HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

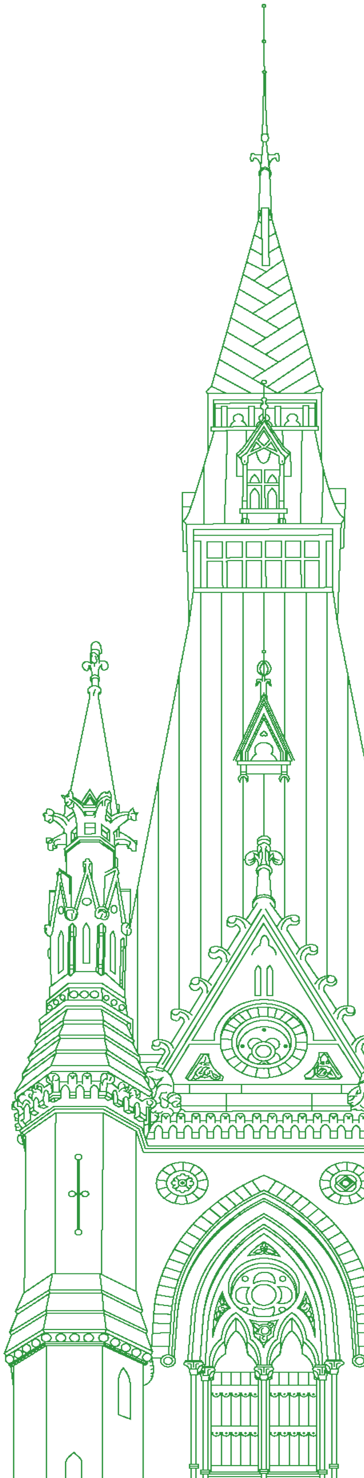
Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 028

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Tuesday, June 7, 2022



Chair: The Honourable Jim Carr

Standing Committee on Public Safety and National Security

Tuesday, June 7, 2022

● (1205)

[*English*]

The Chair (Hon. Jim Carr (Winnipeg South Centre, Lib.)): Pursuant to Standing Order 108(2) and the motion adopted by the committee on Thursday, March 3, 2022, the committee is resuming its study of the assessment of Canada's security posture in relation to Russia.

With us today we have, as an individual, Dr. Ken Barker, professor, institute for security, privacy and information assurance at the University of Calgary; Juliette Kayyem, Belfer senior lecturer in international security at Harvard's Kennedy School of government; and from Beauceron Security, David Shipley, chief executive officer.

Welcome to all of you. I will be asking you to make a five-minute opening statement. When you have 30 seconds left, you will see this card. I'm pretty strict about time, to be fair to everybody.

I would now like to invite Dr. Ken Barker to make an opening statement.

Sir, the floor is yours whenever you're ready.

Dr. Ken Barker (Professor, Institute for Security, Privacy, and Information Assurance, University of Calgary, As an Individual): Thank you very much for inviting me. It's my pleasure to join you today.

I'm going to probably say some things here that are maybe a little bit different from what you might be expecting from a security expert. Specifically, I'm going to talk about how the cyber-attack vulnerabilities really have not changed since the start of the Russia-Ukraine war. What I'm talking about is that the vulnerabilities haven't changed, not necessarily the threat posture.

Basically, exactly the same threats exist now that were available before. The Russians are unlikely to have gotten any better at their attacks in the last two months or with the onset of the Russia-Ukraine war. Nothing's really changed, so what's going on with Canada's vulnerability?

As an energy producer, Canada is more likely to be targeted by an attack from Russia. Obviously, the pressures from sanctions, etc., are causing them to look for potential opportunities to attack alternative sources that might support the west. Attacks on these sectors have occurred since the start of the war, but it appears the sector—as a vulnerable resource and as part of Canada's critical infrastructure—was well prepared and has actually successfully defended the attacks that we have seen over the last two months.

Attacks are actually quite different from successes. There are actually a staggering number of attacks from all actors, state and stateless, on a daily basis and they've been going on for years. If these were not appropriately defended, this would have been a serious problem long before the war itself. In fact, it has been a serious problem and we've done a lot of things to try to protect ourselves.

However, we don't know what we don't know, so there is something called zero-day attacks that could occur. These are unknown attacks from before. These can be launched at different times on us unsuspectingly because we're just not prepared for them. We don't know that they're out there or what these vulnerabilities are. However, we haven't seen an increase of those over the last two months. Likely if attacks were being launched at this point of unknown origin then we would probably have had some kinds of cracks in the systems, but we haven't really seen that in the way that many people expected.

Canada's making an investment through the CSIN program and I think this is a key step in the right direction. It's a critical investment in Canada's current and future cybersecurity. This was initiated in 2019, long before this occurred, so the reality is that Canada has actually made some pretty good steps in the last little while in order to set itself on a very solid footing.

What we really want to do is build some sort of a cyber-safe ecosystem. Canada's critical infrastructure in general is vulnerable because it's built on legacy systems that are known to be particularly vulnerable. What I mean by legacy systems is that they're systems that were in existence before the Internet of things started to occur. With the advent of the IoT and the need to replace old components with Internet-connected ones, we are actually opening up a potential threat and attack on some of our critical infrastructure. This is part of what's being investigated both in terms of research and at the corporate level within the private sector.

