure being especially vulnerable. We don't have the same system as the United States, as you know. Why are we especially vulnerable?

Mr. Christopher Porter: Just to be clear, it's not that Canada per se is especially vulnerable. I guess I meant more that it's an especially important vulnerability for Canada. Obviously, the use of paper ballots takes away a lot of the concerns that we have in the States. Nonetheless, I think this is a high priority for a number of aggressors that would target Canada, both internal political activists and also China, Russia and others that might seek to influence the process.

Much like the financial sector, elections are processes that are high-trust events. We benefit tremendously from living in free and democratic societies and also from being able to conduct trade and transfer money worldwide. The flip side of that is even a small problem, or even the perception of a problem—maybe not even a real breach—does outsized damage to both elections and the finance sector.

Ms. Pam Damoff: I'm going to stop you, because I just wanted some clarification on that, so thank you.

Mr. Christopher Porter: Yes.

Ms. Pam Damoff: I had a meeting this week with the Canadian Association of Mutual Insurance Companies. They actually joined us today. The meeting was about open banking. I didn't even know what it was and they explained it to me. I know the United States is looking at moving toward that. Are you familiar with it?

The concept is you get financial tech firms, like Wealthsimple that we have here, that would have access to banking data. You have the banks up here, which in Canada are extremely heavily regulated. The information would flow into a portal like Expedia.ca and they could access it to tailor your request.

To me, that type of system seems ripe for all kinds of cybersecurity and privacy breaches. It is something that apparently Europe is doing, and the United States is moving toward that as well.

● (1555)

Mr. Christopher Porter: I'm not familiar enough with that system to comment on it specifically. Those types of arrangements in general, where you have a data broker that acts as a public trust or an industry-wide trust generally have the effect of improving cybersecurity day to day, but also of making the system more brittle. One compromise becomes a massive compromise.

I don't know enough to comment on that situation specifically, though.

Ms. Pam Damoff: Are you familiar with it at all?

Mr. Jonathan Reiber: I'd be lying if I said I was.

Ms. Pam Damoff: Okay, that's fine.

I'm going to turn it over to Mr. Spengemann.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thanks very much.

Thank you both for being here.

My interest is in small business and in good cybersecurity as, if you will, a global, common public good, a national public good. What can we do to make life easier for entrepreneurs that may be datacentric but early in their lifespan may have problems affording good cybersecurity. Are there things that government can do to step in to fill the gap? Established businesses with large datasets and large client databases and revenue have an easier time. Start-ups don't.

I'm wondering if you could comment.

Mr. Jonathan Reiber: Sure. There are a number of different ways to try to spur investment across the country. The regulatory environment has matured significantly in recent years for this purpose really. Cybersecurity is a bit like life insurance. You need some kind of nudge. In life insurance it's usually the birth of a child. In the case of expenditures, however, I think you need an outside nudge.

On GDPR, Colorado and California state laws, the new law that you passed...but also in New York's financial services sector in New York state, they passed a new law that really pushes down a requirement for breach management. This means that companies have to be compliant, and this will affect how companies drive behaviour within the market and how they end up spending money.

Services aren't that expensive. It's really not a question of expense. It's a question really, as I said earlier, of leadership.

I like to talk about the new security stack and the old security stack when it comes to bundling cybersecurity investments. In the past you had the old security stack, things like encryption, intrusion detection systems and firewalls. Now we have this new capability called microsegmentation which provides this deep resilience for data centres.

I would recommend for any organization that's looking to make investments in cybersecurity that they think about this new security stack to cover both the perimeter and the interior.

Service expenditures have really decreased in recent years as the market has evolved, but I would point you toward those regulations as good steps—

Mr. Sven Spengemann: —to the point where those expenses wouldn't even be a barrier to market entry in most cases.

Mr. Jonathan Reiber: Oftentimes if you have your IT budget as 10% of your total expenditure, which, in the Pentagon's case is like $40 billion, then your cybersecurity investment should be about 10% of that, which is really about as much as we spend for U.S. Cyber Command.

Mr. Sven Spengemann: Okay. That's really helpful.

Mr. Porter, do you have any comments on this question?

Mr. Christopher Porter: Yes. Thank you for the question.

The targeting of small businesses is an issue that's near and dear to my heart on the policy side. First off, although it's not directly my expertise, I think the move to the cloud has made it possible to get high-quality security providers in much more scalable ways, where you pay per bandwidth or per seed or per licence as opposed to a large capital fixed cost. Even as opposed to a few years ago, those solutions are much more affordable. However, to stop a world-class actor you need more than just the technology. You need some sort of organizational infrastructure where you're training and keeping employees, and threat hunting. That is beyond what small businesses can do for themselves.

At FireEye we offer managed defence, where we'll manage your network for you. Even with that, that's a 95% solution. To me, the policy failure that this House could address.... At least in the States the policy failure has been that you tend to pick a few industries to defend, and to defend the biggest companies that are there, because those are the ones that are most obviously a threat to national security if they're compromised.

Mr. Sven Spengemann: Right.

Mr. Christopher Porter: What we're not as good at in the west is death by a thousand cuts, so actors that destroy 1,000 small businesses won't get the President's or the Prime Minister's attention, but one big compromise will. I think that's a policy failure that should be addressed. In Canada, I would recommend that you, even though it's very difficult, at least say it's a priority for you to defend everyone, not just the biggest businesses and not just these siloed industries. It may be a very large Herculean task, but it would be nice to see that at least as a stated priority to start working towards.

● (1600)

Mr. Sven Spengemann: That's very helpful. Thank you.

Thanks, Mr. Chair.

[*Translation*]

The Chair: Mr. Paul-Hus, you may go ahead for seven minutes.

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

Thank you for being here today, gentlemen.

I had the opportunity to meet Mr. Reiber in Silicon Valley, back in October. That's when I got the idea to have the committee meet with a representative from FireEye as well.

My first question is about where Canada stands globally in the cybersecurity arena as compared with the United States.

Clearly, the U.S. is a superpower and therefore a target of choice. With China and Russia, you are somewhat of a natural choice. In Canada, we are still seen as the good kid, the nice guy, if you will. From a military standpoint, the U.S. has a huge army, in comparison with Canada's rather small one. However, we've always said that we would work together to defend ourselves should a problem arise.

On the cybersecurity front, given the current American defence infrastructure, private organizations and even public ones such as the CIA and the Department of Homeland Security, do you think that, in the event of an attack, co-operation between our two countries would be possible and you would be able to help us?

[*English*]

Mr. Jonathan Reiber: For some reason the translation didn't come through, so I'm relying on my high-school French, which is not terrible. I'll try to answer.

Your question is, it seems to me, within the evolution among CIA and DHS and the military, how much do they collaborate for common defence, and could they help Canada? Is that part of the question?

Mr. Pierre Paul-Hus: If Canada is a victim of cyber-attacks, is there a possibility that the U.S. could help Canada quickly?

Mr. Jonathan Reiber: Sure. That's what I thought. Yes.

Mr. Pierre Paul-Hus: Are Canadian laws obstacles? Do you know?

Mr. Jonathan Reiber: Under article 5 of NATO, for everyone who is a member of NATO, there is a resolution that says a cyber-attack, if it triggers a certain point, would require a common defence.

