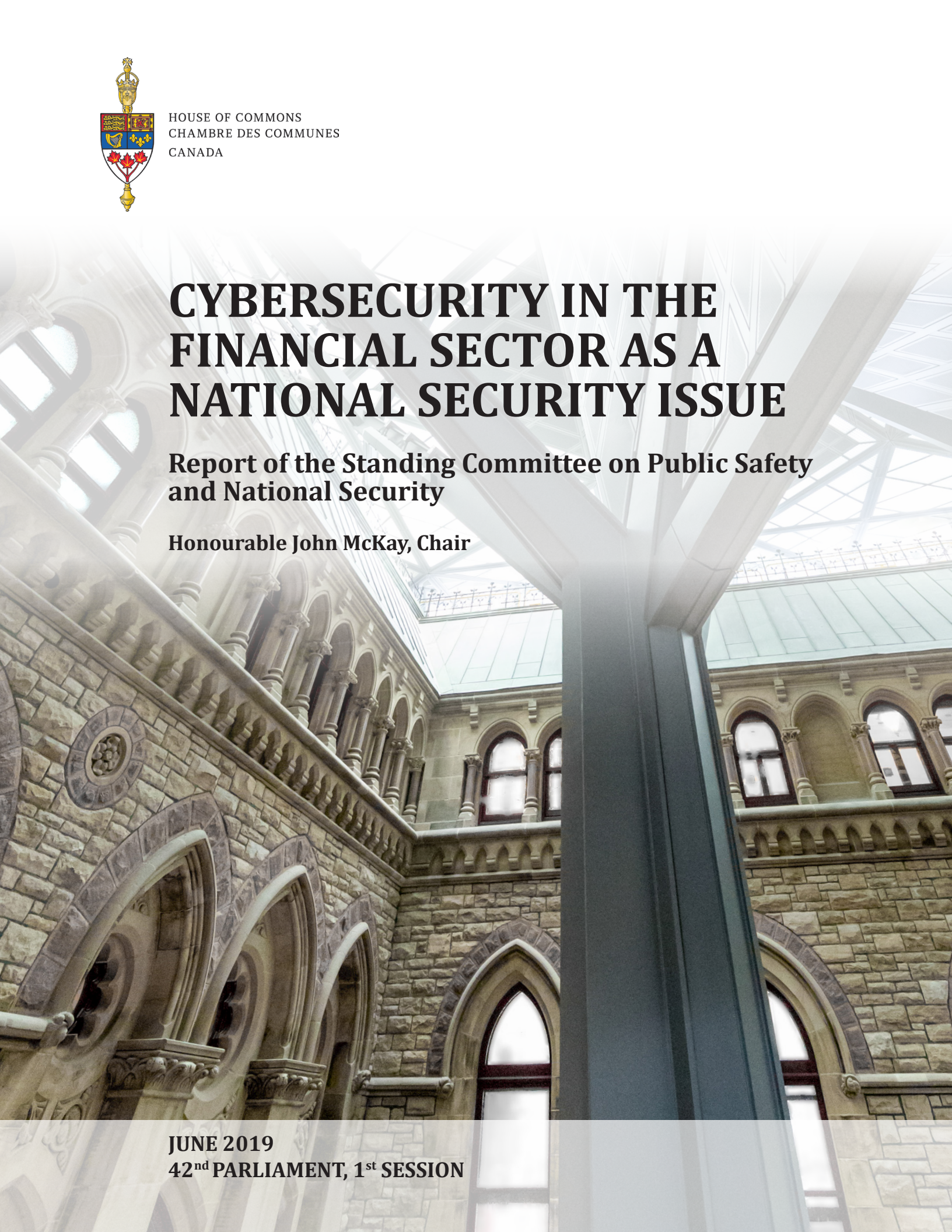


HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

CYBERSECURITY IN THE FINANCIAL SECTOR AS A NATIONAL SECURITY ISSUE

Report of the Standing Committee on Public Safety and National Security

Honourable John McKay, Chair

JUNE 2019
42nd PARLIAMENT, 1st SESSION

CYBERSECURITY IN THE FINANCIAL SECTOR AS A NATIONAL SECURITY ISSUE

Report of the Standing Committee on Public Safety and National Security

Hon. John McKay
Chair

JUNE 2019

42nd PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committee presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY

CHAIR

Hon. John McKay

VICE-CHAIRS

Pierre Paul-Hus
Matthew Dubé

MEMBERS

Julie Dabrusin
Jim Eglinski
David de Burgh Graham
Karen McCrimmon (Parliamentary Secretary – Non-Voting Member)
Glen Motz
Michel Picard
Ruby Sahota
Peter Schiefke (Parliamentary Secretary – Non-Voting Member)
Sven Spengemann

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Chandra Arya
Richard Cannings
Pam Damoff
Anju Dhillon
Earl Dreeshen
Emmanuel Dubourg
Terry Duguid
T.J. Harvey
Randy Hoback
Gudie Hutchings
Stéphane Lauzon

Dave MacKenzie
Ken McDonald
Yves Robillard
Shannon Stubbs

CLERK OF THE COMMITTEE

Naaman Sugrue

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Holly Porteous, Analyst
Dominique Valiquet, Analyst

THE STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY

has the honour to present its

THIRTY-EIGHTH REPORT

Pursuant to its mandate under Standing Order 108(2), the Committee has studied cybersecurity in the financial sector as a national economic security issue and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Recommendation 1

Recommendation 2

Recommendation 3

Recommendation 4

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

CYBERSECURITY IN THE FINANCIAL SECTOR AS A NATIONAL SECURITY ISSUE

CHAPTER 1—CONTEXT OF THE STUDY

A. Mandate of the Committee

On 23 October 2018, the House of Commons Standing Committee on Public Safety and National Security (the Committee) adopted a motion stating that pursuant to

> the Standing Order 108(2) the Committee undertake a study of at least 8 to 12 meetings on cybersecurity in the financial sector as a national economic security issue; that witnesses be invited to speak on the issue in order to identify dangers and to propose concrete protective and preventive measures; and that the Committee make recommendations and report its findings to the House.

Over the course of 12 meetings held between 28 January and 29 May 2019, the Committee heard evidence from 45 witnesses and received six briefs. Along with evidence taken from Canadian government officials and representatives of Canada's private sector and academia, the Committee documented the testimony of witnesses from the United States, Australia and Israel. The Committee appreciates the expertise and participation of all the witnesses who participated in this study.

This report represents the Committee's initial examination of cybersecurity. The Committee hopes that its successor in the 43rd Parliament will explore additional dimensions of this issue in future studies and assess the government's progress towards implementing its recommendations at regular intervals.

Several factors influenced the Committee's decision to start with the financial sector. The first was its belief that national and economic security are tightly bound.[1] Canada cannot claim to have national security if threats to the livelihoods and savings of its citizens and corporations go unanswered. For this reason and in cooperation with its closest allies, Canada should undertake every reasonable effort to prevent or punish cyber aggression.

1 In fact, Mr. Richard Fadden, who served in many senior executive positions in the Canadian security and intelligence community, told the committee that there is no distinction between national and economic security. See House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Richard Fadden, as an individual), 42nd Parliament, 1st Session, 10 April 2019.

At the same time, the Committee recognizes that Canada's standing in the world is determined by more than its willingness to use coercive means to deter threats, including cyber threats. International trade and investment in this country are predicated on trust and confidence. Trust and confidence are, in turn, inspired by reliability. Reliability in the complex and dynamic context of cyberspace is certainly no mean feat to achieve but, for Canada's financial institutions and the businesses that depend upon them, it starts with sound security practices.

Adherence to sound security practices is challenging not only because these best practices are evolving but also because the financial sector is confronting major technological challenges. Some of these challenges are self-imposed. For example, banks and other financial institutions are expanding and digitizing their service offerings, often partnering with financial technology (fintech) start-ups to do so. As small businesses, these fintech start-ups may not be in a position to fully protect themselves against cyber threats. Other challenges are imposed by external forces. For example, now in various stages of adapting to cybersecurity in a post-perimeter[2] world, this sector has no choice but to confront the promise and peril of artificial intelligence (AI)[3] and quantum computing.[4]

Witnesses emphasized that, to retain trust and a competitive edge, the financial sector must build security into every new digital service offering. Failure to build on a solid foundation could be disastrous. The head of Communications Security Establishment's (CSE's) new Canadian Centre for Cyber Security, Scott Jones, described what is at stake, saying:

2 "Post-perimeter" or "zero-trust" security refers to a security model that treats all devices connected to an organization's network as Internet-facing, meaning they could be potentially compromised. In contrast to older, outward-focused models that assume users and computers operating within the perimeter formed by a firewall can be trusted, the post-perimeter model takes nothing for granted and continuously monitors for signs of malicious activity.

3 In this context, "artificial intelligence" refers to machine learning. Machine learning is a subset of artificial intelligence that seeks to create machines that can teach themselves to recognize and draw conclusions about patterns in data without being explicitly programmed to do so. The process is iterative and generally requires repeatedly directing the machine – or, more accurately, the algorithm – to identify patterns provided in datasets, examining the results and adjusting the algorithm based on this feedback.

4 "Quantum computing" refers to the use of quantum mechanical phenomena such as super-positioning and entanglement to achieve computational capacity many times greater than that of current classical computing. For example, whereas classical computing relies on electronic bits that can only exist in two states, on (1) or off (0), quantum computing exploits the capacity of subatomic particles to exist in more than one state at any given moment. This quantum super-positioning means the quantum counterpart to the binary bit, the "qubit," can hold much more information.

> A significant disruption to the financial sector could have effects that reverberate across Canada's entire economy. The effects of a cyber-disruption could be immediate, such as financial loss, or they could occur over the medium to long term in the form of decreased consumer confidence. The risk of a cyber-compromise increases as the financial sector continues its transition to digital services and connects more devices to the Internet.
>
> Nevertheless, this digital transformation has the potential to create tremendous opportunities for growth. To not leverage innovations in digital technology would mean being left out of the global economy. Retrenchment is not an option.[5]

B. Canada's Embrace of Digital Services

Canada's economic well-being rests on the fortunes of its small- and medium-sized enterprises (SMEs). Mr. Scott Smith, the Canadian Chamber of Commerce's senior director of intellectual property and innovation policy, told the Committee that:

> There are 99.7% of businesses in Canada that have fewer than 500 employees, but they employ over 70% of the total private labour force. Small to medium-sized enterprises contribute 50% of [Canada's Gross Domestic Product, GDP], 75% of the service-producing sector and 44% of the goods-producing sector. They also represent 39% of the financial, insurance and real estate sector.[6]

SMEs may account for a little over half of the value of Canada's output, but another recent House of Commons study suggests these entrepreneurs have not yet lived up to their export potential.[7] For example, according to the Business Development Bank of Canada, cybersecurity is among the top challenges firms have when it comes to e-commerce.[8] Is the prospect of preparing to fight off cyber threats while trying to keep an online business afloat too daunting for some? Perhaps. Startup Canada said 44% of its small business affiliates see the "high cost" of researching, integrating and maintaining digital technologies as a "primary barrier to technology."[9]

---

5 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Jones, Head, Canadian Centre for Cyber Security, Communications Security Establishment), 42nd Parliament, 1st Session, 30 January 2019.

