HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 149 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, February 20, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, February 20, 2019

● (1535)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Colleagues, it appears that we have quorum. We will be under some time constraints. We will likely be interrupted by votes.

I want to apologize in advance to our witnesses. We will try to conduct this in as orderly a fashion as we can and try to save time where we can.

The normal course is that we have witnesses read into the record their statements of up to 10 minutes, and then we go to questions from members.

I haven't been able to speak to all colleagues, but I am going to propose to colleagues that the statements as prepared and submitted be taken as read and put into the record. Rather than having the witnesses read their statements again, they would simply summarize their statements, and then we'd move to questions, all in an effort to save some time.

Is that acceptable to you, colleagues?

Mr. Picard.

Mr. Michel Picard (Montarville, Lib.): I think that's a very good suggestion.

I suggest that we maybe allow them one comment on a main subject of their choice.

The Chair: Exactly.

I don't think I banged my gavel, and I should have banged my gavel. I apologize.

Mr. Michel Picard: Consider it banged.

The Chair: We'll deem it banged and deem those statements read.

[*See appendix—Remarks by Professor Jill Slay*]

[*See appendix—Remarks by Professor Yuval Shavitt*]

The Chair: Professor Slay, since you are the witness who would be the most vulnerable to technology, maybe I could ask you first, if you will, to summarize your statement.

Then I'll ask Professor Shavitt if he will summarize his statement, and then we'll go immediately to questions.

If that's fine with you, then we look forward to what you have to say.

Professor Jill Slay (Professor, La Trobe Optus Chair of Cyber Security, La Trobe University, Melbourne, As an Individual): Thank you very much.

I have just developed a paper that looks at some of the key cybersecurity challenges. I have extended my thinking beyond the technical to those that I think are important for both of our governments.

I've explained to you that I think there is a need for a clear understanding of cyber threat. The diagram I have provided explains to you through a little flower picture that there are different vectors of attack, so cybersecurity and cyber threat is not the traditional understanding of technology, of computer network security, but it also covers issues such as law and policy and administration. Therefore, when we are looking holistically at cybersecurity, we must get all those elements aligned.

One of the issues I focused on in Australia for many years is seeing cybersecurity as part of national security. Very often, those of us who are considered experts have come from technical backgrounds where we have been applauded and awarded funds for particular niche pieces of technical research, but there has been a reluctance for academics to see their work as part of national security. Somewhere within the policy mechanism of government, of prime ministers' departments and those departments that deal with the more secret issues around cybersecurity, there has to be an alignment of the agendas of the computer scientist and that of the national security agencies.

The other issue I've raised with you, which obviously I've been working on in Australia for a couple of years, is that as there is more of a focus and more of a need to deal with cybersecurity as part of national security, it's really important for us as countries and as allies to define what a cybersecurity practitioner is. We need to be able to answer the question: Who is an expert in this field?

We, in Australia, have done some work on that over the last couple of years actually to develop a national standard, professional standards in cybersecurity, so that we can answer the question: Who is a cybersecurity professional and who is a cybersecurity technician? This makes workplace issues, HR issues and government employment issues much easier, because our discipline has grown in some ways as an art rather than a science.

I've indicated the type of work we've done in developing national professional standards.

The last point I was making was essentially, in all of our countries, we're going to have a limited amount of money for research, for training, for alignment of cybersecurity with national security. We each have cohorts of researchers who are able to do really good research in areas such as artificial intelligence, machine learning for cybersecurity and IoT security, but very often I find as an academic that the research and teaching agenda is not aligned with the national security agenda.

I can do wonderful publishable work, but in a constrained environment. It's sometimes very unclear from government what they might do with the outcomes of my research. It's very important from a policy point of view to align research funding policies and education policies with the national security policies, the national security environment, so that we actually fund work that is important to the country.

I'll stop there.

● (1540)

The Chair: Thank you for that.

I'll call on Professor Shavitt.

Professor Yuval Shavitt (Professor, Tel Aviv University, As an Individual): Thank you.

I'm a professor at Tel Aviv University. I'm also a member of the Blavatnik Interdisciplinary Cyber Research Center. In this aspect, I fully agree with Professor Slay that cybersecurity is not only about technology, but it is also an interdisciplinary problem.

There are other aspects, such as the legal and social aspects, etc., and at the centre, we do this. We do interdisciplinary research. I'm also the CTO of a company called BGProtect, which is related to what I'm going to talk about.

I've studied Internet routing for over two decades. About 15 years ago, I started an academic project called DIMES, in which, using volunteers, we followed Internet routing around the world. At the peak of the project, we had 1,500 software agents running on volunteer machines in more than 40 nations around the world, so we got a very good picture of how Internet world routing behaves.

About four years ago, we took all this expertise and started BGProtect, which is a company that wants to help government and international institutions strengthen their security by monitoring the routing towards their networks in terms of what they had a fear of. Internet routing is a distributed protocol called BGP, and it is used to tell everybody where to find the servers or the clients on the Internet. However, when it was designed several decades ago, the Internet was very small and based on a lot of trust. Nobody was thinking about security.

About 10 years ago, a new type of attack came into the world: the IP hijack attack. Basically what you do in this attack is take the traffic between two end points and force it to go through your own network. By doing this, you form what is called a man-in-the-middle attack. These attacks are really.... These are large-scale attacks and are able to do a lot of things. Of course, if you get all the traffic passing through you, you can do espionage, or you can do what we call downgrade attacks and be able to insert Trojans into networks. You can penetrate networks. There are many types of attacks. This is why it is so dangerous. We have seen these attacks increasing in number throughout the years, especially in recent years.

We are here to look at these attacks. As a university professor, I'm doing research on this and have published a paper about this. Also, I do it as a company.

Now, when we look at these attempts, we see that these are not simple ones. They cannot be done by script kiddies. We're talking about government agencies and large criminal organizations doing these attacks, and we have to understand that this is not a dichotomy. There are governments using non-governmental bodies, and sometimes even criminal bodies, to do jobs that they want to distance themselves from. Think about the financial sector. It is especially targeted both by governments and of course by criminal organizations.

What can be done? One thing, of course, is to monitor your traffic to make sure that your flows of information won't go where they shouldn't go. This is obvious. This is something that we do at the company.

Another thing you need to do—and this is what we do also in Israel—is to set up CERTs. CERTs are what the Americans call fusion centres. They are organizations where, for governance in financial sectors, banks can share, in various levels of anonymity, data about attacks they are witnessing. This data can be distributed again—there are several levels of distribution—to other financial organizations, so that when there is an attack, such as a new virus, a new hijack attack or any other attack, data can be quickly shared with all the participants of the CERT in order to let them prepare for an attack that is going to come. This is very important. We do it in Israel. We have a national CERT and now we've also set up sectorial CERTs.

Finally, I cannot ignore the debate in Canada, in the U.K. and in the rest of the western world about equipment manufacturers. We know from the Snowden report that many American companies were collaborating with the U.S. government to get information from flows that they had.

● (1545)

There's no reason to believe that this is limited only to the U.S., and I would dare to say that in non-democratic countries it's probably happening even more often.