Large corporations are actually likely to be reasonably well protected right now. The reality is that lots of money has been invested by the private sector because they recognize their vulnerability. As a result, they've managed to move things forward quite a bit over the last 20 years. Small and medium-sized enterprises, however, are simply vulnerable to various attacks and additional investment needs to be made to protect them in some sort of way. However, they are unlikely to be a specific target from Russia unless they exist in certain cybersecurity sectors and/or are suppliers to the critical infrastructure.

The key issue is that we have a critical shortage of experts in this area. Post-secondaries are trying to address that. We need to upskill and re-skill existing workers. We have a lack of education and knowledge in the workforce and in the general public, and hiring international expertise might help but it's unlikely to be sufficient simply because they're so much in demand.

With that, I'm done.

● (1210)

The Chair: Perfect. Absolutely on the schnozz. Way to go.

I now invite Ms. Juliette Kayyem to make an opening statement of up to five minutes.

Please proceed whenever you're ready.

Ms. Juliette Kayyem (Belfer Senior Lecturer in International Security, Harvard Kennedy School of Government, As an Individual): Thank you for having me. One of my former students is now an MP. Taleeb was in there... I can't see a thing, but it's a thrill to be here.

When I was asked to be here, I made it clear, because I wanted to declare, that the exact risk assessment for Canada is not something I'm an expert in. I'm an expert in what in our space and what I've worked on globally is called “right of boom”, which is essentially what the capacities are, especially in the cyber-field, assuming that a bad thing is going to happen.

Like Ken was saying, there are a lot of questions about increased vulnerability for a country like Canada, given the Russian conflict. There is a big issue in my space, in the sort of preparation space, around why we haven't seen more activity. The answers to that may be be multiple. The best one we know so far is that maybe, much like military capacity, Russian cyber-capacity to destroy as compared to disrupt—disruptions we can handle—was overestimated. It could also be that the invocation of article 5 by NATO might have had a disciplining effect, the idea that any attack on critical infrastructure that impacted individuals would be viewed as an attack similar to a military attack. We don't know and we're not done yet, so what does that mean for preparation for that?

Overall—and I was just in Canada getting a briefing on this about two weeks ago, so it's a funny coincidence—much like the United States, Canada's focus and its private sector critical infrastructure focus have been on what we call “left of boom” capabilities—in other words, stopping some sort of infiltration, some sort of boom, so to speak. Those are important and those are essential, but what hasn't been done enough, especially in coordination with the United States and the northern states, is what would happen if there was a disruption.

We measure success on whether you can stop more harm from occurring. In other words, how quickly can you respond? How quickly can you get systems back up? My standard is this: Can you make something less bad? In the cyber critical infrastructure space, as Ken was describing, there's a tremendous amount of focus on stopping the hack, the ransomware or the nation-state, and less on what you would you do if that were to happen. Do you have more than an on-off switch, which is generally what these have?

There have been lots of lessons learned so far because of this. We've learned this from Colonial Pipeline in the United States, which didn't have much capacity.

A lot of it has to do with response time. Do you know when your system has been infiltrated? How quickly can you protect yourself from what we call cascading losses? In other words, even if there is a disruption or a destruction, which is something even greater, can you stop the cascading losses and can you require the private sector to do that?

What does cascading losses mean? It's just essentially that there is the initial thing, and then there are all the things that happen after the fact that could have been stopped if you had been able to manage the harm.

The second is what sort of regional planning has occurred. We certainly know in this space that no company acts alone, no locality acts alone, but in terms of regional planning and communication, we know that there is a need for a greater understanding of what the consequences of the vulnerability are. It's not just what the risk is, not just what the vulnerability is, but what the consequences of the vulnerability are.

Then the third area where there is a lack is, I would say—and this is going to sound familiar, I think, across every country—more communication about whatever risk you are seeing in the government to the private sector so we could begin to prepare.

● (1215)

The Chair: You have 10 seconds.

Ms. Juliette Kayyem: It's consequence management capabilities. It's all about response when you cannot exactly measure what the risk is.

Thank you.

The Chair: Thank you very much.

I would now like to invite Mr. David Shipley to make an opening statement of up to five minutes.

The floor is yours, sir.

Mr. David Shipley (Chief Executive Officer, Beauceron Security): Thank you, Mr. Chair, and thank you to the committee for the opportunity to be here.

I'm going to talk about three key recommendations. The first is the need for mandatory incident reporting so that we actually know what's happening left and right of boom. Second, I'm going to talk about the need for standards in basic cyber-hygiene to try to prevent the likelihood of incidents happening. Third, I'm going to talk about the desperate need to help small and mid-sized businesses and the subnational public sector—health care, municipalities and higher education—to secure themselves.

My name is David Shipley and I'm the co-founder and CEO of Beauceron Security. I have worked in cybersecurity for the past decade. I hold a certified information security manager designation from ISACA, and I've spoken with Canadian media hundreds of times over the past decade about cyber-attacks and social media manipulation.

Beauceron serves nearly 600 customers ranging from North America's biggest banks to national telcos, government, small business and more. Our technology is used to educate more than a half a million people to know more and care more about their role in cybersecurity. According to the Verizon "2022 Data Breach Investigations Report", 82% of all cyber-attacks succeed because of the human element of cyber, whether that's people falling for expert use of emotional manipulation in emails known as phishing, or human error in the use or design of technology. The word "cyber" itself points to the importance of the human element. Cyber comes from the Greek word *kubernetes* and it's focused on the relationship between people, technology and control. A future in which individuals, organizations, governments and society are in control of the technology they rely on every day is a bright one for Canada, but that is not our dysfunctional present.