6 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Smith, Senior Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce), 42nd Parliament, 1st Session, 18 March 2019.

7 See, for example, House of Commons Standing Committee on International Trade, *E-Commerce: Certain Trade-Related Priorities of Canada's Firms*, Ninth Report, 42nd Parliament, 1st Session, April 2018.

8 House of Commons Standing Committee on International Trade, *E-Commerce: Certain Trade-Related Priorities of Canada's Firms*, Ninth Report, 42nd Parliament, 1st Session, April 2018, p. 19.

9 House of Commons Standing Committee on International Trade, *E-Commerce: Certain Trade-Related Priorities of Canada's Firms*, Ninth Report, 42nd Parliament, 1st Session, April 2018, p. 19.

Nevertheless, to reach international markets, and make further inroads with domestic customers, Canadian SMEs must embrace digital delivery. Financial institutions and fintechs are a core element of this digitization process, facilitating secure online and mobile transactions. For example, small businesses are turning to online payment platforms to reach international markets. PayPal – the largest of these platforms and, at 21 years old, one of the oldest fintechs – counts 250,000 small Canadian businesses as clients.[10]

With an annual 55% growth rate expected to continue through 2020, Canada has become a "hotspot" for fintech start-ups. Mr. Smith drew attention to the fact that most of these fintech start-ups are mobile payments-focused SMEs and warned that these smaller players "collectively constitute a very large attack surface."[11]

The statistics behind Canada's broader financial digitization speak for themselves. Ninety percent of Canadians use the Internet[12] and, according to the Canadian Chamber of Commerce, 72% are doing their banking online or through a mobile device.[13]

Canadians are increasingly shopping online, with 86% of those 18 years and older having made an online purchase in the last 12 months.[14] In January 2019 alone, Canadian retail e-commerce sales were estimated at $1.4 billion, accounting for 3.3% of total retail trade.[15] A recent Statistics Canada survey found that between 2010 and 2017, e-commerce's contribution to the digital economy doubled, climbing from 5.5% to

10 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Brian Johnson, Senior Director, Information Security, PayPal Inc.), 42nd Parliament, 1st Session, 29 May 2019.

11 "Attack surface" (also called "threat surface") refers to all available Internet-accessible end-points attackers may attempt to exploit to achieve their objectives. House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Smith, Senior Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce), 42nd Parliament, 1st Session, 18 March 2019.

12 Canadian Internet Registration Authority, *Canada's Internet Factbook 2018*.

13 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Trevin Stratton, Chief Economist, Canadian Chamber of Commerce), 42nd Parliament, 1st Session, 18 March 2019.

14 Canadian Internet Registration Authority, *Canada's Internet Factbook 2018*.

15 Statistics Canada, *Table 4, Retail e-commerce sale—unadjusted, February 2019*. Please note that Statistics Canada notes that this figure is not seasonally adjusted.

12.4%.[16] The Business Development Bank of Canada predicts that, by 2020, annual Canadian retail e-commerce purchases will reach $56 billion.[17]

Recommendation 1

The Committee recommends that, in the next Parliament, the House of Commons Standing Committee on Public Safety and National Security establish a sub-committee dedicated to studying the public safety and national security aspects of cybersecurity, with potential areas of inquiry including international approaches to critical infrastructure protection, impact of emerging technologies, and cyber supply chain security.

CHAPTER 2—CHALLENGES, THREATS AND RISK MITIGATION

A. Cybersecurity in a Post-Perimeter World

Over the course of its study, the Committee learned that cybersecurity best practices have undergone profound change in the past decade. Anti-virus programs, firewalls, and intrusion detection systems still have their place in organizational cybersecurity, but the context of their use has completely changed.

It is no longer enough to deploy these tools in the belief that they will form a hard perimeter separating internal trusted space from the external untrusted space of public networks (i.e. the Internet). Bring-your-own-device to work policies, USB drives and social engineering attacks[18] have all punched holes through perimeter defence. Organizations have little choice but to assume breach and continuously hunt for the signs of it, said witnesses.

16 Please note that, in this survey, Statistics Canada defines the digital economy as "activities that enable digitization or are highly affected by it." Statistics Canada goes on to state that "the digital economy includes the information technology equipment that it relies upon to function, as well as e-commerce transactions and the digital delivery of products to consumers." See Statistics Canada, "Measuring digital economic activities in Canada, 2010 to 2017," *The Daily*, 3 May 2019.

17 Business Development Bank of Canada, cited in House of Commons Standing Committee on International Trade, *E-Commerce: Certain Trade-Related Priorities of Canada's Firms*, 42nd Parliament, 1st Session, April 2018, p. 7.

18 As its name suggests, social engineering attacks circumvent security policy through psychological manipulation. Communications Security Establishment describes a range of cyber threat techniques, including social engineering attacks, in a public awareness document. See Canadian Centre for Cyber Security, "Annex A: The Cyber Threat Toolbox," *An Introduction to the Cyber Threat Environment*.

Informing this hunt are an array of data inputs that must be analysed and acted upon quickly to stop a threat in its tracks. AI is a natural partner for cybersecurity practitioners in this endeavour, providing automated threat identification and, in some circumstances, automated response.

While it was clear to the Committee that larger organizations in the financial sector have integrated AI tools into their cybersecurity programs, witness testimony suggests SMEs – both those in the financial sector and those that depend upon it – are not necessarily able to do so.

Given the array of threat actors targeting Canada's financial institutions, the accelerated rate of technological change taking place within this sector and the extent to which Canada's economic activities now take place within a digital context, the need to examine cybersecurity is clear. Digitization has not only opened up markets for Canadian businesses, it has dramatically increased the available attack surface to cyber threat actors wanting to target Canada.[19]

B. Threat Environment

Witnesses spoke with one voice when they described a relentlessly dynamic threat environment. They said our banks, credit unions, trust companies and other financial institutions face state and non-state threat actors that are opportunistic and continuously innovating their tactics and techniques.

The opportunistic nature of these threat actors was apparent in the Royal Canadian Mounted Police's (RCMP's) description of how cybercriminals target Canada's financial sector. They attack the core infrastructure of financial institutions directly and, if that does not work, they swim further downstream to target individual users. The Director General of the RCMP's Financial Crime and Cybercrime unit, Chief Superintendent Mark Flynn, characterized the way cybercriminals work as follows:

> Cybercriminals may attempt to directly compromise the financial institution's computer infrastructure through attacks that grant unauthorized access to the core systems themselves. These attacks are attempts to make a profit through the theft of money

19 Communications Security Establishment's (CSE's) Canadian Centre for Cyber Security uses a slightly different term, "threat actor surface," which it defines as "all the available endpoints that a threat actor may attempt to exploit in Internet-connected devices within the cyber threat environment." CSE goes on to say, "Services, devices, and data can all be targeted to compromise production and delivery systems, such as supply chains and service management systems. As these processes continue to evolve, the threat surface will expand." See Canadian Centre for Cyber Security, "Cyber Threat Surface," *An Introduction to the Cyber Threat Environment*, 2018.

> from those systems or through the movement of money through those systems, to steal private information or, in some cases, to damage the reputation of the company. These crimes are perpetrated by individuals working alone, organized crime groups or professional cybercriminals employed by larger entities, including foreign state actors.
>
> Criminals also indirectly attack financial institutions by obtaining user credentials or other personal information to gain unauthorized access to individual user accounts. Obtaining these user credentials can be done in a number of ways: by using accessible tools from the Internet to obtain passwords, through social engineering or by simply purchasing large databases of personal information on the dark web. The relatively low cost of these attacks has enabled both malicious individuals and new organized crime cyber groups to undertake these attacks on an unprecedented scale.[20]

It is worth underscoring the RCMP's observation that personal data held by banks and other financial institutions is of great interest to cybercriminals, particularly as the financial sector begins to explore tailoring their service offerings through advanced analysis of customer data collected via the Internet of Things (IoT).[21]

We know, in the wake of the Mirai botnet attacks,[22] that poorly secured IoT devices are pervasive. Not one witness had a positive assessment of the current state of IoT security. Mr. Christopher Porter, Chief Intelligence Strategist for FireEye, Inc., summed up the situation perfectly when he said, "[m]y number one concern with the Internet of things, … – Internet-connected physical devices – is that many of those devices are not updatable at all. Even if you discover a flaw in them, it's not technically possible to go in and fix it."[23] Mr. Scott Jones went one step further by calling on industry to demand more from product vendors. Specifically, he stated:

> I think the key thing for us is that – you're right – the equipment we're buying does not come secure by default. It's very poorly built, and that's getting worse with the Internet of things. That's a dynamic that we have to change, and we're encouraging industry to

---

20 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chief Superintendent Mark Flynn, Director General, Financial Crime and Cybercrime, Federal Policing Criminal Operations, Royal Canadian Mounted Police), 42nd Parliament, 1st Session, 28 January 2019.

21 See, for example, Jim Eckenrode, Executive Director, Deloitte Center for Financial Services, Deloitte U.S., "Future Scenarios for IoT in Financial Services," sponsored content, *CIO Journal, The Wall Street Journal*, 6 January 2016.

22 Mirai is the name given to malware used to create multiple networks of compromised Internet of Thing devices. The resulting "botnets" were, in turn, used to conduct a series of damaging cyberattacks that first gained public attention in 2016, when distributed denial of service attacks on Internet Domain Name Servers operated by U.S. company, Dyn, caused Internet outages across Europe and North America. See, Brian Krebs, "Mirai Botnet Authors Avoid Jail Time," *Krebs on Security* (Blog), 19 September 2018.

23 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Christopher Porter, Chief Intelligence Strategist, FireEye, Inc.), 42nd Parliament, 1st Session, 6 February 2019.

> ask for security to be built in. They shouldn't have to pay extra. There are security features that should come in as part of any piece of equipment.[24]

Mr. Mark Ryland, Director of the Office of the Chief Information Officer for Amazon Web Services, told the Committee that vendors are beginning to take up the "secure by design" challenge, saying:

> [W]e've all recognized the problems in the past with the Internet of things – home devices, etc. – being deployed in a very insecure fashion. Historically, it was the cheapest and easiest thing to do. If you look at the newer technology that we provide, or that Microsoft or other large-scale providers give you, by default their systems are far more secure. They're updatable in place, which they didn't use to be. They use secure protocols by default; they didn't use to do that. You can go right down the list of how the business interests of these large providers align with building systems that are secure by default, whereas previously, that was left to the person who was building the smart refrigerator or the smart toaster or whatever.[25]

Without a doubt, the IoT represents a major threat vector for the financial sector and the Committee believes every effort must be made to close it off.

Recommendation 2

Along with encouraging Canadians to adopt sound cyber hygiene habits, the Committee recommends that the Government of Canada undertake efforts to ensure the digital products and services they rely on, including products that are part of the Internet of Things, are "secure by design."