Now, when you have equipment, this equipment can be designed with vectors, with mechanisms, to sometimes divert traffic against what seems to be happening according to the routing protocol, so you have to monitor this type of equipment especially. We're talking about all sorts of telecommunications equipment, but especially routers. To do this, it's not enough to just look at the routing protocol, because here the diversion is done not through the routing protocol, but through the hardware itself. You need to do active monitoring.

This is something that we are doing. We've seen an increase in such attacks in the last two years. It's important not to limit ourselves to BGP but to also look at the actual data plane and where the packets are actually going, especially if you don't trust your equipment manufacturer.

The Chair: Thank you, Professor Shavitt.

Ms. Damoff, please, for seven minutes.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you, Mr. Chair. I'm sharing my time with Mr. Spengemann.

Thanks to both of you for your presentations.

I have limited time, Mr. Shavitt, and I have some questions about a paper you wrote about China Telecom, which said that we're diverting, through these points of presence, Internet traffic. How are these things established? How is it happening? Who regulates it, or can you regulate it? Is there anything we can do as a government to put in place any regulations or structure to stop that from happening?

● (1550)

Prof. Yuval Shavitt: There is a problem with regulation in the U. S. and I think also in Canada. If I, as an Israeli, were to try to buy a telephone company in Canada, I'm sure that I would not be able to do it, but if I would like to buy a telecommunications supplier, an ISP, I can do it. For some reason, data communication was ignored, because traditionally it was used by hippies. Now, it's really a critical infrastructure, and regulations need to be changed in terms of who can own this type of infrastructure in your own nation.

In general, many Internet companies, many ISPs, are spread out worldwide. You have Russian companies here and you have Canadian...well, maybe not Canadian, but you have American companies in Russia. You have Telia, which is a Swedish company, all over the world. It's okay.

There's one country—China—that doesn't allow foreign players to establish communications in its own land, so I don't understand why Canada and the U.S. allow the Chinese to have a communication infrastructure presence in the U.S. and Canada that actually helps them to do these kinds of attacks.

Ms. Pam Damoff: What kinds of laws do you have in Israel? Or are there other countries that have best practices that Israel adheres to?

Prof. Yuval Shavitt: I think Israel is almost like China in this respect. I don't think that a non-Israeli entity is going to have telecommunication infrastructure within the country.

Ms. Pam Damoff: Are there any other countries besides Israel and China that are like that?

Prof. Yuval Shavitt: I don't follow the law that closely—

Ms. Pam Damoff: That's okay.

Prof. Yuval Shavitt: —but the real thing here is about symmetry. This is why we single out China, not because they are the bad guys and not because they're doing it more than other countries are, but because there's a lack of symmetry here. If they don't allow democratic countries to have equipment or POPs in their country, why should they be allowed to have their POPs in our nation?

Ms. Pam Damoff: Thank you.

Sven, I'll turn it over to you.

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

Thanks to both of you for being with us.

Professor Slay, I appreciate the fact that you're with us notwithstanding the time differential in Melbourne.

I want to stay with the theme that I've spoken to some of your predecessor witnesses about, and that's the environment we want to create in Canada and that we are creating for small business as an environment to start up in. Many small businesses are involved in data-centric, data-intensive lines of business. Some are involved in the development of software directly, and some of them, even more directly still, are involved in the development of defence-related procurement issues, software-related issues.

To what extent are small businesses particularly vulnerable in the cyber domain? To what extent are security questions in fact a barrier to entry into the marketplace in the first place? Are there jurisdictional lessons or best practices that you could tell us about in Israel, Australia or the other areas you're studying?

Prof. Jill Slay: Do you want me to answer?

Mr. Sven Spengemann: Sure. Both of you can, in sequence.

Professor Slay, if you would like to start, please go ahead.

Prof. Jill Slay: Can I just go back to the previous question? Australia has just brought in legislation to control foreign ownership of all critical infrastructure and to regulate on even, for instance, universities and their foreign partnerships. It has become a huge issue, and it would be worth you having a look at the current situation in Australia, given that we're both part of the Five Eyes.

We are not quite the same as Israel, but we've actually tried to fix the problems we believe we've caused ourselves by not being aware of the danger of foreign ownership.

If you have a look at that with small to medium enterprises—

Mr. Sven Spengemann: Does cybersecurity represent a factual barrier to entry into the marketplace?

Prof. Jill Slay: Yes, I think it does. We had a government cybersecurity initiative in 2016, and there was already a big focus on the big end of town. With new Labor Party policy and a general election coming up, there is more of an emphasis on the cybersecurity needs of small businesses. With the skill shortage in the market, the expensive salaries of cybersecurity practitioners, and the fact that, I think, Australia is about 60% to 70% small to medium-sized enterprises, those small to medium-sized enterprises suffer because they usually get general IT or ICT as a service. In many cases there's a lack of understanding of even the need for cybersecurity as a service.

But if you look at it the other way round, from a financial point of view, there has been a huge investment in Australia with government Department of Industry cyber growth centres, cyber growth sorts of nodes in a network, which in part has been to boost the national cybersecurity posture by producing incentives to get the small players in the market. You will have a lot of very small players, say in Canberra, where people who have retired from government service and who have cybersecurity skills are setting up small businesses and developing niche products, niche hardware and niche software. There's a lot of government incentive to actually produce more of that.

It has actually been very successful, but there has been a large amount of federal government funding to make that happen.

● (1555)

Mr. Sven Spengemann: That's really helpful.

Prof. Jill Slay: So I'm going to try—

Mr. Sven Spengemann: I'm going to cut you off because there's less than a minute left and I do want to hear from Professor Shavitt.

Is it fair to say, then, that there's a public common good being created in Australia, which is helpful in opening market access?

Prof. Jill Slay: Yes.

The Chair: Unfortunately, Mr. Spengemann, you have run out of time.

Mr. Sven Spengemann: I thought I had a bit more.

Thank you, Mr. Chair.

The Chair: It was seven minutes.

Mr. Motz, go ahead for seven minutes, please.

Again, I apologize to colleagues for being a bit ruthless here because we are going to be under some time pressures because of voting.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Chair.

Professors, thank you both for being here.

My colleague Ms. Damoff talked about the rerouting of Internet traffic. The angle I want to ask about is whether in both of your countries you have seen cyber-defence actions that could deter actors like China from actually rerouting the Internet.

Prof. Yuval Shavitt: It's hard to deter, because attribution is a big problem in the cybersecurity world. You can do attacks with little or no risk of being detected. Even if it is detected, you can always claim that there has been some configuration error or mishap, etc. It's very hard to show that there's really malicious motivation behind what is happening. You can see a hijack attack, which can also be a configuration error. To distinguish this, you really need to put somebody in a room and force him to tell you what the truth is.

In Israel we have a national defence program through which we monitor the routes towards critical infrastructure in Israel.

Mr. Glen Motz: What about in Australia, Dr. Slay?

Prof. Jill Slay: I can't comment on that. I only know what's in the public domain.