Those who seek to harm Canada and its interests understand how to use technology and control harm. Russia's capability in this regard is well documented. They have developed the capability, with state-backed hacking teams, to cripple critical infrastructure, as was mentioned earlier, hack into political parties and governments to find and leak sensitive information, and more. They have cultivated a robust cybercrime industry and have relationships with organized criminal gangs to avoid accountability for their actions. Russia also understands the use of websites and social media platforms as a means to control people with disinformation. Marcus Kolga with the Macdonald-Laurier Institute and others have documented this well. Social media manipulation is part of the spectrum of weapons when we talk about cyber-conflict.

Russia's actions in cyberspace have had severe consequences for Canadians. Cyber-attacks from Russian criminal gangs have crippled Canadian municipalities, health care organizations and more, with costs into the tens of millions of dollars. The cybersecurity firm Emsisoft estimated there were more than 4,000 Canadian organizations victimized by ransomeware alone in 2021, with estimated damages as high as $654 million.

While the Government of Canada has made significant efforts to protect itself from cyber-threats, most of the rest of Canada is in the hands of the private sector or subnational public sector. To reduce that risk we must get better insight into cyber-attacks, improve our regulations on basic cyber-hygiene and increase our resources to our most vulnerable organizations.

First, we must implement mandatory cyber-incident reporting that goes beyond federally regulated industries and that includes health care as well as vital supply chains, including manufacturing and food. We are lagging behind the United States and Europe in this respect. Most organizations are not going to voluntarily engage with the federal government during incidents. They are told by their legal and risk teams, or by their insurer, to limit information sharing and disclosure since working with government is seen to offer limited gains and to present much to lose. This means we lose crucial insights into attacks on Canada and, even more importantly, root causes and key lessons are not learned or shared effectively.

Second, we need national mandatory cyber-hygiene. CyberSecure Canada is a great start, but voluntary uptake will continue to be low. We need to take a lesson from the U.K.'s similar programs and tie access to government procurement with achieving basic cybersecurity standards.

Third, our most vulnerable sectors are the subnational public sector, such as higher education, municipalities and health care. They need dedicated funding from the federal government to improve their security as quickly as possible. On the private sector side, our small and mid-sized businesses desperately need help affording the security tools they need in an increasingly hostile environment.

I would be remiss if I didn't comment on the need to regulate social media as an important part of our national cybersecurity strategy to put Canadians in control of the technology they use. Social media algorithms that amplify fear, anger and hatred are tools highly leveraged by Russia and other enemies to fracture our society. We must give back to Canadians control over the content they see by mandating that the default view for social media be one of chronological order, not one algorithmically decided, and require an opt-in model for algorithmic content.

● (1220)

The Chair: You have 10 seconds, please.

Mr. David Shipley: Failure to act today damns us to a future where our businesses are crippled from waves of foreign extortion attempts, our citizens and politics are poisoned with division and disinformation, and our ability to provide the essentials of life is significantly diminished.

The Chair: Thank you very much, sir.

Thank you all for your remarks. We now move into the first round of questions.

Leading off will be Ms. Dancho with a six-minute slot.

Ms. Raquel Dancho (Kildonan—St. Paul, CPC): Thank you, Mr. Chair.

Thank you to all of the witnesses for being here and Mr. Shipley for being able to be here in person.

My first question is for Mr. Shipley.

I wanted to pick up on a few of the recommendations you had for the mandatory cyber-hygiene. One that I picked up on was tying it to government procurement requirements. Do you have any others that you would recommend?

Mr. David Shipley: The idea of tying it to government procurement came from the U.K. cyber essentials program, which is what some of our program was modelled after. They dramatically improved their supply chain security for the U.K. national government. The benefit to the rest of the country is that they had a more secure SMB sector. This is a great starting point.

We've seen the benefits of good hygiene. The efforts by Ukraine and the United States government to prepare for the conflict we now see has significantly reduced the impact of Russia's efforts in that country. Good hygiene and good left of boom saves us a lot of misery.

I've been on the phone with a small or mid-sized business. It was a hardware store. They'd been hit by ransomware. This was the worst three days of that owner's life. It turned out to be weeks to fully recover. They were back to pen and paper. Had they only had more help and resources or an incentive to invest in security and the help to do it, they could have avoided that bad day.

The last thing I'll mention about supply chain is that you never know how a supply chain vulnerability will play out. It was tax software in Ukraine that led to the crippling in 2017 with the massive wiper malware called NotPetya. It was a small tax software firm.

Small and mid-sized businesses can have an oversized impact. We just don't know how the combination will come out.

● (1225)

Ms. Raquel Dancho: Can you give us some examples of how we can...? You mentioned the small hardware store. What role does government play to incentivize? What does that look like? Is that like a tax break? What would you imagine that could be?

Mr. David Shipley: Well, 48% of small businesses don't spend anything on cybersecurity today. It could be in the form of tax credits. You could also look at models like CDAP, which has helped with digital adoption and was much needed in the pandemic. Unfortunately, that digital adoption has actually increased vulnerabilities for small and mid-sized businesses.

We need to tie being secure into grants, loans and other things that have a direct tie to businesses.

Ms. Raquel Dancho: Thank you very much.

I just have some questions now for Mr. Barker.