One interesting thing about cyber-attacks so far is that they haven't crossed a threshold that has immediately made a clear statement for a warranted military response in a way that would necessarily be required. I would say the Russian attack on the 2016 presidential election, looked at historically, certainly qualifies as an instance when a counter-offence action by the military would have been warranted. I think that others in the Obama administration have said the same thing. The difficulty in that particular instance is that the decision calculus is complicated, and I won't go into that because that's not really the nature of the question.

Mr. Pierre Paul-Hus: Thanks. I just have seven minutes.

Talking about the relation between the public sector and private sector—you worked at the CIA, the Pentagon and now you're in the private sector. Here in Canada we try to find how we can work with the private sector because, as we know it's more difficult to have a public servant working in that kind of business.

Mr. Jonathan Reiber: Sure.

Mr. Pierre Paul-Hus: Do you think Canada must switch to have the same way of work that you have in the U.S.?

Mr. Jonathan Reiber: I think this is an evolution we've gone through. Really since 2014, there's been a significant push to build connective tissue between the private sector and the government. Certainly, I think it's immensely valuable. We had a ramp in terms of defence innovation fellows—the U.S. Digital Service and the Defense Digital Service, those two components—that brought people in from the outside. It was tremendously helpful.

I recommend to every country that's dealing with cybersecurity issues to find a way to build connective tissue to allow tech entrepreneurs to work in the government, and likewise to have people from the national government to work in technology, for certain.

● (1605)

Mr. Christopher Porter: It's interesting in cyber work because 95% of the attacks that are happening are on private sector networks against private sector victims. Often, in the United States and elsewhere, the first to know about it might be the private sector. Governments can have more powerful responses and their investigations can go more in depth. The private sector doesn't replace government work, public sector work. It's complementary.

It's important to know, for example, that at FireEye some of our core teams that are discovering crimeware are based out of Canada. Even though we're proudly a U.S.-founded company, we're an international company in terms of our workforce. That's rapid information sharing across borders, which also is sometimes difficult for governments to do.

To answer your question, yes, I do think that Canada and the U.S., as the closest of allies, would come to each other's aid in principle under appropriate circumstances. I would defer to my colleague on what those are, but at a working level, absolutely, Canadian and U.S. researchers work together every day and exchange information on threats. I think you'll find that not just in times of crisis, but every day.

Mr. Jonathan Reiber: Yes. I think there's obviously a deep level of co-operation between the intelligence services and the security services for incident response. I know there's a trilateral commission among the U.S., Mexico and Canada where that co-operation happens. It obviously happens between the two allies themselves.

Mr. Pierre Paul-Hus: Okay. Thanks.

I wanted to hear your view about the Chinese company Huawei. There's a debate here in Canada about that company—some people say there's no issue, while others say there is. The U.S., Australia and New Zealand have decided to ban Huawei. What is your view?

Mr. Christopher Porter: For FireEye as a company, it's not an issue that we follow. We're looking at software threats, not the sort of hardware threats that are alleged.

I absolutely understand in principle why, particularly for government networks, you would want all your telecommunications equipment made by your own country or by a close ally. I think in principle it makes sense, but I don't know anything non-public, other than what I read in the newspapers, on the Huawei issue.

Mr. Jonathan Reiber: I wouldn't comment specifically on Huawei. I would say that we've been dealing with issues of supply chain risk since...gosh, I wouldn't want to say how far back in history. Certainly since the dawn of the crypto-analytic platform in signals intelligence, supply chain problems have been paramount.

There's a diminishing marginal rate of production if you decide you're going to try to pursue every single chip in the universe to make yourself secure. For certain elements of, say, a national security community or the public safety community, I think it's perfectly reasonable to say, “We are going to now manufacture a certain number of chips on our own”. But the cost is quite significant, and it alters how people do things economically. I don't think you could possibly do so in any kind of global way across sectors for an entire economy. You could probably do it for a number of subsectors.

The Chair: Thank you, Mr. Paul-Hus.

Mr. Dubé, you have seven minutes, *s'il vous plaît*.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Chair.

Gentlemen, thank you for being here. I apologize for my tardiness and missing your presentations. It's a problem when you're alone here; you can't separate yourself in two. I was stuck with some media upstairs.

I do want to ask about the role of the private sector. It's something that has come up quite a bit, and I think it's one of the underlying tensions in this field of navigating what role the public and private sectors have to play.

I'm just wondering if you see any concerns over the fact that a lot of these things are being offered as services. There's always this notion of wanting to protect what you do best and the clients that you have versus another company operating in the same field. Is there any concern that the sort of regular rules of business and industry might undermine any kind of uniformity or ability to have standard practices and ensure that everyone's on a level playing field when it comes to our own interests here or in the U.S., for example?

Mr. Christopher Porter: I think you'll find that, at least within the information security community, a large majority of the biggest companies work together on standards and exchange information, even with peer competitors, for example, collecting threat intelligence. We often co-operate behind the scenes in the public good by exchanging information.

Standards setting is generally great for existing enterprises. I don't share your concern. I understand where it would be that way in theory or principle, but I haven't seen that when I've worked in the private sector. I have people I consider good friends and colleagues in many different companies. You compete for individual contracts, but overall, that doesn't hold back standards setting.

For example, I would point to the tech accord community that Microsoft leads. A lot of that public policy work looks at what sort of standards we as a community can have and how we can work together for the public good. That's still competing for individual contracts, and still keeping competitive business secrets to ourselves —you're right—but how can we work together, as well, to make sure those services do get delivered?

The example I always give is that, at least in the the old west, banks were relatively undefended from physical threat. As governments have played a larger role, and as physical security markets have matured and there have been more standards and regulation, those physical security companies make more money than ever. That sort of regulation didn't hurt their ability to either provide services or be successful as businesses.

● (1610)

Mr. Jonathan Reiber: I concur with my colleague's statement that the standards community has done a good job of rising up in this way. I think the NIST cybersecurity standard that was passed after the initial effort to pass cybersecurity legislation in 2011 and 2012 was a very positive outcome from an earlier effort to try to come up with a mandate or a set of standards. I would refer you to the NIST standard.

I would also say that to prevent a focus on one technology, or one part of the problem against another, the information sharing and analysis organizations that have cropped up within the different centres have facilitated sector-specific development of cybersecurity requirements. The financial service sector in the United States is, in this way, the most mature of the bunch. The FSISAC, Financial Services Information Sharing and Analysis Center, is a good resource for understanding how the sector meets its own interests when it comes to cybersecurity.

Mr. Matthew Dubé: Thank you for that.

I'm just wondering if, as we look to the future, and put it more in lay terms.... I think we talk a lot about the cost of using services. What you offer other companies, if you're a company, to protect your own data, if you're collecting customer information and whatnot.... I think those are some of the high-profile cases.

I'm just wondering how you see, going forward, when some of the risks might not be from business X stockpiling data for a rewards program, let's say, but more in what they're selling. In other words, if you're selling any kind of household device, with the proliferation of smart devices and things like that.... Is there a concern that there might be a lot of investment, a lot of money spent to protect your own interests, but not necessarily the interests of the end user, who is purchasing equipment or devices from a given company—for more required updates, and things like that?