To achieve this objective, witnesses told the Committee, private-public partnership will be key. Payments Canada's Chief of Operating Officer, Mr. Justin Ferrabee, described the scope of his organization's collaboration as follows:

> From a wider, collaborative industry perspective, we work very closely with partners in the financial sector through cybersecurity industry groups such as the Canadian Financial Services Cybersecurity Governance Council, the Canadian Bankers Association cybersecurity specialist group, and the Financial Services Information Sharing and Analysis Center.

---

24 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Jones, Head, Canadian Centre for Cyber Security, Communications Security Establishment), 42nd Parliament, 1st Session, 30 January 2019.

25 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Mark Ryland, Director, Office of the Chief Information Officer, Amazon Web Services, Inc.), 42nd Parliament, 1st Session, 15 May 2019.

> We also participate in and lead industry exercises for business continuity and cyber-resilience and share intelligence with partner agencies and organizations in the cyber community. These connections include the Canadian Centre for Cyber Security, Public Safety's critical infrastructure protection branch, RCMP's national critical infrastructure team, and the Canadian Cyber Threat Exchange. Further to these collaborations, we are actively engaged in the international cyber-risk community with our partners at the Bank of Canada.[26]

Someone who watches financial sector cyber threats for a living – TD Bank's Chief Information Security Officer, Glenn Foster – highlighted the agility with which these adversaries can identify and exploit new threat vectors, saying,

> Current attacks are very sophisticated. They're evolving on an almost daily basis. From the time of zero day[27] out in the public to the time the commercial vendor can patch, to the time that large institutions can patch those vulnerabilities, the window, although getting so much shorter, is still significantly greater than the speed at which adversaries can develop scripting and start scanning everyone on the Internet. Part of that automation, in some cases using AI to be more rapid in how it identifies these vulnerabilities, is becoming a much more significant problem for us.[28]

Worse yet, according to cybersecurity practitioners who spoke to the Committee, the average dwell time for an attacker that has managed to penetrate a corporate network is 101 days and, in instances where they have penetrated a corporate datacentre, six months.[29] This gives the attacker time to move laterally throughout a victimized company's internal network and data holdings, quietly bleeding the company of its most sensitive information and implanting additional malware that can be activated at a future point if need be.

---

26 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Justin Ferrabee, Chief Operating Officer, Payments Canada), 42nd Parliament, 1st Session, 8 April 2019.

27 A "zero day" is an exploitable software vulnerability that is either unknown to or unaddressed by those responsible for maintaining its security.

28 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Glenn Foster, Chief Information Security Officer, Toronto Dominion Bank), 42nd Parliament, 1st Session, 3 April 2019.

29 Whereas ADGA Group's Director of Cybersecurity, Steven Drennan, cited a global average dwell time of 101 days on an organizational *network*, Illumio's Head of Cybersecurity Strategy, Jonathan Reiber, cited an average dwell time of 6 months for an organization's *datacentre*. See House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Steve Drennan, Director of Cybersecurity, ADGA Group), 42nd Parliament, 1st Session, 10 April 2019; and, House of Commons Standing Committee on Public Safety and National Security, *Briefing: Defend Forward and Assume Breach: Preparing Canada for a cyberresilient future* (Jonathan Reiber, Head of Cybersecurity Strategy, Illumio), 42nd Parliament, 1st Session, 10 April 2019, p. 3.

The Committee received no attacker dwell-time data specific to the financial sector. It can only hope, therefore, that this sector fairs much better on that count.

Citing a recent Statistics Canada report[30] that indicated "nearly half of Canadian organizations in the banking sector were impacted by cybersecurity incidents," Scott Jones, the head of CSE's new Canadian Cyber Security Centre, said cybercriminals are the financial sector's main threat.[31] Though they may be interested in creating havoc, nation-states and nation-state-sponsored threat actors are less of a concern, he said, explaining that, among Canada's 10 critical infrastructures, the financial sector is "a relatively hard" target for a nation-state to disrupt. So, based on this and other witness statements, it appears that, overall, the financial sector is indeed better than most when it comes to cybersecurity best practices.

However, even if many organizations within the financial sector are doing a good job of protecting their assets from cyber threats, the Committee is concerned about the smaller businesses in this sector. The RCMP's comments about criminal opportunism come to mind, as do the Canadian Chamber of Commerce's observations about the SMEs that dominate Canadian fintech. On this latter topic, Mr. Smith said:

> Small to medium-sized enterprises have several challenges when it comes to security: limited financial resources, limited human resources and a culture of disbelief, the so-called "we're too small to be hacked" syndrome.[32]

For the financial sector to be considered truly cybersecure, security must be end-to-end. As Satyamoorthy Kabilan, Vice-President of Policy at the Public Policy Forum, quipped:

> [Financial sector cybersecurity] is like armoured vehicles with armed officers taking money between two cardboard boxes, and it's the cardboard box at the end that we worry about, because the user at the end may not be as well defended or may not understand things as well as the bank or the financial institution or the provider of the services might.[33]

---

30 See Howard Bilodeau, Mohammad Lari and Mark Uhrbach, *Cyber security and cybercrime challenges of Canadian businesses, 2017*, Statistics Canada, 28 March 2019.

31 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Scott Jones, Head, Canadian Cyber Security Centre), 42nd Parliament, 1st Session, 30 January 2019.

32 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Smith, Senior Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce), 42nd Parliament, 1st Session, 18 March 2019.

33 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Satyamoorthy Kabilan, Vice-President, Policy, Public Policy Forum), 42nd Parliament, 1st Session, 30 January 2019.

C. Risk Mitigation

While there are areas of concern, particularly with respect to SMEs and customer cybersecurity, the Committee believes larger organizations within the financial sector are focused on cyber threats and undertaking appropriate risk mitigation measures. In fact, this sector's pioneering use of AI for fraud detection means it has been better placed than most to start using this technology to detect and respond to cybersecurity threats. According to Scott Jones, the financial sector has leading-edge capabilities in using AI to detect fraud and CSE seeks to leverage this expertise for cyber defence purposes.[34]

Mr. Jonathan Reiber, the head of Cybersecurity Strategy for Illumio, a U.S.-based company, confirmed that the financial sector has significant strengths in cybersecurity. These strengths are those of the battle-hardened, he said, stating that,

> The interesting thing about the financial sector is that it has been under attack probably since it moved over to the Internet. There are a number of major breaches that have caught the attention of the national security community as well as the banking sector, and it has led the banking sector to invest quite a lot in cybersecurity capabilities. It's for that reason that they're so far ahead.
>
> I may have already commented on this, but they're much further advanced than a lot of the other sectors in the U.S. You could opine that part of the reason is that they're able to attract the best talent to their workforce. They're able to pay good salaries to attract people who want to work hard.[35]

It is clear, also, that members of this community are habituated to collaboration on security matters. For example, witnesses repeatedly welcomed the opportunity to work with the Canadian Centre for Cyber Security and the RCMP's new National Cybercrime Coordination unit. Witnesses also highlighted the useful contribution to information sharing that the Canadian Cyber Threat Exchange Centre (CCTX), a non-profit organization, has already been making.

The CCTX is an Ottawa-based, non-profit organization that provides a means for businesses, including banks, to share information about threats and vulnerabilities as well as cybersecurity best practices. Its nine founding members, which included the Toronto Dominion Bank and the Royal Bank of Canada, were all large enterprises.[36]

---

34 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Scott Jones, Head, Canadian Cyber Security Centre), 42nd Parliament, 1st Session, 30 January 2019.

35 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Jonathan Reiber, Head, Cybersecurity Strategy, Illumio), 42nd Parliament, 1st Session, 6 February 2019.

36 Canadian Cyber Threat Exchange, *About CCTX: Founding Members + Advisory Board*.

However, since it first commenced operations in December 2016, the CCTX has actively sought to attract smaller businesses through reduced membership fees.[37] Mr. Bob Gordon, CCTX's executive director, told the Committee about his organization's efforts towards this goal:

> [T]he large companies that founded the CCTX made it clear that the CCTX cannot be just for large organizations. We need to attract small and medium-sized organizations. In every sector of the economy, all sizes of organizations are experiencing cyber-attacks. We've grown from the initial nine founding members to just under 60 today, with additional applications being processed weekly.
>
> In January this year, we changed our membership and fee structures to make membership more attractive to small and medium-sized organizations. Those changes have been really well received. Small organizations now represent 28% of our membership, and we're working to ensure this number grows significantly. As we increased the number of small organizations, we were developing cybersecurity reports and services specifically tailored to meet the needs of the small business owner.[38]

While each organization must bear individual responsibility for cybersecurity risk mitigation, sector-wide collaboration and information-sharing are the *only* way to address systemic cybersecurity risks. In this connection, the Committee also notes the key role of Payments Canada in providing for sector-wide cybersecurity.

Payments Canada operates this country's two payment systems, the Large Value Transfer System (LVTS) and the Automated Clearing Settlement System (ACSS). Due to their critical role in the stability of Canada's financial system, the Bank of Canada has designated the LVTS and ACSS as "Financial Market Infrastructures" (FMIs) under the *Payment Clearing and Settlement Act*. Should either system suffer a catastrophic failure, the resulting loss of trust and confidence in our financial system would be profound. Payments Canada must, therefore, satisfy the Bank of Canada that the LVTS and ACSS are "resilient to shocks", meaning they can recover quickly from any cyber attack.[39]

---

37 Cision, "The Canadian Cyber Threat Exchange (CCTX) is operational and reaching out to Canadian businesses,"News provided by Canadian Cyber Threat Exchange, 9 December 2016.

38 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Bob Gordon, Executive Director, Canadian Cyber Threat Exchange), 42nd Parliament, 1st Session, 1 April 2019.

39 See also Bank of Canada, Filipe Dinis, Chief Operating Officer, "Strengthening Our Cyber Defences", remarks to Payments Canada, Toronto, Ontario, 9 May 2018.

CHAPTER 3—CYBER SUPPLY CHAIN SECURITY

Given Payments Canada's pivotal cybersecurity role, the Committee took note when Mr. Justin Ferrabee, called for a software equivalent to Canada's food labelling standards. He explained his proposal as follows:

> The modern supply chain often includes hundreds, or thousands, of software components that are embedded in critical systems sourced from companies and communities all around the world.
>
> It is a significant task to track and inventory all of the ingredients of a system and make sure that those ingredients remain safe. In the food safety world, we have labelling standards that inform customers about product ingredients and nutritional facts, but in the software world, we have no labelling standard to help consumers understand what components and what risks might exist within the software. Policy to support digital supply chain risk is necessary and system labelling of software components should be studied for its benefits to the economy.[40]

Building on this analogy, it appears that Payments Canada is suggesting the establishment of a mandatory software "bill of materials" regime. To be permitted to sell their products in Canada, all software vendors would be required to provide comprehensive information on them. Like food labels, such information could include the country (or countries) of origin; "ingredients" (i.e. all software features and functionality); "allergens" (i.e. vulnerability declarations); and a "best by date" (i.e. the date on which the vendor will no longer support the product with security patches). Under such a regime, software vendors would list all software components used in making their product, declare that this software has either no known vulnerabilities or contains the least vulnerable software version publicly available, and provide a mechanism to patch any vulnerabilities that arise over the declared lifespan of the product.