Mr. Glen Motz: When we talk about rerouting—and we've talked about China rerouting and, Dr. Shavitt, you certainly have mentioned that other countries also reroute traffic—can either one of you speak to the kind of information that has been taken by these countries? What are they after?

We had testimony here before from an academic who considered the attempt to gain access. They steal government information, industrial intellectual property, and potentially secrets from government. This is a study mostly about the financial sector, so when you're seeing this rerouting, from your research, what sort of information are they rerouting, or what are they after?

Prof. Yuval Shavitt: I'm an engineer, so when I catch a hijack, that's enough for me. I don't know what they're going to take. They take everything, basically, and they decide what they keep and what they don't.

We have to understand that it's not only about information. Rerouting is also done for inserting Trojans, for trying to penetrate a network. It's not only about information. When we talk about information, we see, for example, lots of financial institution attacks. Many universities are attacked. Obviously, people are looking for data in government installations and government agencies.

Mr. Glen Motz: Professor Slay.

Prof. Jill Slay: In Australia, I don't always know the nature of the attack, but some of the major ones I can think of include the Bureau of Meteorology, where we announced that it was the Chinese who sat in there for at least six months, and the Australian National University, along with probably many other universities. ANU, for instance, has strong links to defence. We know there was a major breach there. We suspect that most of our public universities are vulnerable. I can think of a start-up dealing with telecoms and satellites in Adelaide where the IP was stolen almost after the start-up. They hid in the system for months and months stealing IP.

For many of us who have clearances and who work with government, when we're at work we almost need to live in an environment in which we presume we have already been breached. We go to great lengths to hide our IP—I do, as do others like me—if we are in that public university environment.

● (1600)

Mr. Glen Motz: That leads me to another thought.

Both Israel and Australia are considered to be some of the world leaders when it comes to cybersecurity and being on the front end of dealing with that, and also when it comes to some of the financial security issues we've been talking about. Why is that? What are you doing differently in your countries that we as a committee can recommend that this country do to shore up when it comes to cybersecurity breaches and to improve financial security issues with respect to the Canadian public?

Prof. Yuval Shavitt: I think one of the reasons we are good at this is really the size. Israel is small enough to be better managed. There's also very close collaboration between academia, government and industry. People actually move around among the three disciplines. You can have an academic who will take a government role. You can have somebody from industry who will go to the government and then back to industry. The ecosystem is tighter. It's dynamic.

We also have quite strong awareness among the general public. There's better awareness than in the rest of the world. To be secure, we have a program that starts teaching kids as young as primary school about cybersecurity. They're told not to put their name or address on Facebook and things like this. We build it up at all levels. We have a cyber-authority that is managing all this and diverting all this. It seems to work.

Mr. Glen Motz: Professor Slay.

Prof. Jill Slay: I think in Australia we emulate the Israelis. The Israelis are our model for good practice, and perhaps the Singaporeans are as well. I think we have good relationships with Canadians. There are lots of things I think you do very well too. But I think part of the Australian culture is this tendency towards mateship. Professors, people in government, people in the army, people in those areas in the banks—we all know each other, so whereas we might have formal sharing mechanisms, we will also have greatly informal sharing mechanisms.

Take someone like me. I've trained thousands in PICTL and trained thousands of people. Most of those people go on to get mid-career senior jobs in Australia. That builds a huge, comfortable network of sharing of research ideas and commercialization. I think it's part of the Australian psyche, actually, more than anything else, but there's no reason why it can't be the Canadian psyche too.

The Chair: Thank you, Mr. Motz.

Being married to an Australian, I've always been curious about the Australian psyche.

Voices: Oh, oh!

The Chair: Mr. Dubé, you have seven minutes, please.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Chair, and thanks to both of you for being here.

Professor Shavitt, I want to start with you.

In looking at where Internet traffic goes, there are a few pieces that I wanted to look at.

The first is regarding which jurisdiction applies to the protection of data that's being routed lawfully to a different area, whether that's because of how a company operates or a free trade agreement. One example that comes to mind that I know of, being from the Montreal area, is that with the abundance of hydroelectricity we have in Quebec, a number of these companies—Amazon, Google, etc.—are storing servers there because the cost of energy is low.

Not to get too far away from my questions, but I was reading something interesting the other day, which is that streaming music, depending on the jurisdiction, has a larger impact on greenhouse gas emissions than people might realize. There are a lot of interesting things happening with regard to where servers are located.

My question for you is in that vein. Is there any concern that data, through the legal mechanisms that exist, might be going through areas that people aren't necessarily aware of and causing risks for privacy and other things? One example that comes to mind as well is that we all use credit cards. Many of these companies aren't Canadian, so the information is being stored elsewhere. Is that a concern you have? How does that play into some of the research you've done?

● (1605)

Prof. Yuval Shavitt: Yes, this is the primary concern of this research. We see routing that is diverted, either maliciously or accidentally, to locations where you don't want it to go.

By the way, it also hurts performance, so you don't get the network to be as fast as it could be. I can tell you, for example, that we've seen routes from Tokyo to Seoul rerouted non-maliciously through the U.S. and then, after a week, through London. This makes the connection time 10 times slower, and this is a non-malicious diversion.

You see things like this happening all the time. The real problem is how do you distinguish between bad engineering, configuration errors and attacks.

Mr. Matthew Dubé: Here's my question for you. As an engineer, you might not be able to answer it, and I say that with all due respect, of course. I'm just wondering about this. Is there a concern that for me as a Canadian, say, if my data ends up on a U.S. server, and even if the United States is an ally, a democracy, ultimately I don't benefit from the same constitutional and legal protections for my privacy and how that data is treated? Is there a concern about that as well?

You've said that ultimately we obviously look towards non-democracies as more malicious actors, but at the end of the day, everyone is engaged in the same activity, and the individual might be the one paying the price. Is that a concern or is that perhaps beyond what you've done in terms of your research?

Prof. Yuval Shavitt: Concern is really subjective. Each one is concerned about other things, and when you build such a system, you need to build it in a way such that you can tune it to the concern of individuals.

Mr. Matthew Dubé: I appreciate that. Thank you.

Professor Slay, I want to speak more specifically about the Australian experience.

Last year, I believe, legislation was adopted there. This comes back to this idea of the concern often raised about these so-called back doors. I'll express it in layperson's terms. Any sort of back door that's potentially opened to decrypt for law enforcement potentially opens the same avenue for bad actors—to not use the expression “bad guys”.

I'm just wondering what your thoughts are on that legislative experience that Australia has had, or if it's too early to tell if that's what has happened. I believe that concern was raised at the time.

Prof. Jill Slay: I think that issue has not been resolved, because it has gone back to Parliament. From my point of view, I believe the vendors have overreacted to what they believe is the government threatening to weaken their products, whereas I've worked with government for many years and have been one of those who, as a professor of digital forensics, has actually helped them to understand how law enforcement can actually get evidence.

I personally have objected the other way to those who want to stop law enforcement genuinely in serious cases getting evidence, but that issue has been not resolved. It's in the paper this week. Really, we don't know how this will end, because traditionally the government has sort of won the argument from a national security point of view. If you're going to follow us, I think you had better wait a bit.