Mr. Christopher Porter: My number one concern with the Internet of things, which I think is what you're describing—Internet-connected physical devices—is that many of those devices are not updatable at all. Even if you discover a flaw in them, it's not technically possible to go in and fix it. That's an incentive for the manufacturer, where there's limited liability for flaws discovered in their products, that you wouldn't tolerate for a physical threat, for example, or a flaw, a manufacturing defect.

I do have concerns with that as a threat vector. In terms of the proper market incentives.... I was a business major, so I should have a better answer, but that's not what I focus on every day. I'm thinking from a threat perspective. Threat groups are going to be focused on how they can cause physical disruption in ways that undermine entire communities and societies. I'm much less concerned about the everyday kind of criminal malware that could affect those physical devices, and more concerned about how that creates a very intimate way for foreign governments, for example, to disable physical devices in your home as an individual citizen. I would propose that public safety is, first and foremost, a government responsibility.

Mr. Matthew Dubé: We talked about standards earlier. Are you in favour of some kind of standards, almost in the same way that if a vehicle is going on the road, there are standards expected for safety? Should it be the same thing if you're selling phones or things like that, given this new reality we're living in?

● (1615)

Mr. Christopher Porter: Yes, absolutely.

Mr. Jonathan Reiber: When it comes to cybersecurity, it does help to look at the data centre and the cloud environment first. There's a tendency to think about the end result, like IP theft or data destruction or data manipulation, any one of which could make for a sci-fi movie and keep all of us up at night.

If, however, you start with the data centre itself and say, “How am I securing how servers interact from the interior? How am I preventing intruders from moving laterally throughout an environment?”, you're actually covering all those bases. Yes, that's what my company does, but the reason I joined Illumio was that, having worked in the Pentagon and having looked at the range of disruptions that could happen, whether to a weapon's platform or to the financial sector or to the economy, I would say you really want to start in the worst-case place. If an intruder breaks into a data centre and can move around unencumbered, everything is on the table. So yes to standards. Actually the French government has been very forward-leaning in that regard for security data centres, and other countries have as well. If you start there, then everything else, even an intrusion into an IoT in someone's home, will ultimately connect back to a server, and so that could be prevented.

Mr. Matthew Dubé: Right. Okay.

The Chair: Thank you, Mr. Dubé.

[*Translation*]

Mr. Picard, you may go ahead for seven minutes.

[*English*]

Mr. Michel Picard (Montarville, Lib.): Thank you, gentlemen.

When we face a terrorist event, we usually know who hit and most of the time the reasons our country has been involved in their country. Perhaps we have taken a position against their policies and so on. If I were a private corporation and a financial service provider, my question would be what kind of a threat I represent to foreign interests so that I become a target for cybercrime. I have my own business. I do have branches in every country, but I don't impact anyone's wealth from a government standpoint. I don't know where the hit comes from. I don't understand why I'm being targeted. Is it because cybercrime is a national sport in this country or because they're playing bank robber and just taking my money virtually? I'm not sure the private corporations do understand the full picture of what they represent and how it works so they can come up with the right solution.

Mr. Christopher Porter: I share your concern, and I agree with you. Oftentimes I feel that even companies in the financial sector that have fairly sophisticated security organizations internal to themselves don't see the threats coming. They know that threats in general are coming, but to your point, the particular reasons they suffer a breach or are targeted for attack often have nothing to do with that institution. Perhaps the foreign threat is doing it to get back at the Canadian government for some action they took. Just as commonly these days it's for economic competitiveness reasons. Those Canadian financial institutions may not be harming anyone else, but there may be another bank in another country or another investor that wants to out-compete those Canadian institutions. If they can't do it fairly in the open market, maybe they can get help from a cyber-threat group, for example.

Unfortunately, Canada's financial institutions are targeted not necessarily because they're doing anything, other than for cybercrime, obviously—that's where the money is—but when it's a nation-state doing it, it's often for economic competitiveness. They want to either learn from or out-compete those institutions when making foreign investments. It could be for political retribution, even for something that happens in a different country.

The flip side of being in a strong alliance is that if a hacker finds a vulnerability in a Canadian financial institution, they could use that to propagate a political message against another member of NATO, for example. It could have nothing to do with that institution at all. That's why it's so important to have the close ties between Canada's security services, which are going to have better insight into those motivations, and the private sector.

Mr. Jonathan Reiber: I think it helps to start by thinking like an adversary, right? Whether you're a government or an organization that is thinking about threats overall, you need to go through: What is an adversary? How are they going to try to hold me at risk? What are they going to try to do to me? What am I willing to lose? Once you have a sense of what your core interests are, what you're willing to lose and what you need to protect, then you can start building a strategy for investment. That doesn't quite get you there to answer your question, however.

In the United States, we passed an executive order about cybersecurity that called out something called the section 9 list. The Department of Homeland Security conducted an assessment of all the companies and organizations in the country that were most cyber-vulnerable, and the impact of which, if disrupted, would cause the most significant damage. That analysis led to a list, which is classified. It's not a very large number of companies; you could probably guess a number of them right off the bat. That also helped the government focus on its collaboration with those key companies. That way, you can say that we're going to ensure the cyber-defences of these companies are going to be hardened.

That does not mean that those are the only companies the country would focus on. The military, for example, has to look at the adversaries, Russia, Iran and North Korea in particular, and ask: What are they investing in? What are they going to go after? What are they going to try to do? You have to try to blunt and block them if they do something quite significant.

That also doesn't quite get us there, and this is where regulation has to come in. If you've hardened the most valuable companies in a country, if the military is watching the most valuable adversaries, it's the Internet. It's massive. Someone is going to try to hack somewhere else and they're always going to look for the weakest underbelly—wherever they can go.

A great example here is Iran in 2012. The United States was prepared for Iran to do all sorts of things during the nuclear negotiations. What Iran did, which we were able to prognosticate that they would do, was to go after the infrastructure in the Persian Gulf of Saudi Aramco. They hacked Saudi Aramco, as has been publicly reported. That's where regulation absolutely has to come in and say that there have to be breach management requirements; there have to be penalties if companies don't meet these breach management requirements, and companies have to be able to meet certain resiliency investments to defend against breach.

● (1620)

Mr. Michel Picard: What are our chances of fighting at the same level as our enemies, considering that some of them are state-sponsored initiatives where budget is no object? My concern in Canada is that budget is an issue.

Mr. Jonathan Reiber: The good news in cybersecurity is that we can control our own terrain. What that means is.... If you think like an adversary and you think about what the adversary is going to try to do.... They have their terrain where they're launching attacks from the offence. It's not the duty of the private sector to be concerned with that; it's the duty of governments. As an organization, whether you're a government organization or otherwise, you can reorder and configure your terrain to harden yourself quite significantly against an attack. This means you set up your perimeter defence. You have your firewalls. You're encrypting your email. You have multi-factor authentication for your users and you invest in this microsegmentation capability. That way, if someone breaks past your defences, they're going to be stopped in their tracks inside your data centre or your cloud.

If you've done all that and you've invested in cyber-insurance, you're going to have taken some very strong steps. You would assume, then, talking to a bank or a major institution, that they would have done this. The number of times when I give an address to a cybersecurity community and I say to raise their hands and tell me how many of them use multi-factor authentication, it's less than 20% almost every time. When I ask how many of them encrypt their emails, the numbers are also very low. This does get to the sort of nudging and regulatory demand.