You said recently on a podcast—I believe it was Cybersecurity Cubed—about the threat of quantum computing to our existing cybersecurity and cryptography networks. Can you provide some feedback to the committee on how Canada is performing in this sphere?

Dr. Ken Barker: I probably need a bit more context for the question.

The existential threat from quantum is probably a future one. It's not a current one, in the sense that it's actually a threat to the cryptographic systems in place that we currently use to operate all of our systems.

I'm trying to avoid getting too technical here.

A future possibility is that quantum computing could effectively undermine all modern encryption techniques and shorten the lifespan, if you will, of how long something could be considered cryptographically safe. That threat isn't current. It might be 10 or 20 years away, to be blunt. Certainly people who champion quantum technology would argue that it could be just around the corner. They're not wrong. The reality is that it's probably quite some distance in the future.

The threat, though, is still real today in the sense that if it's cracked in 20 or 25 years, we would probably have quantum-safe cryptography available by that point. However, the existing stuff that's currently being secured by modern encryption becomes vulnerable 20 years from now. If it's stored some place in an encrypted way and we think it's safe for the next 2,000 years, it could become vulnerable at that point. All of that legacy encrypted data that we consider very secure at this point could become very vulnerable at that point. Much of it could be released or hacked into and be sitting out some place. It could become vulnerable at that stage.

I'm not sure if I've actually answered the core of your question. It's a very complicated one.

Ms. Raquel Dancho: Yes. I think you've given us all a bit of crash course on this complex issue.

Are any of our adversaries aggressively pursuing this? Are they investing in this? Have you heard of their discussing this?

You mentioned it could be in 10 years, 20 years or 25 years that all of our encrypted technologies could be at risk of quantum computing from adversaries. Should we be having these discussions now, or is it a bit too early?

Dr. Ken Barker: No, I think we should be having these discussions now. The mechanisms that we might want to put in place 20 years from now are going to take 20 years to develop. We're talking about doing fundamental research and development efforts.

Canada, in many ways, is leading in this space. We made investments several years ago that were critical to moving to promoting quantum, but I will say that the rest of the world is starting to catch up. I think there's an opportunity here for us to be world leaders in that particular space. That will, obviously, help protect our cybersecurity.

● (1230)

The Chair: Thank you very much.

Ms. Raquel Dancho: Thank you very much.

The Chair: I would now like to turn to Mr. Noormohamed for his six-minute block of questions.

The floor is yours, sir.

Mr. Taleeb Noormohamed (Vancouver Granville, Lib.): Thank you, Mr. Chair.

Thank you to all the witnesses for being with us today.

In particular to my old professor, Professor Kayyem, it's good to see you. I'd like to, if I could, kick off with a couple of questions for you, please.

You talked about disruption and destruction, and the fact that we can handle disruption but destruction is a whole different ball game. My concern is that one challenge we've been dealing with is that when we look at the impact of Russian bots in terms of spreading misinformation.... First, they were spreading COVID misinformation and trying to sow misinformation with this idea of breaking down trust in public institutions. We saw a proximity of that narrative to far-right extremist views, and then, lo and behold, a connection to very pro-Russian, anti-Ukrainian messaging online.

I'm wondering whether or not this erosion in the public perception of policy starts to move into that realm of destruction in a way that we perhaps haven't thought of. I'd love your thoughts on that. In Canada, certainly, we are starting to see it. It's something that I think all of us here are quite concerned about.

Ms. Juliette Kayyem: I think that's right. I think you're exactly right that not every crisis is a disaster. In other words, if we're built for it, we can—for any type of attack—survive something if we're prepared for it.

It becomes—in words that I quote from the NATO language—“destructive” if you cannot manage even the smaller things. They build on each other. This is the notion of cascading losses. If you cannot stop the harm close to the vulnerability...although you don't even know what those impacts will be downstream, especially in the cyber context, which is what we've experienced with critical infrastructure here in the United States. In a simple ransomware attack like the Colonial Pipeline, which was really simple and not that sophisticated, because they did not have a response capability, it meant the whole system was down for a week. That's not sophisticated.

One way to think about the relationship is.... As a nation and as a government, you're really focused on—from Russia—the destructive stuff. I think NATO made that clear in its language. It's not going to define what the difference is between a disruptive attack and a destructive attack. I think that's been good. In other words, that is actually keeping enough vagueness in the system so that the adversary doesn't know where the line is. The last thing you want to do is to say, “We would view this as destructive and this as only disruptive”.

I think the best response.... This is, now, not the world of rocket science. The fact that we talk about cybersecurity or cyber-attacks make them seem technological. On the response side, it's really not that sophisticated. You don't need to know coding. A lot of it is having communication systems that have multiple defences and systems that stop the cascading losses, in other words, bifurcated or divided regional support systems that can service mutual aid. If an energy system went down, you could share or get systems from others. Those are tried-and-true emergency management capabilities.

I've spent a lot of years trying to focus the cybersecurity world on how you don't have to reinvent the wheel. A lot of what we've learned from both disruptive and destructive attacks was already known.

Mr. Taleeb Noormohamed: Building on that, as we think about the world of cyber...which, for whatever reason, people still see as overly complex and perhaps it isn't as complicated as we perceive it to be, as you articulated. When you look at what has been happening in the United States and you look at where Canada resides on that spectrum, and then when we think about the context of what you said in terms of Russia's inability to prosecute a ground war well and, arguably, either Russia's inability or lack of desire to prosecute an online war right now, what should we be thinking about in terms of Russia?