Mr. Matthew Dubé: That's fair enough.

You'll forgive me for perhaps not being that well read on the topic, but I'm just wondering what the law looks like. Is it case by case? I would assume there would be the intention of a warrant or something along those lines. Could you perhaps provide as brief a response as possible to that for clarification?

Prof. Jill Slay: Unfortunately, I'm not an engineer either, so I don't know the intricacies of the legislation, but essentially, yes, I believe there's a case-by-case basis, law enforcement being able to force.... It's to do with encryptions, something being encrypted—that's how I understand it to work—but it isn't as drastic a blanket piece of legislation as many people present it, in my opinion.

Mr. Matthew Dubé: Okay, thank you.

Professor Shavitt, quickly, in the minute I have left, with regard to the Internet of things, you talked about the time that data can remain in one place before it moves to another. Is there a concern that devices themselves are also very weak in terms of their security protocols, especially as they proliferate more in the future?

Prof. Yuval Shavitt: Of course. The problem with the Internet of things is that we are talking about very low-cost devices, and people will not be able to spend a few cents more to make them more secure. We really have a problem in having many, many billions of devices that really have no security. It's a big problem, and we need to see how to solve it at the system level.

● (1610)

The Chair: You still have 20 seconds.

Mr. Matthew Dubé: That's fine. Thank you, Chair.

The Chair: Okay, thank you.

I hadn't realized it was such a misfortune to be an engineer.

Monsieur Picard, I do not believe you share that misfortune. You have seven minutes.

Mr. Michel Picard: No, I'm not an engineer at all.

I'll start with Professor Shavitt.

Just remind me what you said about the fact that no telecom companies in Israel can come from outside Israel or foreign entities.

Prof. Yuval Shavitt: I'm not sure about the legal aspect, but for sure this is not happening. So, yes, all the telecoms in Israel are Israeli-owned.

Mr. Michel Picard: To your knowledge, what prevents Israel from seeing its own local telecom companies being bought by a foreign interest or having their services rented by a foreign interest, who thereby can get around this interdiction?

Prof. Yuval Shavitt: I think they cannot be bought by foreign entities. There has to be an agreement by some committee. I don't think this can happen. Can somebody be rented? Well, maybe.

Mr. Michel Picard: We enter a grey zone, if I understand that.

Prof. Yuval Shavitt: Yes.

Mr. Michel Picard: Okay.

Professor Slay, a few weeks ago there was an article stating that London has looked at Huawei and is maybe starting to change its perspective on the company with the security issue they had to deal with, and they might not be as scared or have to be as protected as they thought they should be, although in Australia you got rid of the company and that was that.

Are you aware of this change of mind in the U.K., and if so, what do you think of it?

Prof. Jill Slay: I've been following that quite closely.

The first report from GCHQ said they felt it was far too great an effort for their lab to provide assurance about the Huawei equipment, but I believe it was only yesterday that GCHQ said maybe they could assure the equipment. I believe there are political implications in the U.K. because of the nature of their board, which were not necessarily the same for us in Australia. I believe we have already made that commitment not to use Huawei at the federal government level, but we have not always tracked the relationships Huawei has in the country with, for instance, others who are not purchasing for the federal government. For instance, the Government of Western Australia has a contract with Huawei for equipment for their train system, and the University of New South Wales, where I used to work, has bought equipment for some kind of building works.

In Australia the federal government can control federal purchasing. For instance, it was able to control or to in some way stop Optus, one of our telcos, from using Huawei for 5G, but we don't have an overarching blanket control, because we're a democracy and because we have states as well as a federal government.

My own opinion is that the British decision will not affect the decision we have made in Canberra, mostly because we see the link between cybersecurity, the ability to infiltrate our systems' back doors, cyber-espionage and foreign interference. That is the theme at the moment, rather than just the security of the equipment.

Mr. Michel Picard: I'm not sure about that part, but in terms of iPhones, aren't some parts of iPhones manufactured in China? Do I have to start not trusting my iPhone now? If it's that, then I would trust no phones or equipment at all. In my riding, we don't manufacture anything, so I have to buy it from somewhere else.

● (1615)

Prof. Yuval Shavitt: There's a greater understanding now of the risk of not being able to understand your supply chain. It's not a simple problem, because we live in a global world and sometimes you have no way other than purchasing some of your parts in places that you might not want to buy them from.

The idea is that if there is an integrator, it has to have the responsibility to examine the supply chain, identify the risks and be able to control them by inspections, testing, etc.

Mr. Michel Picard: You said an interesting word. I have no choice. I have the choice of what I put on my Facebook page. I can be as discreet as possible or maybe look for more friends if I don't have any—I just have two.

Voices: Oh, oh!

Mr. Michel Picard: The market goes on the web, and if we don't go on the web, there's no evolution or progress, because this is where we are and we have to go there. I might not want to share my financial information over my phone or my computer, but the chances are that I won't go every day to the bank to do my statements on paper; they have to go on the web. We know that we are plunging into a hole, and we don't know whether there's a limit to it. Is that the "no choice" that we have?

Prof. Yuval Shavitt: Well, I think we know quite well how to secure websites. It's never perfect, of course, and not everybody is doing whatever they need to do in order to secure them, but there are ways.

Basically, we're talking about risk management here. Probably the cost to go from 99.5% to 100% is going to be too high, but you can get security that is pretty good. You just need to invest money and effort and be aware of what you're doing.

Mr. Michel Picard: As a good citizen, how do you value the fact that you might be the 1% under the risk management where it's, "Well, too bad, we lost this one"?

Prof. Yuval Shavitt: This is statistics, no?

The Chair: We're going to have to leave that existential question.

Mr. Eglinski, please, for five minutes.

Mr. Jim Eglinski (Yellowhead, CPC): I'll start with you, Mr. Shavitt.

I read your report the other day, the one that you did in 2018. You co-authored a paper entitled "China's Maxim—Leave No Access Point Unexploited". It was very good. I actually understood quite a bit of it after I read it three times.

Voices: Oh, oh!

Mr. Jim Eglinski: It was a very comprehensive report. I believe that in the fifth or sixth paragraph you talked about a great concern, which is that all countries need to get together and address these issues.

Have you seen a response from different countries since you published that paper?

Prof. Yuval Shavitt: I would rather not comment on this matter.

Mr. Jim Eglinski: You would rather not comment? Okay. I'm going to move away from that, then.

You talked about monitoring flow, which you do in your home country. One of the most important things, of course, is to activate monitored data plates, to know what kind of equipment is there. I'm kind of curious with regard to this monitoring.

You're keeping an eye on what is being routed and where. By the time you find out that someone is undergoing unusual routing changes, has that data already been lost? Is there a way for you to stop it before it gets that far? You did talk about technology and the cost of investing in protection, so I wonder if you could give us a little on that.

Prof. Yuval Shavitt: There are ways to actually prevent hijacks in some cases. In other cases, you just need to detect and mitigate. Let's suppose that somebody is setting up an espionage campaign against you. Would you rather have this campaign last for 25 minutes or 25 days? If you can stop it after a few minutes, or after half an hour, say, it's much better than letting them eavesdrop on you for weeks. We've seen attacks that have lasted for weeks and even longer.