I think, though, that if we take these steps, we can put ourselves at a significant advantage against those who would try to intrude against us. You can block 95% of the intrusions that would happen, or you can prevent the damage from 95% of the intrusions that would happen. There does ultimately have to be a partnership with the government in order to impose sanctions, or punitive measures, in the cases where you may not be able to do so as an organization.

Mr. Michel Picard: Thank you.

The Chair: Thank you, Mr. Picard.

Next is Mr. Motz, for five minutes.

Mr. Glen Motz: Mr. Porter, if we're considered a country that would be a first target, would that not increase the need for us to be at the forefront of cyber-defence? Despite our smaller population and budget restraints, how can Canada increase its edge, either on our counterparts or in an effort to defend ourselves? How is that possible? Can you cite some best practices from around the world that we might be able to look at?

Mr. Christopher Porter: Yes, absolutely. Thank you for the question, Mr. Chair.

The good news and bad news is that because cyber-policy is still so nascent, and your allies are still grasping at something that will actually work, Canada has a de facto opportunity to be a leader in this field by finding a solution that works. I think that's absolutely achievable.

I'll start by reorienting the question just a little bit. Within the NATO alliance there's a general attitude that governments will learn secret things and they will take some action to defend mostly their own networks, and then maybe companies and individuals as well. Maybe occasionally they will declassify that and share that with companies. That process is typically very slow and very long term. In the private sector, if we don't turn around actionable threat intelligence in 48 hours, we really have let our clients down. I think governments typically operate on timelines of several months. In some cases this is for good reason. I'm not going to pretend like there aren't good reasons for doing that. There often are.

I would encourage you to think that everything I just said about cyber-intelligence sharing was once true of counterterrorism, for example, until...threats to aviation and with 9/11. There was a much greater emphasis on pushing that information out to local governments, to individual actors and to companies in the U.S., and much greater information sharing and declassification.

I think we need the same thing in cyber-threat intelligence, where the allies are willing to tolerate more risk and push that defensive information out to the private sector more rapidly. It's unrealistic to think that a small business, for example—large enterprises, maybe—would be able to keep up with changes in major threats in a competent way. Between the large private sector cybersecurity companies and better information sharing from the government to those key partners, I think that would go a long way. You would have to tolerate some risk, of course.

The current situation where governments tend to view themselves as the central repository for information and will collect everything and then tell you what to do about it is just not how things work in cyberspace. Governments are still the largest actors, but they're not the only ones.

● (1625)

Mr. Glen Motz: Good, thank you for that. I have a limited amount of time.

Mr. Reiber, in your experience here with Canadian law, do you see anything that is missing from our current law structure that could possibly improve consumer privacy, consumer protection or our ability to defend our critical infrastructure?

Mr. Jonathan Reiber: Sir, I wish I were an expert on that question, but I'm going to have to pass.

Having read your new 2018 cyber-strategy, I think it does provide a good platform on which to build for the nation overall, but I'm not so familiar with Canadian law.

Mr. Glen Motz: All right.

What about you, Mr. Porter? Do you have any comment on that?

Mr. Christopher Porter: No.

Mr. Glen Motz: Mr. Reiber, you mentioned the whole concept of microsegmentation. Would that be expensive for smaller companies to implement?

Mr. Jonathan Reiber: No, not at all.

Mr. Glen Motz: What does it entail? Does it entail different servers or a different configuration of servers?

Mr. Jonathan Reiber: It really depends on what you're trying to achieve. I would defer to my team for specific pricing models.

It's really done on a case-by-case basis. I would recommend organizations to start.... One thing we discovered in our businesses is that most organizations may have some sense of what their crown jewel applications are, what their most valuable applications are within their universe. For example, as I mentioned once before, if you're the Office of Personnel Management, a database that stores all the data for all the personnel would be a key application.

Once you've identified your most important applications, you want to map out your data centre, all your applications, and workloads, which are not quite applications, but they provide the connective tissue within your data centre for your applications and servers. You want to map them out. Most organizations haven't done that. If you think about maps as a key element of geostrategy, in order to control your terrain you have to have this map of your interior. That then shows you how all the applications interact.

If Chris is in the marketing department and I'm the guy who handles the key servers for whatever my organization is, a payment system or otherwise, and he gets hacked through an email, there's no reason why his server should ever be interacting with mine. He's not concerned. He's not an engineer. I'm the engineer. In that way, you draw a map of how your applications work and then you set rules for how they interact with one another.

The degree to which an organization wants to set rules for specific crown jewel applications across their enterprise affects the pricing model to some degree. That's why I'm not going to offer you a specific cost. If you want to map your enterprise and begin to set rules internally, that's when you really harden your interior. One of the benefits of setting rules is it provides alarms. If somebody breaks into one server and you know that server shouldn't be interacting.... Again, if he's hacked in the marketing department and I'm an engineer, we know these servers shouldn't be interacting. If you see an intruder doing it, it will set off an alarm so then the security operations team can know somebody's inside.

The Chair: You know you're in a market for microservers.

Mr. Glen Motz: Yes.

The Chair: Okay. Beware of your fridge, though.

Ms. Dabrusin, you have five minutes.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): I think you mentioned something about who's outside, and that's where you left off. That's where I wanted to start.

In our last meeting we heard from HackerOne. It was really interesting to hear their perspective on how you can improve systems by having people who have that type of knowledge poke at your system to figure out where your vulnerabilities are. They said that legislation is necessary to help provide protections to those, I think they used the term “white hats”. I'm not crazy about that, but whatever the term you want to use for your “good person” hacker....

What's your perspective on having legislation that protects these types of hackers and trying to encourage that?

● (1630)

Mr. Jonathan Reiber: The interesting thing about cyberspace, unlike any other domain, is that the brains are really the weapon, to a large degree. It's the person and what they know and what they're capable of doing. The intention matters a lot.

I think red teaming and penetration testing—my preferred term is “penetration testing”—are absolutely vital for the development of your security strategy. If you've implemented the best capabilities in the world, if you have the new new security stack, if you've spent and been very smart about it, you always want to have someone who's trying to break in to your network, constantly testing it, looking for vulnerabilities, and thinking like an adversary trying to find their way in.

I won't weigh in on specific recommendations for legislation. It's very complicated, and there is international legislation under way through the Wassenaar agreements and the Wassenaar accords, which you—

Ms. Julie Dabrusin: What's—

Mr. Jonathan Reiber: —Wassenaar? My spelling of German and Dutch words is not great, but I can find that out for you.

Ms. Julie Dabrusin: Thank you.

Mr. Jonathan Reiber: The proliferation of malware and penetration testing capabilities globally is a concern, because you never know what somebody's going to try to do once they have that kind of knowledge, or if they have malware that allows them to break in.

The State of Pennsylvania has a law regulating who gets to use malware and for what purpose. I'd certainly think that over time we're going to see an increase in regulation around penetration testing and even ownership of malware for that reason. It's very complicated to verify why and how somebody has malware on their computer. It could be because it was infected, or it could be because they're going to get up to something. Proving it is really a question of the intention of the person who has it. It's complicated.