Are there things that we, the west, are missing in terms of where the next thing might come from? If so, can you share some of your thoughts on that? Where should we be pointing our attention, so that we're as prepared as we can be?

● (1235)

Ms. Juliette Kayyem: I don't even want to pretend to know what the strategy is, but now, unfortunately, we—being the Ukrainians with the support from both of our countries—are likely to be in some long slog that is less transparent because it's not in the major cities. The media, the U.S., Canadians, we will all get less interested in it.

In terms of vulnerabilities, we may get back to an era when there was no disciplining impact, and ransomware and other actors were able to run freely, utilizing Russia and its capabilities. It may look less state-sponsored, but it is state-sponsored.

The Chair: Thank you very much.

Ms. Michaud, I now turn to you for a six-minute block of questions whenever you're ready.

[*Translation*]

Ms. Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Thank you, Mr. Chair.

Thank you to the witnesses for being here today. We certainly appreciate it.

I'm going to turn to Ms. Kayyem.

I want to read something that appeared in the *Washington Examiner* about your book, *The Devil Never Sleeps*. Here's what the article said:

[*English*]

> [It] emphasizes that government and private-sector leaders should no longer focus all their attention and resources on disaster prevention.
>
> Instead, they must learn how to plan accordingly and use all available tools to minimize the negative consequences when disaster does arrive.

[*Translation*]

You say that we should have anticipated Russia's invasion of Ukraine, and that we should have considered what would happen and how we would respond. You talk about focusing less on prevention.

I'd like you to talk more about that. We've heard from a number of experts who said that Canada was not adequately prepared to deal with threats or cyber threats, as compared with other Five Eyes countries, for instance.

How, then, should Canada have prepared, or be prepared going forward, for possible threats to its critical infrastructure from giants like Russia?

[*English*]

Ms. Juliette Kayyem: Thank you for that question.

In some ways, the limitations that exist before a war, such as your capacity or your access to intelligence, will exist even during it. Thank you for the mention of the book. I will say that I've spent 25 years in what we call “all hazards”. Essentially, I'm not looking solely at cybersecurity. I'm looking at the vulnerabilities that nations like yours and mine have. I've been working a lot on the notion of a North American regional response capacity in cyber and climate change, because the kinds of attacks that we're seeing now and the kinds of vulnerabilities that we're seeing now are going to take a combined U.S.-Mexican-Canadian focus, just given our capacity.

That we need to focus our sense of success on whether we can respond and minimize the harm is particularly true in this space. Something that I would urge you to push on the private sector, which has essentially.... This is probably a little crude, but they have essentially focused almost all of their security efforts on “left of boom”. In other words, if we can stop the breach, we'll try to stop bad things from happening and stay, as I like to put it, on the left side of boom. One thing that can be pushed is to ask what their response planning is, what sort of tabletops, if they have a cyber-attack.

The most important thing I'm going to leave you with is this. The bifurcation of cybersecurity and physical security, which has happened in your country and my country, has to be remedied somehow. As we see in all of these attacks, there's really no such thing as a cyber-attack any more. It is a cyber and physical attack. What's happened in a lot of these companies, as I know you're aware of and what's happened even in some of our government institutions, is that both the cybersecurity apparatus and the physical security apparatus—the traditional gates, guns and guards, as we call it—have been built. There are not a lot of synergies between them if there is in fact a cyber-attack, and I think we have to really push that on the private sector.

There will always be physical consequences. These are rarely just issues about privacy or private information or reputation anymore. The adversary wants there to be disruptions and, worse, even destructions.

● (1240)

[*Translation*]

Ms. Kristina Michaud: Madam Chair, I'm going to use my remaining time to ask Professor Barker a quick question, seeing as he's the expert on computers and data repositories that safeguard confidentiality.

In May 2022, the University of Ottawa released the following publication:

[*English*]

How Canada can adapt to a deteriorating security environment, a report by the task force on national security of the graduate school of public and international affairs.

[*Translation*]

In it, the authors urge the government to create a government-wide, top-secret cloud, as many of our allies have done in various forms. This cloud would include vast amounts of data stored by every department and agency, providing a concrete way of protecting the data in the event of an attack.

What do you think of the idea of creating a top-secret cloud to store confidential government information? Would that be a good way to protect against cyber-attacks?

[*English*]

Dr. Ken Barker: I would first challenge the question a little bit. I don't know what a “top secret” cloud is. If a cloud is a shared resource that people have access to for lots of good reasons, then in order to make that top secret you have to do it with access control. Access control is basically just a system where your top secret data is stored and you limit the access to it in some way.

The Chair: You have 10 seconds, please.

Dr. Ken Barker: Thus, I don't actually think.... The vocabulary is maybe populist, but it's not the right vocabulary.

The Chair: Thank you very much.

Mr. MacGregor, it's over to you for a six-minute slot. The floor is yours.

Mr. Alistair MacGregor (Cowichan—Malahat—Langford, NDP): Thank you, Mr. Chair.

Professor Kayyem, I'd like to start with you. I wish we'd had you here before our last meeting, because our previous meeting was with the emergency preparedness minister, Bill Blair. The committee had the opportunity to question him on his role. As you're aware, the Department of Public Safety and Emergency Preparedness was split. We now have two ministers responsible for those two respective areas.

With regard to a lot of what you've been talking about, when I look at the minister's mandate letter for emergency preparedness.... You can read it there online. Our committee ultimately wants to table a report with specific recommendations.