While the Committee believes there is value in requiring software vendors to be more transparent about their products, questions remain about how this labelling approach might work outside of high-assurance environments and be implemented within the context of the existing international standards framework.[41]

---

40 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Justin Ferrabee, Chief Operating Officer, Payments Canada), 42nd Parliament, 1st Session, 8 April 2019.

41 Driven by consumer demand, current commercial software development practices favour rapid to-market cycles. Rather than lose valuable time creating software from scratch, developers therefore turn to a multitude of globally dispersed open-source software development frameworks, operating systems and code libraries. Given this reality, cataloguing all components that go into the making of a piece of software with enough granularity to assist vulnerability tracking would be extremely challenging. Thousands of subcomponents can go into the making of a simple software application. As one cybersecurity industry

A high-assurance environment is one where, for reasons of safety and/or security, all systems operating in that environment must be certified to function exactly as expected. Essentially, systems that have been certified for use in a high-assurance environment can be trusted to not have hidden functionality (e.g. backdoors) that can be exploited for nefarious purposes. To meet this requirement, the systems are built according to exacting standards, undergo rigorous testing and evaluation, and are certified to be secure when operated in a specified configuration. It follows that software certified to operate in a high-assurance environment will have constrained functionality and remain stable over time.

Numerous witnesses echoed Mr. Ferrabee's comments about the importance of addressing cyber supply chain risks. However, whereas Mr. Ferrabee focused on software components, others applied a broader scope. Satyamoorthy Kabilan, Vice-President of Policy at the Public Policy Forum, included managed service providers in his definition, saying cyber supply chains "involve not just the bits and pieces we buy, but also the organizations that provide services to us."[42]

In this regard, the Canadian Bankers Association's response to the Committee's questions about the obligations of financial institutions towards their clients when they outsource services to foreign-based, third-party service providers was concerning. Asked what would happen in a case where a Canadian bank outsourced to a U.S.-based credit card company and the latter suffered a cybersecurity breach that exposed Canadian client information, Mr. Charles Docherty, Assistant General Counsel with the Canadian Bankers Association (CBA), explained that "[i]f it's an independent third party, then the laws of the country where the information is being held by that third party may apply."[43]

A. Communications Security Establishment's Role in Cyber Supply Chain Security Assurance for Critical Infrastructure

CSE plays a pivotal role in providing cyber supply chain security assurance for critical infrastructure. Since 2013, working in partnership with Public Safety Canada and

observer points out, simply listing all licensed software modules rather than all the individual subcomponents of these software modules may make for a relatively short list but would provide insufficient information to be of use in the likely event that a vulnerability is discovered in subcomponent. To read further, see Rob Graham, "Security Essentials: Software Bill of Materials (SBoM) - Does It Work for DevSecOps?", AT&T Cybersecurity (blog), 14 January 2019.

42 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Satyamoorthy Kabilan, Vice-President, Policy, Public Policy Forum), 42nd Parliament, 1st Session, 30 January 2019.

43 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Charles Docherty, Assistant General Counsel, Canadian Bankers Association), 42nd Parliament, 1st Session, 18 March 2019.

Innovation, Science and Economic Development, it has overseen a testing and evaluation program for designated equipment that telecommunications services providers are considering deploying on their networks. This undertaking is referred to as the Canadian Security Review Program. CSE-accredited third-party laboratories are used for product testing and evaluation.[44]

Private sector engagement on the Canadian Security Review Program now takes place through CSE's Canadian Cyber Security Centre, which was established on 1 October 2018.

In his testimony to the Committee, Mr. Scott Jones, noted the prominence given to cyber supply chain security in the Centre's *National Cyber Threat Assessment 2018* and said that his organization was "working closely" with businesses on the issue.[45] This threat assessment defines cyber supply chain as "as the system of organizations, people, technology, activities, information and resources involved in moving a product or service from a supplier to a customer."[46]

Given CSE's current activities in high-assurance product testing and evaluation under the Canadian Security Review Program, the Committee believes that expanding the remit of this program could enhance cyber supply chain security for critical infrastructure beyond that owned and operated by the telecommunications sector.

B. A Possible Role for the Canadian Standards Association?

Mr. Steve Waterhouse, a former information systems security officer with the Department of National Defence, sees the Canadian Standards Association (CSA) as another potential support to supply chain security.[47] Though the CSA has historically focused on certifying product safety, in 2017 it established a Cybersecurity Program that offers cybersecurity testing and evaluation based on internationally recognized standards.[48] Given the existence of these two programs, the Committee believes there is

44 See Canadian Cyber Security Centre, *CSE's Security Review Program for 3G/4G/LTE in Canadian Telecommunications Networks*.

45 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Scott Jones, Head, Canadian Cyber Security Centre), 42nd Parliament, 1st Session, 30 January 2019.

46 See Canadian Cyber Security Centre, "Endnote 14," *National Cyber Threat Assessment 2018*.

47 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Steve Waterhouse, Former Information Systems Security Officer, Department of National Defence), 42nd Parliament, 1st Session, 4 February 2019.

48 Canadian Standards Association, "Overview: CSA Group's New Cybersecurity Program Brings Cybersecurity Testing Services to Manufacturers," News & Press, 19 July 2017.

merit in creating a certification regime whereby the CSE would evaluate and certify the security of all products destined for critical infrastructure and the CSA would certify all other Internet-connectable products to be used in the broader Canadian commercial market. The latter certification regime, along with enhanced consumer awareness of the need for good cyber hygiene, would go a long way towards strengthening the cybersecurity of Internet-connected end-point devices, those "cardboard boxes" Mr. Kabilan spoke of. Though both regimes would benefit from such an approach, the Committee sees particular value in CSA certification providing product security information in plain language that the average consumer can easily understand.

C. Huawei, 5G and Cyber Supply Chain Security

As Scott Jones alluded to in his testimony, for the past six years CSE has been overseeing the testing and evaluation of certain types of equipment that telecommunications service providers are considering deploying on their infrastructures.[49] Huawei products are among those that have been evaluated.[50]

Queried about the national security threat posed by China and, by extension, products manufactured by Chinese telecommunications equipment providers like Huawei, Mr. Jones stated:

> From our perspective, one of the things we highlight in the *National Cyber Threat Assessment* is that we have to be vigilant against every nation-state, and certainly cyber-techniques are within the realm of every nation-state. Some are more aggressive.
>
> Certainly in the past, CSE has been asked to attribute malicious cyber-activity to certain countries, and that's one of those things that we'll continue to do as per government's broader policy. It's something that we are always looking at, but, for me, we don't defend against only one; we have to defend against everybody.[51]

"In my job, I actually trust nothing," he said, adding that "I assume that there are vulnerabilities in every single piece of product we have…."[52]

---

49 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Scott Jones, Head, Canadian Cyber Security Centre), 42nd Parliament, 1st Session, 30 January 2019.

50 See Canadian Cyber Security Centre, *CSE's Security Review Program for 3G/4G/LTE in Canadian Telecommunications Networks*.

51 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Jones, Head, Canadian Cyber Security Centre), 42nd Parliament, 1st Session, 30 January 2019.

52 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Jones, Head, Canadian Cyber Security Centre), 42nd Parliament, 1st Session, 30 January 2019.

The above-cited comments reflect the "zero-trust" philosophy of current cybersecurity best practice.[53] The Committee believes that this approach is an essential guiding principle. The Committee also believes CSE's security review program provides a high standard of testing and evaluation. Indeed, the United States also recognizes the quality of work performed by the CSE-accredited labs that do this work and has accredited these same private-sector labs to perform cryptographic and security testing for products destined for its own critical systems.[54]

However, given the difficulty of definitively establishing trust in the devices and software we rely upon, the Committee questions the wisdom of using technology produced in China. Indeed, Professor Leuprecht called for an outright ban on Huawei participating in the development of Canada's 5G mobile network. He told the Committee that:

> As a result of a recent change in a Chinese law, China can request any domestic company, including Huawei, to assist it to support national interests, including intelligence interests.
>
> A related concern is that China and its industries are suspected to engage in industrial espionage on a large scale as an inexpensive means of R and D transfer. Moreover, Huawei and the ruling Communist Party appear interwoven in many important fashions, including via state subsidies of reportedly $10 billion in a single year. The systematic theft of IP, along with the massive state subsidies, made it impossible for such competitors as Nortel Networks to compete, and ultimately helped precipitate the demise of Canada's premier high-tech company. Since communications are a critical infrastructure, the government should be excluding wholesale any foreign entity with suspected ties to any country where strong evidence exists of significant prior IP theft or intelligence gathering.[55]

53 As noted previously, the post-perimeter security model is also referred to as "zero-trust." This is because the model assumes the perimeter has been breached and the trustworthiness of each device and user must be continuously verified.

54 National Institute of Standards and Technology, "National Voluntary Laboratory Accreditation Program (NVLAP): Directory Search." (Search directory, selecting "ITST: Cryptographic and Security Testing" for the program and "Canada" for the country).

55 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Christian Leuprecht, Professor, Department of Political Science, Royal Military College of Canada, As an Individual), 42nd Parliament, 1st Session, 30 January 2019.

In this connection, the Committee also takes note of concerns raised by Professor Jill Slay, the La Trobe Optus Chair of Cyber Security at La Trobe University in Melbourne, who spoke of Huawei's reputation as "a company that has constantly stolen IP."[56]

Huawei's leadership may have articulated good intentions,[57] but its government's past and recent actions are deeply problematic.[58] For example, Yuval Shavitt, a professor at Tel Aviv University's School of Electrical Engineering told the Committee that state actors, including China, regularly exploit weaknesses in the Internet's architecture to divert massive flows of communications traffic to infrastructure under their control. He explained what he had been seeing as follows:

> 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.[59]

---

56 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Jill Slay, Professor, La Trobe Optus Chair of Cyber Security, La Trobe University, Melbourne), 42nd Parliament, 1st Session, 20 February 2019.

57 For example, in January 2019, responding to a series of questions posed to it by the chair of United Kingdom House of Commons Science and Technology Select Committee, Huawei wrote an open letter that stated "Huawei has never and will never use UK-based hardware, software, or information gathered in the UK or anywhere else globally, to assist other countries in gathering intelligence. We would not do this in any country." See, United Kingdom House of Commons Science and Technology Select Committee, *Correspondence from Huawei*, 29 January 2019.

58 Some witnesses expressed concern about China's past and present behavior towards Canada as well as the potential for it to use Huawei to act against Canada's national security interests. See, for example, House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Christian Leuprecht, Professor, Department of Political Science, Royal Military College of Canada, As an Individual), 42nd Parliament, 1st Session, 30 January 2019; House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chris Parsons, Research Associate, Monk School of Global Affairs, University of Toronto), 42nd Parliament, 1st Session, 27 February 2019; and See House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Richard Fadden, as an individual), 42nd Parliament, 1st Session, 10 April 2019.