Ms. Julie Dabrusin: Mr. Porter, do you have any thoughts as to things to watch for or things that would be gained by doing this?

Mr. Christopher Porter: I want to emphasize my colleague's point that it's helpful to tolerate some risk, particularly at the university level and younger, in terms of allowing people to explore computer security—professional researchers as well—without criminalizing their activity, if there's no malicious intent and if there's not deliberate harm. I think there are a number of regulations under way and laws being passed, in the States and elsewhere, in a good faith attempt to improve cybersecurity but which have the effect of stifling original research.

I obviously can't comment competently on Canadian law, but I urge you to avoid the impulse to criminalize what is essentially math and logic put into electronic form. Don't criminalize that thought process, because the same sort of creative people who are exploring those possibilities are the ones who you hope to employ one day to defend your country as well. There's nothing you can do that would hurt a relationship with the security community more quickly than to criminalize their work, or put a presumption of guilt into what may just be good-natured intellectual curiosity.

Ms. Julie Dabrusin: That leads me to the other question. I believe it might have been you, Mr. Reiber, who pointed out that the third part of the problem was not enough human infrastructure, for lack of a better term. We heard about this a lot, about how we build the human capacity to deal with cybersecurity.

Do you have any tips from what you've seen of countries doing well, or less well, to build that capacity?

Mr. Jonathan Reiber: The first resource that I would point you towards is a map that was just produced by NIST. I guess it's the National Institute for Cybersecurity Education in the U.S. that actually maps out population density and the number of users. It's a good resource to look at how we're meeting the workforce challenge.

I would say master's level education and university level education to appropriate technical specifications like Security Plus or CISSP.... These are certifications to get people trained to do certain kinds of core cybersecurity functions. The degree to which community colleges or whatever the appropriate name is in Canada —you'll forgive me—the associate degree.... The sorts of institutions that can train people in cybersecurity tasks are incredibly helpful, and the degree to which the federal government can offer either some kind of incentive for universities to initiate those kinds of training programs we found to be very helpful.

It also helps if you have state universities that are clustered around industries that need to transition. For us, the manufacturing sector and large parts of the U.S. economy have gone through a massive transition. There are states like Michigan, for example, where Michigan State University should be investing in cybersecurity training for a lot of the auto industry. The auto industry itself is transitioning into cybersecurity. Finding these corollaries around clusters where you can then make investments in university training is very helpful.

The last thing I would say is about the evolution of the cyber mission force, which is our military force. It was initiated in 2012, and it achieved full operational capacity in 2018. These are the individuals who are sort of high end. There are 6,200, and the investment in this force is a major deterrent effort on behalf of the government. These hackers exist within the military—and they are hackers. It did take them five years to get fully trained, though, to get the whole group fully trained, because you had to move people through schoolhouses, and that takes time and effort.

There is a little bit of patience, and that's what ultimately leads me to say: Focus on securing your most important applications first.

● (1635)

Ms. Julie Dabrusin: Thank you.

The Chair: Thank you.

Mr. Christopher Porter: I'd like a few comments, if I may, Mr. Chair.

The Chair: Ms. Dabrusin has been very generously allocated time by her chair.

Maybe you can work your response in at some point.

Mr. Eglinski.

Mr. Jim Eglinski (Yellowhead, CPC): Thank you, Mr. Chair. I hope you'll give me that leeway too.

The Chair: You're not nearly as charming as Ms. Dabrusin.

Mr. Jim Eglinski: Oh, come on, look at my face.

Thank you, gentlemen, for coming today. It's been very interesting listening to you, and it's actually been a little scary listening to you.

I noticed during your presentation, Mr. Reiber, that you talked about four billion people coming online over the last 35 years. I think you mentioned somewhere—or I've heard it—that over the next five years, we're going to see another 25% coming on, especially with China and India progressing the way they are.

Mr. Jonathan Reiber: Yes.

Mr. Jim Eglinski: Of course, cyber-threats are going to increase with that number of people coming online. I know here in Canada, we're not going to see that kind of growth, of course, but it would be proportional, I imagine. The fact that we know China is one of our primary adversaries in cyberspace is very concerning to me, and I think it's concerning to everybody here on this committee.

What are the top four things you would recommend that we could do as a country to protect us in the best way in the future?

Mr. Jonathan Reiber: I wrote down two. I'll try to come up with three and four. It's a great question.

The first thing is to protect critical infrastructure and identify the companies and organizations that matter most for the overall health of the economy and the nation's safety. If a country has not embarked on the process of identifying those corporations and entities within the economy, then it's almost like by analogy, from where we come from within Illumio, that you haven't identified your crown jewel applications.

We're looking internally within the organization to say: What applications matter most? That's the second thing. The first is to identify the most important organizations within the country. Then those organizations themselves need to invest in the whole stack of security for the perimeter and their interior, and they need to identify their core missions and figure out how their most important data relates to their core missions. That's an analytic process that involves the security team, the infrastructure team, multiple components across the organization.

That's four things. The first is critical infrastructure, identifying within the country. The second is identifying your core assets within the organization itself. The third is thinking about your mission and being prepared to operate without access to data. That's very important. If you think to yourself, if you lost your data today, what would you not be able to do and what do you absolutely have to be able to do?

The fourth thing is what I talked about from a deterrent standpoint. Countries have to think about how to deter nation-states from coming after them. If you assume you're going to be breached, the best thing to do is to prevent someone from trying to breach you in the first place. If they do breach you, you need to be ready and you need to be secure beyond breach. But to do deterrence is really very impressive. Ultimately, as the Internet expands, it's not just the next billion users in the next five years in China and India alone—because we will add a billion just between those two countries—it's all the connected devices that are going to be spun out from all those users as well. So we're not just going to see an expansion of humans, but an expansion of all the technologies that every human is touching.

● (1640)

Mr. Christopher Porter: I have a few brief suggestions, if I may.

Mr. Jim Eglinski: Yes.

Mr. Christopher Porter: I have a somewhat different outlook in this from my colleague.

In no particular order, things that could be tried that would improve Canada's cybersecurity is to put a greater emphasis on diplomacy. The solution to every conflict in cyberspace doesn't have to be the threat of military retaliation or sanctions or indictments. I have not seen any evidence that any of them have worked so far. If we're going to say those kinds of activities successfully deter, we're doing those same activities year after year, but then cyber-threats continue year after year, so where's the relationship? I'm much more of an optimist on diplomacy than I think many others are. If you call a hundred experts, I might be the only one, so it's not fifty-fifty for sure.

The second thing—and back to your question—make sure when you're recruiting people for government service that you're not just looking at the same candidates, that you're open to a diverse candidate pool, both personally, but also in their professional backgrounds. Cyber is a part of everyday life, so it's not just going to be technical people you need to recruit. It's going to be people with all kinds of backgrounds: economists and political scientists and so forth.

Finally, just to emphasize something I said earlier, I think it's a mistake for countries to rely too much on a list of who we are and are not going to defend. To me that's a counter-insurgency problem.

Mr. Jim Eglinski: Can I just cut you off for just a really quick question?

Mr. Christopher Porter: Sure.

Mr. Jim Eglinski: Both your organizations are private organizations supplying security. Are the bad guys equal? I'm saying you're the good guys. Have we got the bad guy organizations out there available to clientele?