Looking at what our Minister of Emergency Preparedness is responsible for, is there anything you would like to see in that report for the minister to specifically focus on?

Ms. Juliette Kayyem: There are two areas that I would focus on, given my understanding, which is not as deep as yours.

The first is the cross-border emergency management capacity. If there is a cyber-attack in Detroit, say, in the auto industry, in the OEMs, what capacity, what communications and what structures are in place that are going to essentially treat it as a borderless response? Because it has to be. It's going to impact both countries. It's going to impact, as we've seen with some of the protests recently, border crossings and our capacity to move across the border. Primarily, that would be one.

There's the other thing in terms of what the mandate should be for the emergency manager, because I agree with you. I think the distinction between public safety and emergency management can be hard at times. I said one requirement, but there are two requirements. What is the minister requiring in terms of what we call, in my space, “all hazards” response? In other words, you can't focus just on what the cyber-response is going to be. It's going to have all sorts of impacts. The same is true of climate and the same is true of a terror attack. The consequences are going to be generally the same.

I sometimes think—and I know you certainly do—that in the way the government is structured, and in the way the ministries are structured, we put information security off to the side in protecting our networks. I would just get much more forceful in terms of what reviews are being conducted, what capacity there is, what the consequences would be physically of a cyber-attack on major industry and then what we are doing to close that gap between information security and physical security.

I will tell you that I now advise a lot of companies to not have chief information security officers, chief security officers, and to just have chief preparedness officers, because it's too hard to figure out what the risk might be.

● (1245)

Mr. Alistair MacGregor: Thank you.

Mr. Shipley, I'd like to turn to you.

Can we make any recommendations? What kinds of investments are there in the field of deterrence? Can we make people who are potentially considering a cyber-attack, whatever form that may be...? Are there good defensive options? I'm just thinking of the old adage that the best defence is a good offence. Is that kind of capability being developed?

Mr. David Shipley: I don't have specific insight into what CSE's operations are. We do know that legislative powers were granted and the ability to conduct operations has now begun—

Mr. Alistair MacGregor: Does this exist in the private sector, then, that you are aware of?

Mr. David Shipley: We absolutely do not want the private sector shooting back, because, first of of all, attribution is really hard. I ran cybersecurity for a university. We got hacked all the time and were used as a platform to attack government entities, private sector entities, etc. If someone started shooting back at my university because from their perspective we were the originating source, they would be hitting the end target. It's a fun little shell game.

Attribution is really hard. The private sector absolutely should not be shooting back. That should be a sole responsibility of the federal government, and it should be exercised. I think the challenge from a policy standpoint is, what's policing and what's military? We need better clarity on that, and we do need to flex. It's important that government actually speak forcefully about this.

We saw this with the Biden administration after critical infrastructure attacks in the United States. It was straight from the top: Don't mess with us. Who is the minister that actually is going to respond here in Canada?

Mr. Alistair MacGregor: You mentioned the mandatory incident reporting. We have seen problems through other studies that we've conducted. Whether it's on ideologically motivated violent extremism or it's a firearms study, when you don't have the appropriate range of data, you make poor decisions at the top. If you want to expand on that, how important is it that we have a full picture of the range of threats coming at us and can deploy our resources appropriately?

Mr. David Shipley: My greatest concern right now is the threat to Canada's health care sector. Obviously, we're still in the pandemic. We're still recovering. When a hospital goes down, it goes down for weeks. Cancer patients don't get timely care, other surgeries are delayed, etc. We don't have good information sharing in this country. We've had multiple hits. We had an entire provincial system hit badly, and we don't have those lessons shared out.

The Chair: You have 10 seconds, please.

Mr. David Shipley: Imagine if we had airplane crashes and we didn't investigate them or share the lessons learned. Well, you're going to get more airplane crashes.

Mr. Alistair MacGregor: Thank you for that.

The Chair: Thank you very much.

Colleagues, we now move into a second round of questions.

To lead off, I'll call on Mr. Lloyd for a five-minute block.

Sir, the floor is yours.

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): Thank you, Mr. Chair.

My question is going to be to Mr. Shipley specifically on Russian disinformation. I get concerned that sometimes we have partisan blinders on in this committee. This is not just a far-right phenomenon.

Would you agree that the Russians will and have exploited actors across the whole political spectrum to advance their agenda?

Mr. David Shipley: We've seen evidence of that from the United States and others. The objective can be to simply put each other at each other's throats. Whether left or right, they don't care. As long as we don't trust each other, don't communicate, can't politic and our democracy looks like it doesn't work, then their system looks legitimate and their aims are achieved. It's about paralyzing us.

Now, what frightens me is that there's some evidence that some of the trucker groups in Canada were being influenced by content farms that just wanted to sell crappy T-shirts and hats. Our democracy is being torn apart so someone can sell anti-prime ministerial T-shirts.

Mr. Dane Lloyd: One really compelling case that we saw on the eve of Moscow's invasion of Ukraine was members of Parliament from the left of centre saying that Canada should not support Ukraine because it is a fascist state. That was being said. That is parroting Russian propaganda, and it was all the way into Canada's Parliament.

Would you agree that this was a significant case of disinformation?