59 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Yuval Shavitt, Professor, Tel Aviv University), 42nd Parliament, 1st Session, 20 February 2019.

CHAPTER 4—EMERGING THREATS

A. Weaponized Artificial Intelligence

Witnesses alerted the committee to two emerging cybersecurity threats: malicious artificial intelligence and quantum computing. Though the former threat stands at our doorstep, the latter, whose arrival may be years away, poses such far-reaching impacts that it also demands immediate attention.

For cybersecurity, AI is truly a doubled-edged sword. Cybersecurity practitioners who spoke to the committee agreed that it is an essential tool in a post-perimeter world where one must assume breach and look for signs of compromise on internal systems and workflows. David Masson offered the following explanation of AI's growing centrality to cybersecurity:

> In the past, companies were focused on securing their networks from the outside in, hardening their perimeter with firewalls and end-point security solutions. Today, migration to the cloud and the rapid adoption of the Internet of Things has made securing the perimeter nearly impossible. Another traditional approach, known as rules and signatures, relied on searching for known bad. However, attackers evolve constantly, and this technique fails to detect novel and targeted attacks. Most importantly, these historical approaches fail to provide businesses with visibility and awareness into what is taking place on their networks, making it hard, if not impossible, to identify threats already on the inside.[60]

Steve Drennan, Director of Cybersecurity for ADGA Group, advocated for a "centralized AI" that could provide sector-wide "security orchestration," essentially conducting semi- or fully-automated responses to cyber threats.[61] He said,

> Think of this as next generation solutions that could be deployed on scale for everyone to use and take advantage of. The concept is that one organization could actually lead this effort and put this capability in a central location so that it would be turned on for all of the [financial sector] entities.[62]

60 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (David Masson, Director, Enterprise Security, Darktrace), 42nd Parliament, 1st Session, 18 March 2019.

61 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Steve Drennan, Director of Cybersecurity, ADGA Group), 42nd Parliament, 1st Session, 10 April 2019.

62 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Steve Drennan, Director of Cybersecurity, ADGA Group), 42nd Parliament, 1st Session, 10 April 2019.

Other witnesses called for more caution when it comes to relying on AI for cybersecurity. For example, Christian Leuprecht, offered the following caveat,

> AI is not this sort of fantastic, magical hat we pull a rabbit out of and whatnot. I mean, AI is just math. It's just fancy, sophisticated math and its applications. While the government has invested significantly in various applications of that, the irony is that the government has not made an investment in the cybersecurity side of those applications.[63]

At the same time, Professor Leuprecht also appeared to support the notion of creating a centralized and presumably automated[64] threat detection and response capability to protect Canadian critical infrastructure, including the financial sector.

Referring to deep packet inspection[65] performed by CSE here in Canada to protect government networks and in Australia by that country's telecommunications providers to protect clients, he lamented the reluctance of Canadian telecommunications to follow the same path, despite having similar legal frameworks. He offered the following explanation for the Canadian telecommunications providers' reluctance:

> Two issues prevent this from being fully exploited. First, the level of detection is so expensive that there's little incentive for telecom providers to get into that business. Second, telecom providers consider that amelioration, once detected, legally problematic.[66]

The Committee thinks there may be value in further exploring how this divergence between the Canadian and Australian approaches came about.

---

63 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Christian Leuprecht, Professor, Department of Political Science, Royal Military College of Canada, As an Individual), 42nd Parliament, 1st Session, 30 January 2019.

64 The sheer scale of network traffic to be analysed and acted upon by telecommunications providers would obviate manual approaches.

65 Deep packet inspection refers to the use of tools to examine the header, and possibly content, of Internet Protocol (IP) packets to detect protocol non-compliance, malware, spam and other indicators of malicious cyber activity.

66 House of Commons Standing Committee on Public Safety and National Security, *Evidence*, (Christian Leuprecht, Professor, Department of Political Science, Royal Military College of Canada, As an Individual), 42nd Parliament, 1st Session, 30 January 2019. The Committee notes that telecommunications providers have expressed concerns about potential legal liability because, under section 430(1.1) of the *Criminal Code*, it is illegal to destroy, alter, obstruct or interfere with the lawful use of computer data. This and other legal issues were raised in a 2013 Defence Research and Development Canada-commissioned paper, *The Dark Space Project*. Bell Canada was listed among the paper's authors. See, Dave McMahon, Rafal Rohokinski, Bell Canada, *The Dark Space Project*, Defence Research and Development Canada, Centre for Security Science, July 2013.

AI can also help prevent poorly written software from ever entering the market place. Software developers can now use AI-enabled platforms to find and eliminate vulnerabilities in their code.[67]

However, there is a downside to automated code analysis. There are growing signs that AI is being used to assist, if not conduct, cyber attacks. Witnesses told the Committee that AI will "lower the bar", making it easier for attackers to conduct complex attacks such as those conducted against Ukraine's power grid.[68] Some suspect it will not be long before humans step out of the loop and AIs battle other AIs directly. When this happens, organizations that rely on traditional perimeter defence systems to protect themselves will be dangerously exposed. As Darktrace's David Masson put it,

> When we see the first AI attack – we, as a company, think it might be this year; we've been seeing hints of it for quite a few years, but it could be later on – many of the current techniques and systems that are used for protecting networks from cyber threats will become redundant overnight. That will happen very, very quickly.[69]

All of this is concerning to the Committee and certainly highlights the limits of relying on user awareness to defend organizations from AI-enabled cyber attacks.

Recommendation 3

The Committee recommends that the Government of Canada recognize both the promise and the peril of artificial intelligence for cybersecurity, ensuring that this duality is addressed in its national cybersecurity framework.

B. A Practical Quantum Computer

Like AI, progress in quantum research will both advance and threaten cybersecurity. For example, breakthroughs in using quantum effects to communicate information over long distances could spell the end of surreptitious eavesdropping on networks. There is also hope that one day soon a quantum computer will emerge that is more powerful than a classical computer and stable enough to be applied to a broader range of computational tasks. A quantum computer that has these qualities is often referred to as

67 See, for example, Zurich-based DeepCode's AI-enabled code analysis tool, www.deepcode.ai.

68 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (David Masson, Director, Enterprise Security, Darktrace), 42nd Parliament, 1st Session, 18 March 2019.

69 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (David Masson, Director, Enterprise Security, Darktrace), 42nd Parliament, 1st Session, 18 March 2019.

a “practical quantum computer.” Among other things, a practical quantum computer could be used to “super-charge” AI, thereby improving software security analysis.

However, such a computer would also easily solve the hard math problems that form the basis of public key cryptography.[70] Michele Mosca, a professor of mathematics and cryptography at the University of Waterloo and director of the non-profit organization, Quantum-Safe Canada, told the Committee he anticipates a practical quantum computer will be built in the next 8-15 years. He described what will happen if we fail to prepare for this event as follows:

> [F]irst, a direct attack on the financial services sector – money stolen, legitimate activities impeded, loss of confidence in the Canadian financial sector; second, cyber-attacks on other sectors driving our economy, where much of our money is invested – most importantly, critical infrastructure such as government services, power and other utilities, transportation systems and smart cities; third, theft of strategic intellectual property that is protected by quantum-vulnerable cryptography; and fourth, disruption of Canadian jobs, today's and tomorrow's, that produce or rely on technologies that are not resilient to quantum attacks and don't have a plan to become quantum-safe.[71]

As such, a quantum computer represents an existential threat to the financial sector, which relies on public key infrastructure[72] to function securely. As Mr. Jonathan Reiber put it, quantum computing will “totally alter the nature of cybersecurity.”[73]

Even assuming a quantum computer appears later rather than sooner, we still need to start planning for a post-quantum world now. Witnesses noted that quantum-resistant encryption standards are now in the third year of a competitive eight-year development program initiated in 2016 by the United States National Institute of Standards and Technology.[74] Canadian researchers contributed some of the 26 proposed encryption algorithms. Once the soundness of each proposed algorithm has been thoroughly

---

70 Most public-key cryptography relies on so-called “one-way” mathematical functions, such as factoring prime numbers or that are easy to perform in one direction but computationally difficult to perform in reverse.

71 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Michele Mosca, Director, Quantum-Safe Canada), 42nd Parliament, 1st Session, 27 February 2019.

72 Public key infrastructure refers to “a cryptographic key and certificate delivery system that makes possible secure electronic transactions and exchanges of sensitive information using a system of trusted third parties called "certificate authorities." Government of Canada, “Public Key Infrastructure,” *Termium Plus*.

73 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Jonathan Reiber, Head, Cybersecurity Strategy, Illumio), 42nd Parliament, 1st Session, 6 February 2019.

74 To read further, wee National Institute of Standards and Technology, *Post-Quantum Cryptography*.

evaluated, witnesses said, international adoption of whatever standards emerge from this process can be expected to take a decade or more to achieve.

In the meanwhile, enabling infrastructures such as a quantum key distribution (QKD) system[75] need to be built. As it turns out, Canada invented QKD and has an opportunity to show the world how to build a tamper-proof system that can provide secure communications throughout the vast territory of this nation.[76] At present, in Calgary, Ottawa, Waterloo, and Quebec, there are QKD collaboration centres running on separate fibre optic networks and in various stages of planning and development.[77] Quantum-Safe Canada hopes to link the networks of these collaborating centres via satellite to enable a national-level QKD system that would, in turn, join a global network.[78] It believes that, for purposes of testing satellite communications between these collaborating Canadian research centres, there is a "clear need" for Canada to integrate QKD into these centres' existing network infrastructures in the next three to five years.[79]

Canada faces sharp competition in this field. For example, China has expressed a desire to become a quantum superpower by 2030 and is hard at work on establishing its own national-level QKD system, starting with the 2000-km Quantum Beijing-Shanghai Trunk line.[80] China also recently achieved success in key distribution at intercontinental distances using its Micius satellite.[81]

---

75 Quantum Key Distribution refers to the use of quantum effects to establish key agreement between parties to a secure communication.

76 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Michele Mosca, Director, Quantum-Safe Canada), 42nd Parliament, 1st Session, 27 February 2019.

77 Dr Michele Mosca, Brian O'Higgins, and Bill Munson, Quantum-Safe Canada, *The Quantum Threat to Cyber Security: Danger and Opportunity Submitted in support of a presentation to the Standing Committee on Public Safety and National Security regarding Cybersecurity in the Financial Sector as a National Economic Security Issue*, 22 February 2019, p. 3.

78 Dr Michele Mosca, Brian O'Higgins, and Bill Munson, Quantum-Safe Canada, *The Quantum Threat to Cyber Security: Danger and Opportunity Submitted in support of a presentation to the Standing Committee on Public Safety and National Security regarding Cybersecurity in the Financial Sector as a National Economic Security Issue*, 22 February 2019, p. 3.