Mr. Christopher Porter: Certainly, yes. You can hire services very similar to how you can buy anything else online. That's how those markets are designed, particularly for criminals.

The Chair: Thank you, Mr. Eglinski.

Mr. Jim Eglinski: Thank you for allowing me that question.

The Chair: I didn't know that Washington still thought that diplomacy was important.

Voices: Oh, oh!

Mr. Jonathan Reiber: Can I just assure you that I like diplomacy, in case anyone is wondering.

The Chair: Ms. Sahota, you have five minutes.

Ms. Ruby Sahota (Brampton North, Lib.): Thank you.

There is something that I know all countries have been thinking about, but definitely our government in particular has been thinking about the upcoming election and interference, influence. Legislation has required social media companies' platforms to be more transparent as to who's advertising on their platforms. There's also been a lot of investment in cybersecurity, which is needed, I think, and even more needs to be done.

What responsibility do you think social media platforms have and what kind of greater role can they play in protecting people from fraud when they're using their databases, having foreign actors invading that space and their not knowing or not doing anything about it? Could I have comments from both of you on that?

Mr. Christopher Porter: Most of the large social media companies make significant investments, particularly now, in security and are doing their best, I think, to root those out. I can't speak on their behalf, but many of them do make significant investments. It's just also an enormous task for even a very large private sector company to combat sophisticated foreign military government operations. I think it's asking a lot of anybody's security team to do that on their own.

I would just re-emphasize that for Canada's purposes, a lot of the vulnerability is going to be not just in physical infrastructure. Big databases and physical things are certainly vulnerable as well, but individual candidates and campaigns and the parties themselves are also prime targets for adversaries who want to interfere in your elections.

If they were being targeted on social media or for disinformation campaigns, I don't know if they would have the same level of resources and wherewithal that the infrastructure behind voting would have to support them.

So make sure that individual candidates, campaigns, and the parties are also supported with some of the same cyber-threat intelligence that's provided for the voting mechanisms and infrastructure. I think that's very important. Certainly since 2016, we've seen that most of the threats have been social media-generated threats but they've been at individual campaigns, not necessarily at what's being defended, which is government-run infrastructure.

That's still a vulnerability not just in Canada but throughout the west.

● (1645)

Ms. Ruby Sahota: Yes.

Mr. Jonathan Reiber: Social media companies have certainly invested quite significantly since 2016. One of the things you can read about in their open public communications is the degree to which they've built partnerships with the government. For Canada, I think that for any infrastructure in your country that could be manipulated, that ultimately becomes a very important step for tech companies to take.

If there isn't already an information sharing infrastructure or public-private co-operation mechanism that exists in advance of that election, I would say that we have something called the enduring security framework in the United States, which brings together key IT companies and infrastructure owners and operators with the intelligence community and the national security community to share threat information and design solutions. That's a bit of a longer-term thing, but that's one recommendation.

The second thing I would say is that, at least within our environment, within the United States for our elections systems, election registration is handled by different departments in each state. In those instances where they have not yet done so, organizations need to secure their data centres to prevent people from manipulating the electoral rolls and the registration rolls.

By analogy for Canada, figuring out who manages voter registration and where they store that data and on what server ultimately will help you to make the right investments for manipulating the actual outcome of the election.

I would say that another thing is informing the public very much about what could happen. I think the Department of Justice in the United States was very good at this. Harvard also had a non-profit program that educated secretariats of state across the country in crisis management. You can find that campaign on Harvard's website. It's the defending digital democracy project.

Ms. Ruby Sahota: When did that happen?

Mr. Jonathan Reiber: That was over the last two years.

There are good materials there for how to train election officials to do crisis response and crisis management.

Ms. Ruby Sahota: Was that a result of what happened in the 2016 American elections?

Mr. Jonathan Reiber: It was a direct result of what happened in the 2016 election.

A number of the individuals who run that program—and this is just one among many—have emerged from the administration. They were taking the lessons that they had learned.

I would say that the social media component is obviously quite significant, and the Canadian population needs to be educated about potential risks, and that is certainly a part of it.

With regard to the social media companies themselves, you should engage them to work with them so they can put forward messages on their own platforms in advance to inform their Canadian users about what they're doing to prevent election interference. I believe they're probably already doing that, but that would be another step you could take.

The last thing I'll say, and I know you're out of time.... I'm overly verbal.

The Chair: You figured this thing out.

Mr. Jonathan Reiber: The next step is who's going to be manipulated next? Elections were one thing, right?

The thing that I'm most concerned about is census data. Within the United States we have our census coming up, I think, in 2022 or 2025—I can't remember. Imagine if somebody could break into the research institutions and manipulate demographic data to portray the United States as accelerating one demographic shift or another. That would alter how people perceive our society overall.

Ms. Ruby Sahota: Yes.

Mr. Jonathan Reiber: So, the next step is research institutions that have yet to invest, that do a lot of really valuable research for a country's overall identity. If I were an adversary, that's exactly where I'd be going, and I hope they're not listening.

Ms. Ruby Sahota: Oh boy.

The Chair: It's hard to tell who are the white hats and who are the black hats.

Ms. Ruby Sahota: Yes.

The Chair: Mr. Dubé, you have a generous three minutes.

Mr. Matthew Dubé: Thank you, Chair—

The Chair: Excuse me.

I see that the lights are flashing. That means we have about a half an hour.

I'll go to Mr. Dubé. I'd like to ask a few questions.

My suggestion, colleagues, is to run to 5:10 p.m. Both of our witnesses have come from a long way to talk to us, and there may be follow-up questions.

Is that acceptable to colleagues?

Some hon. members: Agreed.

The Chair: Mr. Dubé.

Mr. Matthew Dubé: Thank you.

Just really quick, since I have my generous three minutes....

You mentioned securing data centres as a way to deal with—I always hate saying the Internet of things; I feel like I'm in a Mary Poppins movie when I do—the Internet of things. Securing data centres, does that also deal with data manipulation? You've talked a lot about that as well, and I think especially in the context of a study on the financial system, that could be an issue as well.

● (1650)

Mr. Jonathan Reiber: Yes. It very much deals with data manipulation in that, in order for you to alter.... Let's say you're trying to redirect a ship, as the Russians did in the Baltic Sea, reportedly. They spoofed GPS and redirected some ships in the Baltic Sea. That's just been reported. Or take the case of electoral rolls where you're altering who's on the roll and who isn't. In order to do that, you need to make your way onto a server, because applications don't just exist in the ether. I mean that in the least patronizing way possible as I say that.

Applications and servers are really, in many ways, one and the same. Anytime you log into a cloud-based application and enter your data, it's touching a server somewhere in the world. If you've secured a data centre from the inside, you're preventing an intruder from being able to move laterally and implant whatever malware for whatever purpose they choose, whether it's manipulation, theft or destruction.

Mr. Matthew Dubé: You'll have to forgive my layperson knowledge on this. This study makes us all feel like Luddites. I just want to make sure I'm understanding correctly.

If someone's not updating their firmware, or whatever, the data centre being secure is enough, even in the event that you have the worst security imaginable on your device. I just find it hard to square that circle. I don't know if I'm understanding it correctly.