● (1250)

Mr. David Shipley: I'm not familiar with the specific instances of that. However, based on what you're saying, I'll add that we've had warnings from our intelligence agencies talking about influence operations against MPs of all stripes, from various nationalities that have interests, whether it's Russia, China, etc. This is part of the game, and this is what they do, whether to score points, to try to keep us disengaged in this conflict or whatever the national aim, that's part of it. It's part of the importance of educating MPs and politicians about protecting themselves.

One thing that concerns me is how protected our political parties are in general from cyber-operations, influence operations. The hack of the Democratic National Committee in the States lays bare that what happens when a party isn't secure can have dramatic impacts on a country's course.

Mr. Dane Lloyd: Thank you.

I want to put it on the record. Have you seen evidence of how the Russian “Ukrainians are Nazis” narrative has been used to create fear amongst left-of-centre political groups across the world and possibly in Canada? Has that been something that has been observed?

Mr. David Shipley: I think there's been reporting, covering attempts to.... I mean, it makes complete logical sense. How do you keep Canada out of the fight and get as many people on each side? I've seen right-of-centre folks saying, “This isn't our fight and why do we care what's happened?” There are left-of-centre folks saying, “Well, there are Nazis and fascism.”

It's just about muddying the waters. The problem is that we live in a post-truth era, and we have to work on that. There has to be truth still out there.

Mr. Dane Lloyd: I appreciate your putting that on the record.

I'm going to shift over to Professor Kayyem.

In your excellent work on this issue of domestic security, I'm very concerned about electromagnetic pulses. This might be an open fact, but I want your opinion. A nuclear explosion in the atmosphere can have very little kinetic effect on the ground but it could have a devastating effect on our electronics.

Would this be considered a violation of article 5 and require a NATO response?

Ms. Juliette Kayyem: I really think that NATO and the Biden administration have been really brilliant in this, in terms of new threats. They're not actually looking specifically at the threat. If you take cyber or what you mentioned, electromagnetic disruption, they're looking at the consequences. They were early in making a distinction.

It took a while for me to figure out what they were doing, because they weren't quite transparent about it. They were, “Look, there are disruptions in the world, and we'll accept those disruptions for the price of doing business.” In other words, because we're connected, because the Internet works, because we need our electronics, we're always going to assume there's some level of vulnerability.

There will be disruptions because people just behave poorly, but those aren't reasons to go to war.

Mr. Dane Lloyd: An electromagnetic pulse would not be a reason—

Ms. Juliette Kayyem: It would be, if it disrupts.... The standard is, does it disrupt civilian capability to live? In other words, will a mother not be able to feed her children, or—

Mr. Dane Lloyd: I have only 10 seconds.

Would you recommend that we do more to protect ourselves from electromagnetic pulses?

Ms. Juliette Kayyem: Yes, on most anything, I do.

The Chair: Thank you very much.

Ms. Damoff, it's over to you for five minutes whenever you're ready.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you.

Thank you to all of our witnesses for your testimony today.

I actually want to follow up on a comment that my colleague, Mr. Lloyd, was talking about.

Professor Kayyem, this is directed towards you.

Misinformation and disinformation campaigns do tend to target pre-existing social and political divides in an attempt to divide us even more. We're seeing that more and more.

I'm just wondering. Do you have any recommendations to the government to ensure that we're treating this threat properly and adequately, and any recommendations on steps that we can take to both recognize what's happening but also to counter it?

Ms. Juliette Kayyem: Yes, and this has been hugely contested in the United States. A recent attempt to create an oversight body, a new entity within the Department of Homeland Security dealing with disinformation, fell apart almost immediately when it was attacked.

Sometimes I think we make it not just too hard, but we now know what works—I'll go back to this—reliable voices from the government that are actually addressing the misinformation. I think for a long time our governments thought that no one could possibly believe that. If you actually come out early, whether it's called a "myth buster".... At FEMA, the Federal Emergency Management Agency, they have something called "myth busters", which is a way to just combat the rumours that go on during any crisis. That's first.

Second is, as we say in crisis management, consistent numbers and hope. In other words, government spokespeople have to provide facts consistently. They can't go into hiding. Then, what are you doing to make things better? Hope is always important.

Third—and I think we're learning a lot from Ukraine—we used to think that our governments were in a passive mode to this misinformation, as if Russia is doing this and we have nothing. Actually, I think the successes of Canada, the U.S. and other countries in calling out what we knew Russia to be doing early and often very much changed the battlefield literally in the effort against Russia. It prepared the Ukrainians. It prepared us. It prepared all of you.

I do think there are some excellent lessons learned out of the counterattack of the misinformation coming solely just out of the Ukraine war.

Talking about after action, I think it's something we should study because we don't need to be passive anymore. We always thought that the best response was just to move on. It is not.

● (1255)

Ms. Pam Damoff: I just want to follow up on something that you said because you said "reliable voices from the government", except that part of these misinformation campaigns are discrediting the government. How do you get people to trust what a government is saying when that's part of the campaign? It's not just government. All of our institutions are part of these disinformation campaigns.

Ms. Juliette Kayyem: In some ways we'll never get to perfect, so I live in a world where less bad is my standard. We still have 19% unvaccinated in the United States. That's not a great number, but given a lot of misinformation, it's not as bad as I had worried before, so in some ways I think we were able to capture it.

When I say "government" though, it's not simply at the national level. If you look at COVID specifically, one of the ways to overcome vaccine reluctance based on misinformation was very much a local-based communication strategy. In our case, Dr. Fauci had lost his ability to be persuasive among a pool of people. That's okay, and that happens. You pivot to much more localized spokespeople.