79 Dr Michele Mosca, Brian O'Higgins, and Bill Munson, Quantum-Safe Canada, *The Quantum Threat to Cyber Security: Danger and Opportunity Submitted in support of a presentation to the Standing Committee on Public Safety and National Security regarding Cybersecurity in the Financial Sector as a National Economic Security Issue*, 22 February 2019, p. 3.

80 John Costello, *Chinese Efforts in Quantum Information Science: Drivers, Milestones, and Strategic Implications*, Testimony for the U.S.-China Economic and Security Review Committee, 16 March 2017, pp. 13-14.

81 "Chinese satellite uses quantum cryptography for secure videoconference between continents," *MIT Technology Review*, 30 January 2018.

Decisions will also have to be made at both national and international levels regarding the prioritization of systems to be transitioned to the quantum-resistant encryption standard. Because, as Professor Mosca notes, it depends so heavily on public key encryption, the Internet will be among those infrastructures that will need to be prioritized. During this incremental transition, quantum-resistant schemes will need to function alongside current cryptographic standards. Implementing this parallel operational structure correctly could be challenging from a cybersecurity perspective.

Witnesses urged the government to overcome this urge and begin planning now to avoid future chaos. Professor Mosca offered the following warning about the potential consequences of delay:

> [I]f managed reactively, if we choose to do that … we'll be susceptible to quantum attacks. We'll also be susceptible to mundane attacks, the everyday attacks we see today that simply exploit the mistakes intrinsic in a rushed crisis response…. That's what will happen if we manage this reactively. Not responding proactively means that new opportunities that we've invested in over decades will be lost, and much of our existing economy will be at risk.[82]

Canadian public and private sector organizations need to grasp this nettle early on to successfully transition their infrastructures and data holdings to quantum-safe encryption.

In fact, Mr. Brian O'Higgins – the founder of Canadian encryption provider, Entrust, and chair of Quantum-Safe Canada – said great opportunity accompanies the quantum challenge. Canada has long had an excellent reputation for its cryptography skills, he said, adding that:

> We're still riding off that kind of aura that Canadians are good in encryption technology. There's an opportunity now with quantum resistance. Encryption has to change wholesale around the world. It has to be resistant to a quantum attack. Guess what? Canadian quantum technology from the University of Waterloo and other places is world-leading. There's a good opportunity to repeat that kind of effect.[83]

Finally, preparing Canada to compete in a post-quantum world will demand a workforce whose skillset is even rarer than that required for generalized cybersecurity activities, witnesses said. Because it has made decades of investment in quantum science and cryptography, they said, Canada is lucky enough to possess a small core of world-beating

---

82 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Michele Mosca, Director, Quantum-Safe Canada), 42nd Parliament, 1st Session, 27 February 2019.

83 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Brian O'Higgins, Chair, Quantum-Safe Canada), 42nd Parliament, 1st Session, 27 February 2019.

talent. With the right support, this core could help build the quantum-capable workforce Canada needs going forward.

Recommendation 4

The Committee recommends that the Government of Canada increase this country's existing quantum skills capacity and continue to support research and development of quantum technologies and encryption standards that will ensure Canada's electronic information and information systems remain secure in a post-quantum world.

CHAPTER 5—ADDRESSING THE CYBERSECURITY SKILLS SHORTFALL

Cybersecurity expertise is in high demand. Countries around the world are vying to attract and retain individuals with appropriate training and skills in this area and Canada is no exception. In fact, our banks have been making heavy investments in hack-a-thons, post-secondary research programs, and other activities aimed at identifying and nurturing Canadian cybersecurity talent. According to the Canadian Bankers Association (CBA),

> [CBA] members have funded cybersecurity labs at the University of Waterloo. Members have invested internationally, including in Ben-Gurion University in Israel, which is a globally renowned cybersecurity hub. Another member has a strategic alliance with the Israeli bank, Leumi, and the National Australia Bank to collaborate in areas of digital banking, financial technology and cybersecurity.[84]

The Committee invited the input of witnesses who are familiar with the cybersecurity workforce building efforts of Australia and Israel. Their observations are included in the following two sections.

A. Australia

The Committee was interested in hearing about Australia's approach, so it invited Professor Slay to discuss her perspective on cybersecurity education. She said her government is trying to instil cybersecurity awareness early on in young people, explaining that in Australia:

84 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Charles Docherty, Assistant General Counsel, Canadian Bankers Association), 42nd Parliament, 1st Session, 18 March 2019. See also, Royal Bank of Canada, "Royal Bank of Canada and Ben-Gurion University Enter into Cyber Security Partnership," News Release, 26 June 2018.

> 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.[85]

Changes are also underway regarding Australia's post-secondary framework of study for cybersecurity. Professor Slay said her country's professional association for the information, communications and technology (ICT) sector, the Australian Computer Society, has a national ICT curriculum which it is now updating to be more cross-disciplinary in nature. Specifically, she stated that:

> [W]e 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.[86]

B. Israel

Israel's cybersecurity eco-system was referenced many times by witnesses who appeared before the Committee. For example, Glenn Foster, Chief Information Security Officer of the Toronto Dominion Bank said it looks to Israel to recruit cybersecurity talent.[87] Cybersecure Catalyst, a recently established non-profit organization based in Brampton, Ontario, offered the following illustration of just how dependent on Israel Canadian financial institutions have become:

> An interesting way to see the Canadian labour market problem in cybersecurity is to travel to Israel. Israel is generally acknowledged to have the strongest cybersecurity technology ecosystem in the world. The Israeli government has established a new major centre for cybersecurity activities in a small town in the Negev Desert about an hour by car from Tel Aviv, called Beersheba. In January, I travelled Beersheba to meet not with Israeli companies but with representatives of Canadian financial institutions that have

85 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Jill Slay, Professor, La Trobe Optus Chair of Cyber Security, La Trobe University, Melbourne), 42nd Parliament, 1st Session, 20 February 2019.

86 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Jill Slay, Professor, La Trobe Optus Chair of Cyber Security, La Trobe University, Melbourne), 42nd Parliament, 1st Session, 20 February 2019.

87 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Glenn Foster, Chief Information Security Officer, Toronto Dominion Bank), 42nd Parliament, 1st Session, 3 April 2019.

> established offices at Beersheba because they can find cybersecurity talent in Israel much more readily than they can in Canada.[88]

Israel starts teaching its children good cyber hygiene – measures they can undertake to protect themselves from cybersecurity risks – much earlier than Australia. According to Professor Shavitt, a professor at Tel Aviv University's School of Electrical Engineering,

> 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 … It seems to work.[89]

As to teaching cyber skills, Israel also starts early, said Mr. Yuval, who explained that:

> 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.[90]

C. Canada

In September 2018, Ryerson University announced plans to launch of a Brampton-based, not-for-profit centre called Cybersecure Catalyst. This new centre will pursue training and certification, research and development, commercial incubation, public awareness; and policy-related work.[91] The Committee invited Cybersecure Catalyst's executive director, Mr. Charles Finlay, to discuss the centre's role in building Canada's cybersecurity workforce.

Mr. Finlay said that, when it was planning its course offerings, Cybersecure Catalyst sought financial sector input and was told this sector faces a multi-level skills shortage. He described what he heard as follows:

> When we asked major financial institutions and other private sector entities what they needed most from a university-based cybersecurity centre, the answer wasn't some specific technological tool or identified advance in the science. The overwhelming

88 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Charles Finlay, Executive Director, Cybersecure Catalyst), 42nd Parliament, 1st Session, 1 April 2019.

89 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Yuval Shavitt, Professor, Tel Aviv University), 42nd Parliament, 1st Session, 20 February 2019.

90 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Yuval Shavitt, Professor, Tel Aviv University), 42nd Parliament, 1st Session, 20 February 2019.

91 Will Sloan, "University launches cybersecurity centre" (reprint from *Ryerson Today*), Ryerson University, Research News, 6 September 2018.

> answer was more people.… In particular, we heard from financial institutions that they need their existing personnel to be upskilled to meet emerging threats, and they need more people to come into the sector to staff entry-level positions within their organizations. Every one of the major financial institutions in Canada has many current openings for cybersecurity personnel.[92]

Mr. Finlay went on to cite a July 2018 report by the Toronto Financial Services Alliance and Deloitte, which indicated Canada would have 8,000 empty cybersecurity positions to fill by 2021.[93] He commended the government's 2019 federal budget allocation of $80 million to post-secondary educational institutions for cybersecurity courses but said much more needs to be done. Urging the government to reach out to those in Canadian society who are currently underrepresented in cybersecurity, Mr. Finlay said:

> We will not solve the labour market issue of cybersecurity for financial institutions or for any other institutions if we don't open the cybersecurity sector to more women, racialized groups, new Canadians, indigenous Canadians, veterans and to those who have been displaced from legacy sectors.[94]

The Committee agrees that Canada cannot afford to overlook any source of cyber talent. It also supports Cybersecurity Catalyst's efforts to tailor its offerings to meet a wide range of needs. Mr. Finlay confirmed to the Committee that Cybersecurity Catalyst is working with the United States' well-respected SANS Institute. SANS, the Committee notes, maps its own course offerings to the U.S. National Institute of Standards and Technology's (NIST) National Initiative of Cybersecurity Education (NICE) Framework. NIST's NICE Framework "establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed."[95] Anything that helps an employer correctly identify their skills shortfalls or assess the qualifications of a prospective employee is to be welcomed.

The Province of New Brunswick's efforts to transform itself into a cybersecurity education hub also received favourable commentary from witnesses, who said major companies are "snapping up"[96] students graduating from CyberNB's high school

---

92 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Charles Finlay, Executive Director, Cybersecure Catalyst), 42nd Parliament, 1st Session, 1 April 2019.

93 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Charles Finlay, Executive Director, Cybersecure Catalyst), 42nd Parliament, 1st Session, 1 April 2019.

94 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Charles Finlay, Executive Director, Cybersecure Catalyst), 42nd Parliament, 1st Session, 1 April 2019.

95 National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework*.

96 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (David Masson, Director, Enterprise Security, Darktrace), 42nd Parliament, 1st Session, 18 March 2019.

cybersecurity programs. Facing stiff competition for cybersecurity talent, Toronto Dominion Bank said it is also forging partnerships with academic institutions that offer courses in this field, including the University of New Brunswick.[97]

Asked how the Canadian Centre for Cyber Security is helping to address Canada's skills shortage, Scott Jones said his organization had done some mentoring work and sponsored events like Hackergal to encourage girls to code. However, he went on to suggest that the sheer size of Canada creates challenges and that the Centre's educational outreach program "doesn't necessarily scale easily."[98]

There is recognition that any strategy to build a cybersecurity workforce would be incomplete without a plan to encourage the acquisition of coding and digital skills early on in our children's education. To the extent that it can, given provincial and territorial jurisdiction over educational curricula, the federal government has tried to contribute to this objective.