Some types of attacks are very short. By the time you detect and try to mitigate, it's already lost. Many of the attacks, especially the ones that are sponsored by government agencies, can last many weeks.

● (1620)

Mr. Jim Eglinski: Okay.

You mentioned something earlier. Our whole study is dealing with cybersecurity in the financial sector, but we kind of wander off because cybersecurity is such a big thing. You mentioned that in your country, financial institutions have been hit pretty hard.

Prof. Yuval Shavitt: No, I didn't say this. I said that overall, from what we see globally, financial institutions have been hit pretty hard.

Mr. Jim Eglinski: Okay. Have you seen that in your own country?

Prof. Yuval Shavitt: We've seen some attacks on financial institutions in our country, yes.

Mr. Jim Eglinski: Okay. Thank you.

Dr. Slay, I was looking at your Twitter account, just getting to know you a bit better. Prior to March 2018 you used to concentrate all your focus on Russia as the bad guy, and then you kind of changed your train of thought to China.

Could you relate why your interests went in a different direction and to a different country?

Prof. Jill Slay: If I'm open with you, I lived in Hong Kong for 10 years. I speak fluent Chinese but I also have clearance. Also, I'm very, very careful about what I put on Twitter, so you're just going to see the fact that I've been selective.

I have gotten to the stage where I am very frustrated with the way that, as a professor, I'm constantly targeted by the Chinese. I have attribution. My stuff's been stolen. They've planted Ph.D. students on me. Therefore, I've decided to be more vocal about it. That's what you're seeing.

For me, the problem as I've become more well known is that I'm much more likely to be targeted. I fear that all professors in our field, whichever country they're in—and I wouldn't think that Canada is exempt—will be targeted by, particularly, China because they're really on the hunt for IP, and they have been for many years.

Mr. Jim Eglinski: Can you tell me what your concerns are with the Huawei 5G products in your country, and why you think it was a good idea to ban them?

The Chair: In 10 seconds or less.

Prof. Jill Slay: I think there are two ways with Huawei. Some things I can't comment about because, as I've just told you, I have a clearance. By reputation, Huawei is a company that has constantly stolen IP. If you have a look at the best-known case, of the Cisco routers, from, I think, 2012, there's a sense of business ethics.

Also, the other, more logical one is that if you buy their equipment, there is the potential for them to need to have access to the equipment for maintenance. If they choose to do espionage, then they can actually insert malware in your equipment. It could be hardware or it could be software, but we're very vulnerable.

The Chair: Thank you, Mr. Eglinski.

Ms. Dabrusin, go ahead for five minutes, please.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you.

I believe, Professor Slay, you talked about national professional standards in cybersecurity. One thing that's come up a few times when we've heard testimony is the need for more trained individuals, more training for people to be professionals in cybersecurity. Is Australia doing something in particular that's doing a good job of building the pipeline—for lack of a better term—of young people who are learning the skills to get into cybersecurity so that they can help us with this issue?

Prof. Jill Slay: Yes. We're putting huge amounts of money and effort into this. Through the Australian Cyber Security Growth Network, through the growth centres, we now have systems. We've emulated the Americans in many ways, so we have the equivalent of its CyberPatriot school kid Capture the Flag. We're trying to insert cybersecurity into the curriculum for everybody from grade 7 to grade 9. We're trying to insert cybersecurity awareness into the curriculum at TAFE colleges, which are community colleges or technical colleges, into every kind of diploma. That should be happening quite soon. This is national funding doing this.

From the Australian Computer Society's point of view, we have a national curriculum in ICT, so we're trying to actually develop national curriculum in cross-disciplinary cybersecurity so that we focus not just on IT issues but also on law, ethics, criminology and psychology, in a three-year degree. My university has one, and quite a few have that kind of curriculum. Government has stated that it's a cross-disciplinary issue, so therefore the whole education system has to recognize that as well.

● (1625)

Ms. Julie Dabrusin: Mr. Shavitt, is Israel doing something to build that capacity?

Prof. Yuval Shavitt: We are doing similar things to what there is in Australia. We have a curriculum for young children. You can do matriculation at the end of high school in cyber. It used to be computer science. Now you can choose either computer science or cyber. At university we also now have a specific program for cybersecurity.

One thing we have that probably Australia and Canada don't is the military as a huge facilitator. Every year, hundreds of thousands of young Israelis are drafted to the intelligence forces and other units where they are trained. They actually do lots of high-level cybersecurity work in a very compressed environment. This gives us a big edge.

Ms. Julie Dabrusin: We don't have a similar system to that.

I'm just trying to figure out what people are doing well that we might be able to learn from. It's really interesting to hear some of the different things that are happening.

One of the others we heard from, HackerOne, spoke about using hackers—well-intentioned hackers, for lack of a better way of describing them—who will test the system. There might be bug bounties, I think they called them, to help find where the problems and weak spots are. Have you seen that in either of your countries? Is there some value to legalizing that kind of work?

Prof. Yuval Shavitt: First of all, it is legal. Many companies have bounties. If you report a problem, you can get a cash prize, and it can be as high as $100,000 if it's something really.... This is happening around the world. It's limitless. If Cisco or some other company has a problem, they don't care if the solution comes from Belgium or from Canada.

In addition, at least in Israel, we have a volunteer Red Team. These are cyber experts who devote a day a month or a few days a month to test, with permission. They do pen testing on critical infrastructure. It can be a hospital, a water installation, etc. At the end, they give a report saying, “These are the problems you have.” I think this is really valuable. When you have permission, there is no legal problem. I don't think you need a new law for that.

The Chair: Thank you, Ms. Dabrusin.

As colleagues and witnesses can see, the lights are flashing. Normally I'm obliged to suspend at this point, but I'm assuming there will be some unanimity to continue for about 20 minutes. That will give us 10 minutes to get upstairs to vote. Is that fine?

An hon. member: I'm fine with that.

The Chair: Okay.

Mr. Motz, go ahead for another five minutes, please.

Mr. Glen Motz: Thank you.

As was indicated, both Israel and Australia are known as powerful cybersecurity countries. With stronger cybersecurity firms, as well as by attracting investments in both your countries to deal with cybersecurity, are your countries under similar attacks to those we have had in Canada? Do you experience the same number and the same type that we do, or do you have more of somebody trying to pierce the systems?

Prof. Jill Slay: May I answer?

Mr. Glen Motz: Please do. Both of you can.

Prof. Jill Slay: Last week we publicly announced a major attack on Parliament—on all our email and all our service. The Prime Minister talked about it on Monday. They also attacked each of the three major political parties. This morning I woke up to find that a huge Melbourne hospital has had an attack with ransomware and that patient records have been garbled and can't be properly decrypted.

I would say that you must not see yourselves as the sort of poor country cousins in any way. We are all under the same amount of attack. As the Five Eyes in particular, we rely on each other to support each other. I think the level of attack is pretty high at the moment though. For us, that's because we're facing a general election, but there are other political issues. I see it from both a political and a criminal point of view. There are nation-states and cybercrime, and it's only growing.