Ms. Pam Damoff: I have only about 30 seconds left so I might give it back to you in order to allow my colleagues to have the time to finish. It's close to one.

The Chair: Then we will move to Ms. Michaud.

You have two and a half minutes, and then we'll go to Mr. MacGregor with two and a half minutes. That will take us to the end of the session.

Ms. Michaud.

[*Translation*]

Ms. Kristina Michaud: Thank you, Mr. Chair.

Mr. Shipley, I'd like to ask you a question about the incident at Sunwing a few weeks ago, which highlighted the importance of reporting cyber-attacks. In an article, you say that Canada should follow the U.S.'s example. A few months ago, the U.S. passed a law requiring organizations in the critical infrastructure sector to report any substantial cybersecurity incident to the Department of Homeland Security within 72 hours of learning of the breach or 24 hours of paying a ransom.

Do you think that's a good way to help small, medium-sized and large businesses in the private sector or those that operate critical infrastructure in a country like Canada?

[*English*]

Mr. David Shipley: We are lagging in getting instant reporting in place now. We have Canadian organizations that are going to be telling the United States what has potentially happened to them, and we're completely in the dark. The push to start with federally regulated industries, such as transportation, banking, energy, telecommunications, that's good, but the pain is often outside of those federally regulated industries.

What Europe has done is set certain size thresholds. What size of businesses has a meaningful impact on the economy? Then it set thresholds for participation and reporting on that. That's important, because a small and mid-sized business.... In the case of Sunwing, it was the IT provider for the ticketing system that got hit in the U.S. It wasn't Sunwing that got hit; it was the IT provider.

How do we get the lessons learned and how do we share them, so that we can find and fix vulnerabilities and learn lessons? We have to move beyond blame culture in cyber. This organization was a victim. Why was it a victim? How can we learn from that? For example, for our hospitals, how can 100 other hospitals not get hit after we have one hit so that we get better?

● (1300)

[*Translation*]

Ms. Kristina Michaud: Thank you.

I don't have much time left, but I'd like to discuss Costa Rica, a country much smaller than Canada. A few weeks ago, Costa Rica had to declare a state of emergency because of a cyber-attack by Russian hackers. The departments of finance, health and labour, among others, came to a complete standstill.

Do you think we have reason to fear similar attacks in Canada, or would you say that we are adequately prepared and protected?

[*English*]

Mr. David Shipley: We have had Russian ransomware gangs attack us. We need to get better at it. Cryptocurrency, the flow of money, is fuelling this problem.

The Chair: Thank you.

Mr. MacGregor, we'll go over to you for the last two and a half minutes of this session.

Mr. Alistair MacGregor: Thank you, Mr. Chair.

Mr. Shipley, when you were talking about the relationship that Russia has cultivated with criminal organizations, it reminded me of a few centuries ago when England cultivated a relationship with privateers to basically do its dirty business for it.

On the mandatory incident reporting, going beyond federally regulated industries, the federal government has its relationship with the provinces, even with the Federation of Canadian Municipalities, so those subnational governments. When it comes to the private sector, I guess I want to know.... I agree with you that this is important, but often, when criminal organizations are holding a company hostage, one of their biggest threats is that, if you go to the police, we'll come after you.

How do we bypass that specific threat? That's what has made private companies loath to go to the authorities, because that is a very real threat to their organization.

Mr. David Shipley: For barriers to the companies reporting, number one, the insurance companies often say, “We're running the response for this breach. It's cheaper for us to pay out the ransom. You're not involving the police. Shut up.” If you're a publicly traded company, this could affect share price. The lawyers get super wired about this.

We have to change the risk equation. It has to be that you need to report or you face consequences. Then all of a sudden legal, insurers and others will be saying, “We have to bring CSE and others into the fold”, and you change the relationship.

If the criminals know that we have laws that say they are going to call us, maybe then they are going to move on to somewhere else. I'm with Dr. Kayyem. I'm of the world of doing better and not getting it perfect. The old expression in New Brunswick was—my dad used to joke—“I don't have to outrun the bear. I just have to outrun you.” The same applies in cyber. We just have to get incrementally better about doing that.

Mandatory reporting changes the equation. We need it. If we go this route of provincial, you're going to have have-not secure provinces and secure provinces. Is that the kind of country...? This is a national security issue, and we have to deal with it. We are too small to deal with this without centralizing it, so we have to.

Mr. Alistair MacGregor: Yes, the fact that it's criminal, we have the authority over criminal law. It's often originating from outside of provincial boundaries, so that means the federal government does have jurisdiction. Yes, writing it into insurance contracts—

The Chair: You have the last word, Mr. MacGregor.

Mr. Alistair MacGregor: I'll leave it there. Thank you, Mr. Chair.

The Chair: I'd like to thank the witnesses very much for sharing your expertise and the body of knowledge that you've accumulated over the years. Maybe you go back 25 to 30 years, but this is timely and current and very much a part of today. On behalf of this committee and all parliamentarians, I want thank you for your time, your insights and your wisdom.

Colleagues, that is the end of this portion of the meeting. Have a good day everybody. In another couple days, we will resume on Thursday.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

Also available on the House of Commons website at the following address: https://www.ourcommons.ca

Publié en conformité de l’autorité du Président de la Chambre des communes

Aussi disponible sur le site Web de la Chambre des communes à l’adresse suivante :
https://www.noscommunes.ca