Mr. Christopher Porter: I find that hard as well, because I think part of the issue is that many of the most advanced groups use legitimate credentials. If you're the president of the bank, they trick you into getting your credentials, and there is no strictly malicious behaviour; they're just abusing your credentials.

For the finance sector, the question is, if that were to be discovered one day, how far back could you roll that—a day, a week, a month? Could you fix the accounts if they were off? I think manipulation is not so much a criminal issue as it is a potential vulnerability for the finance sector that could pose a systemic risk. To me, it's the number one systemic risk that data would be manipulated at a major bank, and then you wait a month, you wait a year, and you announce to the public that you had this person's credentials, and you changed two or three accounts. It doesn't really matter. Everybody who thinks their bank charged too high of a fee at one time or another is going to be challenging everything that's ever happened on their account.

I think it's a real risk, and most organizations, either by virtue of their size—they're so big and they have so much data, or they're so small they can't invest in doing it—don't know what normal behaviour is on their network. It's very hard to roll back after the fact, if you don't have adequate backups, and it's a real risk for the finance sector in particular.

The Chair: Mr. Dubé.

Mr. Jonathan Reiber: Chair, if I could just—

The Chair: Go ahead.

Mr. Matthew Dubé: You're being very indulgent.

The Chair: I'm being very...yes.

Go ahead.

Mr. Jonathan Reiber: Thank you, Mr. Chair. I'll try to be as brief as possible.

I'm not trying to argue that if you secure your data centre in the interior that you're set and you can go home and sleep. That's not what I'm saying. There has to be a security stack of investments.

In the case of an advanced adversary, who knows that if they penetrate the secretary of defense, or the president or the CEO of an organization, that person has to have very clear...for any individual there has to be some security capability that secures the user at the perimeter—multifactor authentication, firewalls, all of that.

The argument I was making is that if they break past multifactor authentication or encryption, and they make their way in, if they find a low-value server, then if you have invested to secure the interior of your data centre, you're going to be able to limit damage quite significantly compared to if you haven't. If you haven't done it, forget it. They're going to be able to own any application in your enterprise. If you have done it, you might lose *x* and *y* data, you might lose *x* and *y* servers, but you'd be able to manage that cost, unless it's the president or the secretary of defense, or whoever it is who's been hacked. If it's a lower-level person, the damage will be less.

The Chair: That was a generous three minutes.

Mr. Reiber, as I listened to your presentation, you were essentially saying that there are various layers of protection and that you then have this microsegmentation program so that instead of 3,000 access points, you only have three access points.

In the context of the oncoming 5G network, does that model of security protection still prevail?

Mr. Jonathan Reiber: I haven't thought through how 5G would impact our capability overall, nor do I know enough about 5G to really want to advise you on it.

If I were to make an assumption and set my own fictional narrative, I would say that 5G is going to speed up our ability to transmit data. That should not impact the propositions that I'm making. I would say that they still stand, meaning that if it's simply the speed through which data is being moved, then if you've set rules and policy for how your applications and servers interact.... These are a little bit different. They are two different beasts, and they shouldn't negatively impact one another.

If I were to think about a capability that would disrupt the future of computing overall, leaving aside microsegmentation, I think quantum computing would be the main thing I would be looking into for something that would totally alter the nature of cybersecurity. Even then, I don't think the security stacks would be totally disrupted.

● (1655)

The Chair: Thank you.

Mr. Porter, you're obviously familiar with article 5 in NATO's treaty. These cyber-attacks can happen in microseconds. You may be at war and not even know that you're at war.

Do you think that the architecture as described in NATO, which is a treaty that's somewhere in the order of 50 years old, is adequate for responses on cyber-attacks? It's already happened. The example would be Estonia. Do you think that treaty needs to be seriously revamped?

Mr. Christopher Porter: Mr. Chair, I think the mechanisms in the treaty allow for appropriate joint policy responses by the NATO members. I think a bigger issue is who is going to call for such a response and under what circumstances. I think, at least in the States, you're always waiting for a cyber Pearl Harbor, a major destructive event. It's much more akin to cyber trench warfare, only the people in the trenches are private citizens and companies, not soldiers or government actors.

What do you do with that? I think that's the problem the alliance has right now. It's not the legal mechanisms for invoking joint defence. That's being worked through and I think in a true emergency case would be invoked correctly anyway. Again, I think the bigger issue is that you could die a death by a thousand cuts, and no one would ever think it was worth raising as an article 5 issue.

A second much more tactical kind of issue to consider is that the U.S. and Canada both have significant cybersecurity intelligence capabilities in the private sector and in the government, but not all of the NATO allies do. If there were a major cyber-incident and you wanted to invoke article 5, how would we convince the other NATO members that anything had happened or that we had correctly attributed the event?

We might be highly confident in the U.S. and Canada in our joint analytic work on that issue. Many countries don't have enough people on the other side of the table to receive it, interpret it and take a political action.

Do they have the kind of experts that we do? I think that's an issue. How do you share that capability to understand and interpret the attribution of major cyber-attacks? Those are the two issues to me.

The Chair: Okay.

Finally, the U.S. Congress has basically reacted to the Huawei issue by absorbing the idea that a cyber-attack by China would be so fast and so devastating that it would be, if you will, over before it began.

Is that your view as well?

Mr. Christopher Porter: Mr. Chair, I think that if you were constrained to only conduct such a conflict by cyber means, that might be a reasonable interpretation. However, while there are significant risks, responses to cyber-attacks obviously don't have to be limited to that domain. I would defer to my colleague on how that would play out in the real world. I don't necessarily share that defeatist view, no, because of the other more conventional options that the United States would have in order to respond.

The Chair: Mr. Reiber, do you want to add anything to that?

Mr. Jonathan Reiber: Sure.

I also don't endorse the view that China would simply win a cyberwar, instantly. I think that, certainly, multiple countries have developed the capability to conduct destructive attacks on critical infrastructure, globally.

Of Russia, China, Iran and North Korea, the one that I'm by far the most worried about is Russia. The reason is that they've implanted malware across elements of the U.S. electric grid, and it wasn't clear why.

I don't think, if any one of these adversaries initiated a conflict in cyberspace, that it would terminate in a manner favourable to their terms so quickly, because we've invested in the cyber mission force. That's a large capability of 6,200 elite trained hackers and operators who are watching those countries quite closely.

If you go through an escalation ladder and consider China and Russia in particular, China even more so, they're deeply intertwined with our economy. They know that any element of escalation in cyberspace that goes beyond a certain level is going to begin to have significant economic consequences for them, if it leads to any kind of military confrontation.

I recently wrote a piece about why I think China is the greatest long-term threat in cyberspace. Really, it's because of their advanced weapons development in other domains, like railguns. It's for that reason that the U.S. invested in the third offset strategy that Shawn Brimley led. If we look over the 20-year span of what could happen between these two countries, we'd see an element of keeping parity in terms of technological development.

To my colleague's point, this is an outcome that you want to obviously avoid. It's not something that's in either country's long-term interest. It's in both of our interests, from the United States' and China's standpoint—also for Canada, I imagine—to maintain productive, peaceful relations that over time will lead to the economic flourishing of everybody in the Pacific and beyond. That ultimately comes down to issues of diplomacy and speaking to them about what escalation means and what it doesn't.

In our back pocket, however, we do have to preserve these technological options for the potential for conflict, unfortunately.