● (1630)

Mr. Glen Motz: Dr. Shavitt.

Prof. Yuval Shavitt: I think it's probably the same worldwide. Maybe Israel gets a little bit more because of the Israeli-Arab conflict, but in general, we're all suffering.

Mr. Glen Motz: Fair enough. Thank you.

Canada is one of only two of the current Five Eyes allies who have yet to declare a position on Huawei. The director of our Canadian Security Intelligence Service, CSIS, has publicly expressed concerns about state-sponsored espionage through the next generation of 5G. We know that Australia was at the forefront of barring this company from participating.

Dr. Slay first and then Dr. Shavitt, what would Canada's willingness to do business with Huawei mean, in your opinion, for the longevity of Five Eyes?

Prof. Jill Slay: I have to say that it's a sovereign issue. It's really for Canada to decide.

Obviously, I can't speak for government. I just speak for myself. I think it would be easier for the Five Eyes partnership, just thinking from a technical point of view, if we had a common view on Huawei. But I think the announcement yesterday from the British, which was a halfway announcement that perhaps we might be able to deal with this, which says perhaps, with effort, we can provide the kind of assurance...would also then complicate the system for Canada.

I'm a very black and white person and a very black and white engineer, so I'm comforted by the fact that the federal government is not going to buy Huawei. I'm also the Optus chair, and Optus funds a lot of the research at my university. Obviously, Optus was the company that had the relationship with Huawei for 5G. I felt myself in huge conflict because I was called the Optus chair, so I was highly relieved when I didn't have to deal with that issue.

From a political point of view, I think for maintaining the solidarity of the Five Eyes, I would hope that we could come to the same kinds of conclusions. But I think there will be other people having that discussion this week.

Mr. Glen Motz: Dr. Shavitt.

Prof. Yuval Shavitt: It's a risk management thing. As I said in my initial statement, we know from the Snowden report that American companies collaborate with the American government, so there's no reason to suspect that in other countries it doesn't work this way, especially not in China. It's risk management. How much would you invest in order to avoid having Huawei in Canada? Of course it's going to cost you more for equipment.

I would say that if you decide to use Huawei, you need to put in place monitoring equipment and monitoring facilities to make sure that funny things don't happen.

The Chair: Thank you, Mr. Motz.

Ms. Sahota, you have five minutes, please.

Ms. Ruby Sahota (Brampton North, Lib.): Okay.

I'll start with you, Professor Slay. It was a bit worrisome to hear you mention that you were targeted and that you had Ph.D. students enter your classroom in order to do so as well. Can you explain why you were targeted? I think you stated that everyone in your type of position in academia would potentially be under a threat. How would IP be something that would be linked to you in your position?

Prof. Jill Slay: I think it is part of the international understanding, which has already been stated, that basically, in the same way that China might want to just collect as much data as it can from the system, China has had a much more systematic way of sending Ph.D. students to Australia, the U.S., and, I presume, Canada. Those of us who are deemed to be leaders in our country end up with many Chinese students wanting to be our Ph.D. students.

With one of my very first Ph.D. students, I was working on a project with the police. It was in a public university, so it wasn't classified data. Nevertheless, without going into details, the IP was stolen and taken back to China. I was there, unfortunately, without knowing when it was handed over. Since that time, I have been very cautious about what's going on.

● (1635)

The Chair: Are you being hacked right now?

Ms. Ruby Sahota: I've read a little bit about the political parties being hacked. Do you know what kind of data? I know you're going into an election. We are also going to be having a federal election in October of this year. On another committee I sit on, we've been talking quite extensively with the democratic institutions minister about the potential threats Canada faces as do many countries around the world regarding elections and protecting democratic institutions.

What kind of wisdom can you give us from the experience that Australia has been having?

Prof. Jill Slay: I don't think we've formally announced—and I don't think we will be able to formally announce in the short term—whether any data were stolen. We actually don't know. That's from the parliament service. The greater concern has been raised with the [*Technical difficulty—Editor*] parties, the three major parties, and the fact that very little finance is being made available to them.

It's only in the order of $70,000 a year to actually secure their systems. However, on their systems, they will have all the data of memberships, donations and things like that. Those are the things that are causing public debate this week. We, like you, will be remembering what happened or what was claimed to have happened in the U.S. election. We're being assured by government that it was caught very early and that it's under control, but I don't think there will be much more of a public statement, to be honest. We have to all be careful.

Ms. Ruby Sahota: Do you feel the lack of a public statement is due to wanting to protect the integrity of the system there and not wanting people to be fully aware of what may or may not have happened?

Prof. Jill Slay: They're not ready to announce anything. Attribution is hard and that's part of the discussion. It's easy to pretend to be a nation-state setting up in a different nation-state. We can't tell where the attack is actually coming from. We very often cannot tell where the attack is coming from, because people are very good at espionage and hiding themselves, pretending to be somebody else.

Ms. Ruby Sahota: We've had those conversations, as well, when it comes to private companies. Many people are not revealing the breaches that are occurring due to public scrutiny or shame.

When it comes to our democratic institutions, do you think we should be trying, through the Five Eyes at least and through other democracies, to work together in order to lessen the potential threats, and how so?

Prof. Jill Slay: We should be and I think we are. There is probably a lack of under-reporting publicly, but I'm pretty sure that within international organizations, within governments, there is also a lot of sharing. My experience is that there is a lot of sharing, whether it's law enforcement or whoever. I don't think we're necessarily constrained by those things.

It might be smaller companies that don't want to acknowledge they have been breached. However, particularly in Australia, there is more of an openness now to talk about it, particularly since before Christmas, the government, Alastair MacGibbon, the deputy secretary, the prime minister's adviser, did made it very clear that many companies have been breached, and there is more openness, more willingness to accept that because there's just so much of it.

● (1640)

The Chair: Thank you, Ms. Sahota.

Mr. Dubé, for three minutes, please.

Mr. Matthew Dubé: Thank you, Chair.

Very quickly, I want to hear from both of you. We've talked a lot about foreign state actors as a threat. There has been a certain level of reporting here in Canada about domestic actors operating, not necessarily related specifically to cybersecurity, but in the digital space.

From a cyber perspective relating to our study, has there been any concern, in both Israel and Australia, about domestic actors and malicious actions that have posed a risk for either government or private individuals? Perhaps Professor Shavitt could answer and then Professor Slay.

Prof. Yuval Shavitt: Of course, you're always afraid of criminal activities. Criminals identify the Internet as a great place to make money very easily. Yes, you have to be protected also against domestic attacks.

Mr. Matthew Dubé: Professor Slay.

Prof. Jill Slay: Yes, it's the same for us. We're always aware of the possibility of internal attack. We always joke about the 15-year-old script kiddie who can do just as much damage as a nation-state. We do have that awareness, but currently, with the issues around Huawei and China, I think there's an international focus on external attack.

Mr. Matthew Dubé: With the minute I have left, as we've seen in other fields such as intelligence and law enforcement in more traditional terms, the focus sometimes leads us to forgetting the other side. Is there a possibility, a risk, that the domestic side gets neglected with all this focus on foreign actors?