Innovation, Science and Economic Development Canada's CanCode program[99] is one example of federal-level support for youth cyber skills acquisition. CanCode funds not-for-profit organizations to deliver digital education programs to youth and their educators throughout Canada. To date, the program has reached 1.3 million students and 61,000 teachers,[100] teaching coding and digital skills such as data analytics. CanCode's asset assessment criteria favour organizations that have a demonstrated ability to reach traditionally underrepresented groups, including girls, Indigenous youth and youth with disabilities.[101] The Committee supports this emphasis on reaching underrepresented populations and across Canada.

Missing from CanCode's assessment criteria, however, is any mention of cyber hygiene and ethical software coding practices as part of the skillsets to be passed on to students and teachers. The Committee views this as an oversight that can and should be remedied.

---

97 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Glenn Foster, Chief Information Security Officer, Toronto Dominion Bank), 42nd Parliament, 1st Session, 3 April 2019.

98 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Jones, Head, Canadian Centre for Cyber Security, Communications Security Establishment), 42nd Parliament, 1st Session, 30 January 2019.

99 Innovation, Science and Economic Development Canada, *CanCode*.

100 Innovation, Science and Economic Development Canada, *CanCode*.

101 Industry, Science and Economic Development Canada, *CanCode assessment criteria*.

Recommendation 5

The Committee recommends that the Government of Canada develop a comprehensive cybersecurity skills and training strategy that will instil ethical and secure coding practices early on and create a cybersecurity workforce that leverages diverse backgrounds, meets internationally recognized standards, and is prepared for the cybersecurity challenges of today and tomorrow.

CHAPTER 6—INCIDENT REPORTING

Based on witness comments, it appears that Canada lacks key data to measure the state of its cybersecurity accurately. The best available statistics appear to be those compiled by Statistics Canada in a survey of Canadian businesses conducted in 2017.[102]

According to Mr. Chris Lynam, the RCMP's Acting Director General for the National Cybercrime Coordination unit, the Statistics Canada survey demonstrates that, even with improvements over the past few years, under-reporting of cybercrime remains an issue. He said:

> The 2017 Canadian survey of cybersecurity and cybercrime undertaken by Statistics Canada found that about 10% of businesses impacted by a cybersecurity incident reported the incident to a police service in 2017. Despite under-reporting, the number of cybercrimes reported to police in Canada has increased in recent years. In 2017, nearly 28,000 cybercrimes were reported to Canadian police, which is an 83% increase compared to 2014.[103]

Given the role of prosecution in deterring criminality, the Committee was somewhat taken aback to hear that the police would be quickly overwhelmed should reporting of all cybercrime be made mandatory.[104]

The fact that the sources of many of these criminal activities are scattered across multiple jurisdictions in Canada or in foreign jurisdictions, where the RCMP may or may not have recourse to mutual legal assistance agreements, further complicates criminal

---

102 See Howard Bilodeau, Mohammad Lari and Mark Uhrbach, *Cyber security and cybercrime challenges of Canadian businesses, 2017*, Statistics Canada, 28 March 2019.

103 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chris Lynam, Acting Director General, National Cybercrime Coordination, Royal Canadian Mounted Police), 42nd Parliament, 1st Session, 28 January 2019.

104 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chief Superintendent Mark Flynn, Director General, Financial Crime and Cybercrime, Federal Policing Criminal Operations, Royal Canadian Mounted Police), 42nd Parliament, 1st Session, 28 January 2019.

investigation and prosecution efforts. Though the RCMP and other police forces in Canada have not given up on prosecution, Chief Superintendent Flynn said, "we feel it's more important to reduce the victimization and reduce the losses as soon as we can."[105]

Asked how the RCMP's new National Cybercrime Coordination unit will improve the situation, the Committee was told that the new unit would provide a focal point to encourage cybercrime reporting and it would facilitate coordination of cybercrime investigations to ensure efficient use of existing police resources. Mr. Lynam said the unit will help municipal and provincial police forces perform better in this area, not only by increasing information sharing among stakeholders but also by using AI to assess public incident reporting. In respect of the latter, he explained that,

> [B]y having a very robust and modern public reporting system that has strong analytics behind it, we could very quickly understand that perhaps 10 other people in Canada have been victimized by that same person or that same cyber entity, moniker or email address. Because of that level of impact—we can see that at a national level—we can then work with other police services across Canada to go after that cybercriminal. Right now that doesn't exist.[106]

The Committee's sense of the matter is that, while increased information sharing and coordination will be vital to cybersecurity because it helps police and national security agencies detect when a small event is part of a larger cyber threat campaign and work together more efficiently, the international nature and sheer volume of cyber criminality means prosecution will still not always be possible. Nonetheless, the Committee is concerned that, according to Chief Superintendent Flynn, only a "small fractional per cent" of cybercrime perpetrated against Canadians leads to charges being laid.[107]

Recommendation 6

To ensure accurate and comprehensive statistics, the Committee recommends that the Government of Canada encourage Canadian citizens and companies to report all instances of cybercrime.

---

105 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chief Superintendent Mark Flynn, Director General, Financial Crime and Cybercrime, Federal Policing Criminal Operations, Royal Canadian Mounted Police), 42nd Parliament, 1st Session, 28 January 2019.

106 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chris Lynam, Acting Director General, National Cybercrime Coordination, Royal Canadian Mounted Police), 42nd Parliament, 1st Session, 28 January 2019.

107 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chief Superintendent Mark Flynn, Director General, Financial Crime and Cybercrime, Federal Policing Criminal Operations, Royal Canadian Mounted Police), 42nd Parliament, 1st Session, 28 January 2019.

A. Privacy Breach Reporting

The Office of the Privacy Commissioner of Canada (OPC) believes mandatory privacy breach reporting has already begun to generate cybersecurity benefits. Mandatory reporting of material breaches of personal information[108] by private sector organizations came into effect on 1 November 2018. According to the OPC, this requirement is already beginning to provide a sense of the character and magnitude of Canada's cybersecurity issues. Gregory Smolynec, Deputy Commissioner of Policy and Promotion for the OPC, said that, since reporting became mandatory, the OPC has seen a fourfold increase in breach reports from the private sector.[109]

Six months in, said Mr. Smolynec, certain things have become clear about the nature of private sector cybersecurity practices. "Institutions are not always aware of the personal information they hold, where it goes or who has access to it," he said, adding that insider threats are too often overlooked in organizational cybersecurity practices. On this latter issue, he noted that,

> Oftentimes in the rush to protect against hackers, the internal threat is overlooked, yet privacy breaches involve not only loss of personal information to external forces, but also inappropriate access by internal actors. Mandatory breach reporting requirements can be a tool to enable institutions to confront the adequacy, or lack thereof, of cybersecurity plans and preparations.[110]

Technological innovations, such as open banking,[111] also have the OPC's attention, said Mr. Smolynec. "We have the potential for open banking internationally, and coming to Canada, too, which will change business models and the way personal information and data flow among financial institutions," he said. Describing these changes as

---

108 Under section 10.1 of the *Personal Data Protection and Electronic Documents Act*, any breach of personal information must be reported if it poses a real risk of significant harm to individuals.

109 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Gregory Smolynec, Deputy Commissioner, Policy and Promotion Sector, Office of the Privacy Commissioner of Canada), 42nd Parliament, 1st Session, 3 April 2019.

110 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Gregory Smolynec, Deputy Commissioner, Policy and Promotion Sector, Office of the Privacy Commissioner of Canada), 42nd Parliament, 1st Session, 3 April 2019.

111 The Advisory Committee on Open Banking, which was struck by the Department of Finance on 26 September 2018, defines open banking as "a framework where consumers and businesses can authorize third-party financial service providers to access their financial transaction data using secure online channels." See Department of Finance, *A Review into the Merits of Open Banking: Consultation Document*, January 2019.

"extraordinarily consequential" for privacy rights, Mr. Smolynec called for the adaption of Canada's standards, regulations and laws prior to implementation.[112]

With respect to the pace at which change is being introduced, the Committee would like to underscore the importance of consultation with all stakeholders. In this connection, the Committee notes that the President of the Canadian Association of Mutual Insurance Companies, Mr. Norman Lafrenière, indicated that his organization had been "encouraged not to talk to MPs" about its concerns regarding open banking.[113]

The OPC also seeks more fundamental changes to Canada's privacy laws. Along with order-making powers along the lines of those held by the OPC's British counterpart, the Information Commissioner's Office, Mr. Smolynec argued for a "rights-based approach." He explained the latter element as follows:

> Currently, I would say that our private sector law is principles-based and, in a sense, very broad. It, in passing, refers to the privacy rights of Canadians, but a rights basis would recognize, as Canada does, that privacy is an internationally recognized human right in the context of a human right, that there are also procedural rights associated with it, and that this would be applied broadly across both public and private sectors. Canadians should be informed of their rights and how to exercise those rights. It's both a legislative challenge with an associated public education challenge.[114]

CHAPTER 7—TOWARDS BETTER CYBERSECURITY

A. Vulnerabilities Disclosure

It is extremely difficult, if not impossible, to eliminate all flaws in software, firmware and hardware. Certainly, more can be done to ensure basic flaws such as default administrator passwords are eliminated. But the fact remains that our digital environment contains poorly secured legacy systems, with more being added every

112 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Gregory Smolynec, Deputy Commissioner, Policy and Promotion Sector, Office of the Privacy Commissioner of Canada), 42nd Parliament, 1st Session, 3 April 2019.

113 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Normand Lafrenière, President, Canadian Association of Mutual Insurance Companies), 42nd Parliament, 1st Session, 27 February 2019.

114 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Gregory Smolynec, Deputy Commissioner, Policy and Promotion Sector, Office of the Privacy Commissioner of Canada), 42nd Parliament, 1st Session, 3 April 2019.

day.[115] As Mr. Jobert Abma the founder of HackerOne, a "hacker-powered security testing" consultancy explained,

> The Internet is a very complex system with a lot of people contributing to it. Everything is tied together. Systems and networks change or contain hundreds of thousands of individual hardware and software components and thousands of lines of code. Every time code is updated, which may happen multiple times a day, new vulnerabilities may be introduced.[116]

HackerOne organizes "bug bounty" programs, in which client organizations invite so-called "white hat hackers" to find and fix vulnerabilities on their systems. A "white hat hacker" is someone who is very good at finding flaws in cyber defences but wants to use these discoveries to prevent a cyber attack. Bug bounties offer a means to reward "white hat hackers" for their help and to encourage them to continue disclosing the results of their research responsibly.