● (1700)

The Chair: Okay, thank you.

Mr. Spengemann, did you want to ask a question?

Mr. Sven Spengemann: Yes, Mr. Chair. Thank you very much. I'll be brief.

I just wanted to get you on the record. This is the public safety committee. Going back to business to business and potentially even large business to small business cybercrime, could you talk a bit about the basic law enforcement model?

First of all, start with the lack of reporting. I think you've addressed that in part through your point that we need to look at bridge management requirements as a way to encourage companies to, first of all, report cybercrime incidents. Second is the collection of evidence. Third is prosecutions. Are there prosecutions under way that stay within the North American context? I think it's terribly difficult if we have foreign actors or foreign-based companies.

What about the basic law enforcement model and its application to cybercrime in 2019? Have you any thoughts on that?

Mr. Jonathan Reiber: I'll be very brief on this.

The FBI plays a very important role in prosecuting cybercrimes within the United States and, from the national security division, for actors from the outside that conduct attacks against the U.S. As far as I know, it's the only agency within the national security community that has the authority to conduct cyberspace operations to shut down a server inside the U.S.

We do have a tradition of gathering evidence within the Department of Justice. The FBI and the Department of Justice work very closely together. I wish I could refer you to a case to give you a good example right now, but I can certainly find more to send to you. But this is—

Mr. Sven Spengemann: The capacity is there. The staffing is there.

Mr. Jonathan Reiber: Yes, definitely.

Since the Computer Fraud and Abuse Act.... I want to say it was in the 1980s but I'm probably wrong about that. Don't ever do math in public, or cite dates that you don't know about.

Since the Computer Fraud and Abuse Act, when people inside the U.S. were doing hacking against targets....

A good example is the Dyn case, if you're familiar with the attack. It was so significant that it slowed down Netflix and Twitter, these vital organizations. Everyone was wringing their hands. The Director of National Intelligence went on the record saying this was such a bad threat. It was three people in the United States, who I think are now doing community service, helping the government deal with cyber-attacks.

This was led by an enterprising FBI agent out of Anchorage, Alaska. The way the FBI works, different offices around the country have the ability to do these investigations. They did all of their forensics and figured out who it was.

Mr. Sven Spengemann: Mr. Porter, have you any quick thoughts?

Mr. Christopher Porter: Yes, certainly the RCMP has significant technical capabilities to investigate those crimes on its own. FireEye supports a variety of investigations in Canada at a technical level.

I can't speak to Canada, per se, but in the States it's very important that victimized companies feel comfortable sharing information, that they're either indemnified or that it won't be held against them. That's vital, if you want that threat information, particularly if you think that, whatever case it is, it's not just a criminal issue but could be a national security issue. You want to be clear in law that it's okay to share breached information without that being held against the company, individually.

The Chair: Thank you, Mr. Spengemann.

We have about 15 minutes before the vote.

Mr. Paul-Hus, you have the final question.

Mr. Pierre Paul-Hus: Thank you, Mr. Chair.

We're here to do a study especially about the banking sector. When we had our meeting in California, you talked about the French and how they have strong aggressive measures against cyber-threats. Could you explain that a bit?

Then the last question is about your banks in the U.S. Are the U.S. banks well protected or do they need more protection? How can Canada do better?

● (1705)

Mr. Jonathan Reiber: I think a number of nations have passed stringent regulations to help protect critical infrastructure. The French example for ANSSI, and the directives that have been developed, I think are a very good example. My sense is that they have greater amounts of control over their critical infrastructure from a mandate standpoint than the United States.

Our example, as I mentioned earlier, stems from the section 9 list. We went through and asked what the most important critical infrastructure in the U.S. is from a protection standpoint.

We do not yet have a national data and privacy protection law in the United States. For breach management, we have our states, and each state has a different role. California and Colorado have passed this more aggressive version. GDPR is very aggressive from that standpoint. It mandates a very short period of time to prove that you have a breach under control and levies a penalty if you haven't.

I think the French example, GDPR, and the California and Colorado state regulations are the most progressive and have fairly strong teeth. That doesn't mean they've won friends. A lot of sectors feel now that they have to have a compliance officer to handle all of these requirements, and it can be a lot of work. I think the nature of cyberspace says, “Look. That's too bad; you're just going to have to do it.”

The interesting thing about the financial sector is that it has been under attack probably since it moved over to the Internet. There are a number of major breaches that have caught the attention of the national security community as well as the banking sector, and it has led the banking sector to invest quite a lot in cybersecurity capabilities. It's for that reason that they're so far ahead.

I may have already commented on this, but they're much further advanced than a lot of the other sectors in the U.S. You could opine that part of the reason is that they're able to attract the best talent to their workforce. They're able to pay good salaries to attract people who want to work hard.

My general belief, and this is putting on my historian's hat and looking at all of these sectors, the cyber mission force and the evolution of cybersecurity strategy.... When I first started working on this in 2010—I mentioned the time of Shawn Brimley—you couldn't attract people to work in the cyber-policy office in the Pentagon. It was a bunch of nerds; everybody thought they were just computer geeks.

Now it's a problem that affects all of us. My view is that we now attract such talented people across sectors that we're going to be able to solve this problem. I really think we're going to be able to solve it and people will be able to implement good technologies. The banking sector will have led the way, and someday somebody will write a history of the banking sector where people on the inside talk about what it was actually like.

Mr. Pierre Paul-Hus: Thank you.

The Chair: Thank you, Mr. Paul-Hus.

Mr. Picard has a critical question.

Mr. Michel Picard: Yes. It is technically a yes or no answer.

Do you gentlemen have an Alexa gadget at home, or Google Home?

Mr. Jonathan Reiber: If I had my druthers, I wouldn't have a television.

Voices: Oh, oh!

Mr. Christopher Porter: Yes, seconded.

If I may, I would like to answer his question as well.

The U.S. finance sector is well defended, but it's not just about making an investment of money and technology; it's also about how empowered the people are. If the security operations centre at a major financial institution in Canada, for example, discovers a problem, are they empowered to go down and stop trading? It could be millions of dollars to stop trading in order to remediate a problem. Two companies in the same sector across the street from each other spending the same amount of money on security can have very different outcomes depending on how empowered the people are to affect particularly trading operations.

I would add, as an aside, that bigger than the finance sector but still a systemic threat to Canada's economy, most publicly traded companies that I talk to wish they could invest more in cybersecurity. They don't feel they can justify it, because in the short term it hurts their bottom line. It's viewed as a cost centre. That's an area where regulation helps, because absent that regulation or industry standards, there's a first mover disadvantage: investing in cybersecurity hurts your perceived return.

Those are two things to consider that disincentivize proper cybersecurity.

The Chair: With that, I'm going to adjourn the meeting.

On behalf of the committee, I thank both of you, Mr. Porter from Washington and Mr. Reiber from California, for your efforts to get here. It has been very informative.

Similar to Mr. Dubé, I do feel a bit like a Luddite listening to some of this, but hopefully over time we'll become a little better than that.

Again, thank you.

● (1710)

Mr. Jonathan Reiber: Thank you, Mr. Chair.

Mr. Christopher Porter: Thank you, Mr. Chair.

The Chair: The meeting is adjourned.