Prof. Jill Slay: If we focus on defending our systems from external attack, we're protecting it from domestic attack. Insiders is a different issue.

The Chair: Professor Shavitt.

Prof. Yuval Shavitt: [*Technical difficulty—Editor*]

The Chair: I have a couple of questions, with the indulgence of the committee. Even if the committee doesn't indulge me, I'm going to ask them anyway.

Professor Shavitt, I want to focus on your analysis of the router, which, as I understand it, is your specialty. You talked about the attack points, both the software and hardware attack points, and where they can be compromised and route information to where you don't want it routed. The question I have for you is that this is the current state of affairs with the 4G network, and when it comes to a 5G network, what is the significant difference, if any, in terms of how you protect those routers?

Prof. Yuval Shavitt: I don't think there's a significant difference. It's just that this is a good point in time where you renew your equipment and you want to do it in the best way possible in terms of cybersecurity.

The Chair: Professor Slay, do you agree with that observation?

Prof. Jill Slay: Yes, I do. This is the time to be having a good look at your defences.

The Chair: On the insertion of malware in the hardware part of these routers, you'd apply the same analysis as if it was in a 4G network as you would in a 5G network. Is that correct? Okay.

The second question I had is with respect to the ownership of the infrastructure, because Israel has made a decision, and it is a relatively small country and therefore more able to control the ownership structure. Is ownership actually an illusion, in fact, and any system can be penetrated from outside regardless of the ownership of the system?

Prof. Yuval Shavitt: It's true that any system can be penetrated from the outside, but you have to defend those systems. You don't want to make life easy for the attackers. Again, it's risk management. You want to make the penetration of your critical infrastructure as hard as possible. You can never be 100% secure, but you can get as close as possible.

● (1645)

The Chair: Your argument would therefore be that if it is a domestic actor, the possibility of security increases rather than decreases.

Prof. Yuval Shavitt: Yes.

The Chair: Professor Slay, do you have any comment on that?

Prof. Jill Slay: I think my advice would be that particularly when we're talking about critical infrastructure—I'm also particularly concerned about the cloud—there has been a trend for money saving within government and to use other people's external public-private clouds, and I'm talking about my government. But I've noticed a trend, even now this week, to talk about having the cloud storage on Australian soil.

I would be recommending that you weigh out the costs and benefits from a national security and finance point of view of keeping all your data on shore, in your own country.

The Chair: Thank you.

Professor Shavitt.

Prof. Yuval Shavitt: There's one thing that is easy to do and that governments don't seem to do.

People tend to align with the body that they are part of. Look at the Snowden case. Snowden was a contractor. He was not a government employee. There's a good chance that if he had been a government employee, he would have felt more like he was part of the system, and the chances that he would go against the system would have been lower.

In cybersecurity, don't hire contractors. You should make it possible to pay cybersecurity professionals higher salaries than what government used to pay, but make them part of the system.

The Chair: On behalf of the committee, thank you to both of you for your advice, wisdom and experience.

Colleagues, at this point, I can either adjourn or suspend. We have 10 minutes until the vote. If we suspend, then we can come back and possibly deal with the motion or we can adjourn and we'll deal with motion M-167 at another time.

What's your pleasure?

An hon member: Adjourn.

The Chair: The meeting is adjourned.

SECU-149
3.30
20 Fev. 2019

Cybersecurity in the financial sector as an economic security issue

Submission to the House of Commons Committee on Public Safety and National Security

Professor Jill Slay, La Trobe Optus Chair of Cyber Security

Introduction

In this brief, I look at some key cyber security challenges that I believe both Australia and Canada (and to some extent other 5 Eyes partners) are facing and offer some recommendations to deal with these challenges.

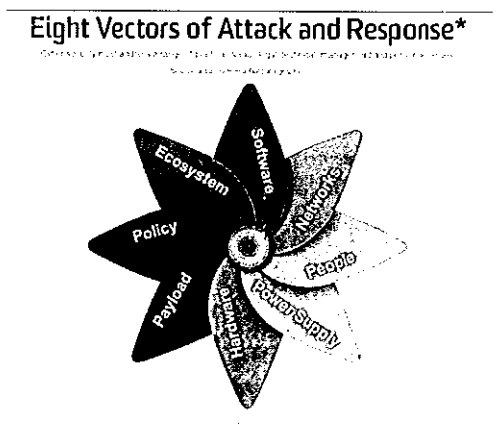
- Development of a clear understanding of the nature of cyber threat
- Cyber Security as part of National Security
- Developing a clear and culturally appropriate set of National Cyber Security certifications (summary of Australian Computer Society work)
- Developing an appropriate academic and government research agenda in cyber security especially machine learning for cyber, other AI approaches and IoT security

Background

One of the major cyber security problems that Australia, Canada and allies contend with is the large volume of attacks on government, industry and home users. While some are targeted and of high value, the trend across the board is one of uncontained growth in threat level, and exponential growth in economic cost. These national problems were brought into stark focus in May of 2017 during the WannaCry ransomware campaign. According to a Europol report (2017), the attack affected an estimated 200,000 computers worldwide by encrypting them and demanding a payment in cryptocurrency. In the UK, the National Health Service alone had 70,000 devices affected including MRI scanners, blood-storage refrigerators and theatre equipment. An estimate puts the world-wide economic cost of WannaCryat $4 billion.

WannaCry's spread was halted due to a programming limitation, but what would have happened if that limitation did not exist? What if WannaCry had targeted our Systems of National Interest? Most importantly, how will Australia and Canad defend against the next, more sophisticated version of WannaCry? How will we deal with issues of cyber intelligence and the human interpretation of the threat that this intelligence conveys? How will we respond under attack? How do our National Security policies support the implementation of appropriate solution? Who will do the research and practice in this specialised field?

There are a large number of issues that I touch on here but, in 10 minutes, I will touch on 3 of them.



Development of a clear understanding of the nature of cyber security

Cyber security is a term that is still misunderstood and it is often seen as 'computer and network security'. When we think of the economic security issues we face, we have to consider the cross-disciplinary nature of cyber security.

'Cyber security' has at least eight foundational components, some of which are narrowly technical (but involve people and organizations); and others of which are simultaneously technical and deeply dependent on non-technical inputs. One view of these ingredients is captured here in a graphic which describes them as vectors of attack and response. This graphic is adapted from an approach developed by engineers in Bell Labs to address problems of defence of connected computers and devices (Gupta and Buthmann 2007). This concept provides understanding of what shapes cyber security and the nature of cyber defence. There is also a wider national perspective since strategy and planning for cyber security depend on the political, legal and social environment as much as they do on engineering and systems approaches, as conceived in the original Bell Labs work.

Cyber Security as part of National Security

Cyber security is, to some at least, still a portion of computer science and a theoretical science looking for formal solutions. In academia in particular, the link between Cyber Security, Cyber Defence, Espionage and Foreign Interference are important linked concepts that are only beginning to be understood.

Cyber security (or cyber warfare) for National Security and Defence is a fairly new concept to technical experts. Cyber security, as a national security issue, was identified first in Australia in the Defence White Paper of 2000 (Defence 2000). The Howard government in 2001 launched an E-Security Initiative, which formed collaboration between federal government agencies, and the Trusted Information Sharing Network, representing major sector groups that were identified as critical infrastructure for the purposes of national security (Parliament 2013). The Rudd Government reviewed Australia's e-security policies, programs and capabilities in 2008. The table below summarises the cyber security initiatives since 2008, the source of policy or advice, and the implications for research and the professional workforce.

Cyber Security Need	Putative Policy/Advice Sources	Socio-Technical Research implications
• Cyber Security • Cyber Warfare and Cyber Defence • Cyber Intelligence and Espionage	• Australian Signals Directorate Top 4 Strategies (ASD 2013) • Defence White Paper 2016 (Defence 2016) • Defence White Paper 2009 (Defence 2009) • ASIO Report to Parliament 2011/12 (ASIO 2012) • ASIO Strategic Plan 2013-16 (ASIO 2013)	Cohort of innovative academic researchers, government and industry leaders in: • Network and data security • Incident response and digital forensics • Software development and reverse engineering • Cyber effects • Open-source Intelligence • Law and Policy • International Defence and Security relations

- The policy and advice of the last eighteen years in Australia (and I believe Canada will not be different) have suggested the need for a highly qualified workforce to deal with cyber warfare, defence, security and to protect all aspects of society.
- My research, and knowledge of the Australian context, indicates that there is limited research in Cyber Security for Australian National Security.
- There is no public-domain link between the National Security Agenda and technical research outputs that continue to be funded, but not necessarily applied.
- There is no established framework on which this kind of relationship may be built, and, while there is an interest in researching new and challenging cyber security issues such as Defensive Cyber Operations, automated Cyber Intelligence and evidence collection, deception and some of the human issues involved, there is no credible and sustained national research focus on the issue of linking the technical cyber security and Defence, law and policy agendas.

Advice

- There is a need to create a framework to specify how the Cyber Security and Cyber Defence of Canada's economy and its Critical Infrastructure might be carried out, incorporating technical, socio-technical and policy perspectives, and to test and validate this framework.
- The alternative to using such a framework is a piecemeal approach to academic cyber security research which draws on the strengths of an individual researcher or research leader and their track record. This work might be publishable in a good outlet, but misses out on providing a solution that is both theoretically cutting-edge, and also devices or techniques that are immediately usable by the National Security community, and potentially commercialisable.

National Cyber Security Professional Standards, Common Body of Knowledge, Curriculum and in

Australian Computer Society is national computing and cyber accrediting, curriculum and ICT standards body with around 40,000 members. It has worked on a set of National Professional Standards in Cyber Security so that Australia can answer the question 'Who is a cyber security professional?' and "What kind of skillis does Australian need in tis cyber security professionals

National Professional Standards

These were launched in September 2017 after work by the ACS Task force at the request of Prime Minister's Special Advisor / Head of ACSC Alastair MacGibbon. The standards have been implemented, assessors recruited and trained and there is teady flow of new members taking the opportunity to achieve this certification. Candidates come from Australia and SE Asia and from a range of cyber security and IT backgrounds. In summary the standards, gained from synthesis of NIST, ISC2 and ISACA work provide an Australian focused certification:

Certified Professional - Cyber Security

Cyber security specialism assessment requirements are equivalent to existing ACS Certified Professional assessment criteria and pathways with the addition of demonstrating in-depth competence in 4 SFIA skills at SFIA level 5.

SFIA skills must be from the following skills:

- IT Governance
- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Penetration Testing
- Security Administration
- Programming/Software Development
- Systems Software
- Testing
- Asset Management

Certified Technologist - Cyber Security

Cyber security specialism assessment requirements are equivalent to existing ACS Certified Technologist assessment criteria and pathways with the addition of demonstrating in-depth competence in 3 SFIA skills at SFIA level 3.SFIA skills must be from the following skills:

- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Systems Development Management
- Asset Management
- Change Management
- Security Administration
- Incident Management
- Conformance Review

We also have 2 projects developing micro-credentials and academic curriculum guidelines in for cyber security. I would suggest that Canada also needs the same so as to determine the nature of the work force and to ensure that curriculum matches workforce need. I see these as major issues to share but can also answer questions on other research issues such as Critical Infrastructure , IoT and Deception Systems.

Professor Yuval Shavitt, CTO of BGProtect – SECU Session February 20, 2019

My name is Yuval Shavitt, I am a Professor of Electrical Engineering at Tel Aviv University, and part of the Blavatnik Interdisciplinary Cyber Research Center. I am also the founder and CTO of BGProtect, a company that was established to defend nations and enterprises against attacks on their routing and thus their connectivity.

IP hijack attacks, also known as deflection attacks, are severe attacks since they enable the many variants of Man-in-the-Middle Attacks, including espionage, downgrade attacks, decryption, impersonation, and more. Financial institutions are one of the prime targets for such attacks since they are lucrative for both criminal organizations and foreign governments. In recent years past, we have documented deflection attacks on many financial organizations, which include many mid to large size banks, as well as stock exchanges, insurance companies, and financial news organizations. These attacks were not limited to BGP hijack attacks and included stealth traffic manipulations at exchange points and at large Internet Service Providers (ISPs). Some of these attacks lasted for weeks without ever being noticed by its victims.

What can be done? First of all, the financial sector should carefully monitor routing towards its crucial IP space, which includes public facing IP addresses and servers, such as, mail, DNS, and VPN. Secondly, there should be national level monitoring of the routing infrastructure to make sure data from financial organizations are not hijacked outside of the country. Finally, there should be a national sector CERT (the American term is a Fusion-Center) where data about attacks can be shared by financial organizations at multiple levels of anonymity.

Federal regulation can also play a role in managing the risk associated with IP Hijack Attacks. Laws need to be updated in order to regulate who is allowed to own data-communications infrastructure in any given constitution. For example, there are international ISPs such as China Telecom, that have locations (POPs) around the world, however, China does not allow foreign ISPs to establish a local presence on their soil. This lack of symmetry provides China Telecom with an unfair advantage. Making matters worse, even when the culprit is identified, they can very easily claim that it was a configuration error and avoid prosecution.

As I mentioned, I am also the CTO of a company called BGProtect. BGProtect is the leader in the detection and mitigation of IP Hijack & Data-Plane Attacks. Our platform and services are currently in use by global financial institutions, governments, intelligence agencies, service providers and international news agencies. Recent hijack attacks are not limited to BGP, but also of data-plane attacks, (e.g., compromising routers). Our system provides the only available service that can identify all types data-diversion attacks regardless of the technique that is used. We have hundreds of software agents on servers located around the world and more than 600M IP router address geo-locations in our database that we use to provide measurement results in real time to analyze global and local routes with our proprietary AI rules engine for anomalies.

With regards to the Huawei issue, it is important to note that essentially all networking and telecommunications equipment can be vulnerable to hacking and backdoors, and the best way to reduce and mitigate these risks is to invest in traffic monitoring equipment, as the saying goes *"an ounce of prevention is worth a pound of cure".*