In this model, there is power in numbers. According to HackerOne's Vice-President of Policy, Ms. Deborah Chang, HackerOne has more than 300,000 registered white hat hackers and counts the United States Department of Defense among its clientele.[117] Ms. Chang went on to say that:

> Thanks to the diversity and scale of the hacker community, hacker-powered security finds vulnerabilities that automated scanners or permanent penetration testing teams do not. Existing models are good at finding predictable security vulnerabilities, but even more important is to find the unpredictable ones: the unknown unknowns. Given a large enough hacker community and enough time, such vulnerabilities will be identified.[118]

PayPal, a client of HackerOne in the United States, told the Committee that companies can place specific bounds on what they will treat as responsible disclosure. Brian Johnson, Senior Director of Information Security for PayPal, described his company's policy as follows:

---

115 See, for example, reference to the risks posed by unpatched legacy systems in House of Commons Standing Committee on Public Safety and National Security, *Briefing: Defend Forward and Assume Breach: Preparing Canada for a cyberresilient future* (Jonathan Reiber, Head of Cybersecurity Strategy, Illumio), 42nd Parliament, 1st Session, 10 April 2019, p. 3.

116 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Jobert Abma, Founder, HackerOne), 42nd Parliament, 1st Session, 4 February 2019.

117 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Deborah Chang, Vice-President, Policy, HackerOne), 42nd Parliament, 1st Session, 4 February 2019.

118 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Deborah Chang, Vice-President, Policy, HackerOne), 42nd Parliament, 1st Session, 4 February 2019.

> If there's a system breach, that's an unauthorized activity and it would be treated as malicious and illegitimate access as with any mal-intended attacker. We don't have bug bounty researchers perform attacks or breaches, and as part of the program policy, they're not allowed to access customer data nor to make any manipulation or changes of information. They're allowed to disclose vulnerabilities that are detected in the system and report those to us through the responsible disclosure program.[119]

The Committee notes that properly organized bug bounties provide a cost-effective means for organizations, including government departments, to identify and patch vulnerabilities. It is aware that some Canadian companies already have bug bounty programs in place but believes the government can do more to promote this important cybersecurity measure.

At the same time, care must be taken to ensure national security agencies and product vendors hold up their end of the bargain. Sometimes, for example, organizations may not act expeditiously on the vulnerability information that has been disclosed to them, which places the security researcher, who has agreed to withhold public disclosure of their vulnerability information, in an untenable position.[120]

Chris Parsons, a research associate at the Munk School of Global Affairs's Citizen Lab, noted that, despite having important cybersecurity responsibilities, CSE has incentive not to publicly disclose information on vulnerabilities.[121] Sometimes, he said, CSE chooses to hide what it knows so that it can continue to use these vulnerabilities to pursue its offensive mission, foreign intelligence collection. To decide when to disclose or to favour its offensive mission, CSE follows a "vulnerabilities equities process."[122] While Mr. Scott Jones assured the Committee that CSE will always "default to

---

119 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Brian Johnson, Senior Director, Information Security, PayPal Inc.), 42nd Parliament, 1st Session, 29 May 2019.

120 Time frames for remediation are usually built into responsible disclosure agreements. See, Standing Committee on Public Safety and National Security, *Cybersecurity in the Financial Sector as a National Economic Security Issue*, submission by Dr. Christopher Parsons, Research Associate, Citizen Lab, Munk School of Global Affairs & Public Policy at the University of Toronto, para. 18.

121 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chris Parsons, Research Associate, Monk School of Global Affairs, University of Toronto), 42nd Parliament, 1st Session, 27 February 2019.

122 Please note that the Committee has chosen to use the term "vulnerabilities equities process" because this reflects the usage of close allies. See, for example, Whitehouse, *Vulnerabilities Equities Policy and Process for the United States Government*, 15 November 2017; and Ian Levy, *Equities process*, (blog) National Cyber Security Centre.

defence"[123] in its decision-making process, Mr. Parsons highlighted the fact, unlike some of our allies, that CSE's process is entirely opaque. He offered the following recommendation:

> To alleviate these concerns, we would suggest that the Canadian government publicize its existing vulnerabilities equities programs and hold consultations on their effectiveness in protecting the software and hardware that is used in the course of financial activities. Furthermore, the government could include the business community and civil society stakeholders in the existing, or reformed, vulnerabilities equities programs. Including these stakeholders would encourage heightened disclosures of vulnerabilities and thus improve the availability of well-written software and reduce threats faced by the financial sector.[124]

Some of our allies, such as the United States, have already gone public with their vulnerabilities equities processes,[125] which suggests that it might be time for consider increased transparency on this subject in Canada.

Recommendation 7

The Committee recommends that the Government of Canada support responsible vulnerability disclosure programs.

B. Strong Encryption Today and Tomorrow

That more needs to be done to ensure security is "baked" into the devices we use and not treated as a pricey add-on feature was a recurrent theme throughout the Committee's hearings. Borrowing from former Ontario Information and Privacy Commissioner, Ann Cavoukian's "privacy by design" concept, witnesses called for adoption of a "security by design" philosophy.[126]

123 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Jones, Deputy Chief, Information Technology Security, Communications Security Establishment), 42nd Parliament, 1st Session, 20 September 2018.

124 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chris Parsons, Research Associate, Monk School of Global Affairs, University of Toronto), 42nd Parliament, 1st Session, 27 February 2019.

125 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chris Parsons, Research Associate, Monk School of Global Affairs, University of Toronto), 42nd Parliament, 1st Session, 27 February 2019.

126 See, for example, House of Commons Standing Committee on Public Safety and National Security, *Evidence* (David Masson, Director, Enterprise Security, Darktrace), 42nd Parliament, 1st Session, 18 March 2019.

Accepting that cybersecurity starts with sound security engineering practices, then, the Committee finds it concerning that national security and law enforcement agencies around the world continue to discuss weakening encryption schemes to enable lawful access, particularly given the acute dependence of the financial sector on this key cybersecurity technology.

This push for lawful access through weakened encryption does not accord with evidence the Committee received about national security agencies' preoccupation with the quantum computing threat. Though Payments Canada's Chief Information Security Officer declined to provide details, he did confirm that CSE has been engaging his organization on the security challenges presented by quantum computing.[127] If CSE is concerned about the threat that quantum computing might pose to public key encryption in the future, then surely it needs to be equally concerned about any threat posed to the integrity of encryption today?

Lawful access appears to some as officially sanctioned "weakness by design." This thinking was reflected in one witness's call to reject lawful access legislation in favour of ensuring public access to "strong encryption." In making his case for "responsible encryption policy," Chris Parsons, defined strong encryption as follows:

> Strong encryption can be loosely defined as encryption algorithms for which no weaknesses or vulnerabilities are known or have been injected, as well as computer applications that do not deliberately contain weaknesses designed to undermine the effectiveness of the aforementioned algorithms.[128]

The Committee agrees that it is important, for reasons of security and privacy, that every Canadian have access to strong encryption. At the same time, it recognizes that this will create challenges, particularly for non-federal law enforcement agencies that, unlike the RCMP, cannot call on CSE for technical and operational support.

Recommendation 8

The Committee recommends that the Government of Canada reject approaches to lawful access that would weaken cybersecurity.

---

127 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Martin Kyle, Chief Information Security Officer, Payments Canada), 42nd Parliament, 1st Session, 8 April 2019.

128 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Chris Parsons, Research Associate, Monk School of Global Affairs, University of Toronto), 42nd Parliament, 1st Session, 27 February 2019.

C. Helping Small and Medium Enterprises Get Cybersecure

When it comes to the economic role of its SMEs, Australia mirrors Canada. According to Professor Slay, Australia has an economic dependence on SMEs roughly comparable to that of Canada. Also like Canada, Australian SMEs often need to outsource key aspects of their operations, including cybersecurity. However, according to Professor Slay, the latter element may not be included in the outsourcing arrangements negotiated by Australian companies. Professor Slay said Australian SMEs may rely on managed service providers for their general information technology and communications needs, but "there's a lack of understanding of even the need for cybersecurity as a service."[129]

To address this gap, Professor Slay said her government's Department of Industry has established the Australian Cyber Security Growth Network. She described this initiative as a means for Australia to develop its cybersecurity industry by funding small businesses that develop niche products, hardware and software.

Digging a little further, the Committee discovered that it features "GovPitch" events, which provide small businesses an opportunity to deliver a short pitch on their product to government agency heads, chief information officers and chief information security officers.[130] The idea is to not only help SMEs with innovative cybersecurity products land government contracts but also to alert government to products they had no idea existed.

That line of thinking sounds similar to that espoused by CSE about its Canadian Centre for Cyber Security. Just prior to becoming the head of the Centre, Mr. Scott Jones shared his hope with the Committee that the Centre would "foster innovation" by acting as a kind of "matchmaker" between companies with a cybersecurity problem for which another company has a good solution.[131] He went on to describe how the Centre was designed to encourage private-public sector partnership, stating that:

> [W]e're making sure that we have a facility where people can come in and work. If you come and visit CSE now, we take all of your technology away because you're entering a top-secret building. The cyber centre will not be that way. The physical facility for this

129 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Jill Slay, Professor, La Trobe Optus Chair of Cyber Security, La Trobe University, Melbourne), 42nd Parliament, 1st Session, 20 February 2019.

130 Australian Cyber Security Growth Network, *GovPitch*.

131 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Jones, Deputy Chief, Information Technology Security, Communications Security Establishment), 42nd Parliament, 1st Session, 20 September 2018.

> will be a place where people can come and collaborate and, frankly, bring their stuff so we can see how it works and we can work together on things.[132]

Like Australia, Canada not only needs to improve the cybersecurity skills and practices of its SMEs, it needs to ensure SMEs have access to the best cybersecurity tools.

As the Committee learned from witnesses, this country has been and continues to be an innovator in key cybersecurity technologies such as encryption, artificial intelligence and quantum computing. The birthplace of these Canadian innovations is often a start-up or a spin-off from an academic research project. The Committee believes Canada should make every effort to ensure these small businesses stay here and grow to their full potential.

Rather than allowing others to run with our ideas, Canada needs to do more to support homegrown cybersecurity innovation. If CSE's Cyber Centre can contribute to this objective, that is a good thing. Better yet, is to support innovation by putting it to work. To that end, the Committee urges the government to emulate Australia's "pitch-friendly" approach and open up its procurement process to the cybersecurity solutions and services offered by Canadian start-ups.

CHAPTER 8—DATA SOVEREIGNTY

"Will even the best ally keep the interests of its friends in the fore, when its own critical infrastructure is threatened?" This was the question Andrew Clement, Professor Emeritus at the University of Toronto's Faculty of Information posed about the United States to the Committee.

Professor Clement heads up a research team that developed a web-based Internet Exchange Point[133] mapping tool called "IX-Map," which enables Canadians to see where their data goes when they access websites. He provided some statistics to the Committee that strongly suggest Canada currently has little control over its part of the Internet. According to Professor Clement "approximately 80% of Canadian internet communications with countries other than the U.S. pass physically through the U.S."[134]

---

132 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Scott Jones, Deputy Chief, Information Technology Security, Communications Security Establishment), 42nd Parliament, 1st Session, 20 September 2018.

133 According to the Canadian Internet Registration Authority (CIRA), "An IXP (Internet Exchange Point) is a hub where independent networks can interconnect directly to one another, providing high-bandwidth and low-latency access at a lower cost than traditional transit." See, CIRA, *Canada's Internet Infrastructure: Made-in-Canada Internet Exchange Points (IXPs)*.

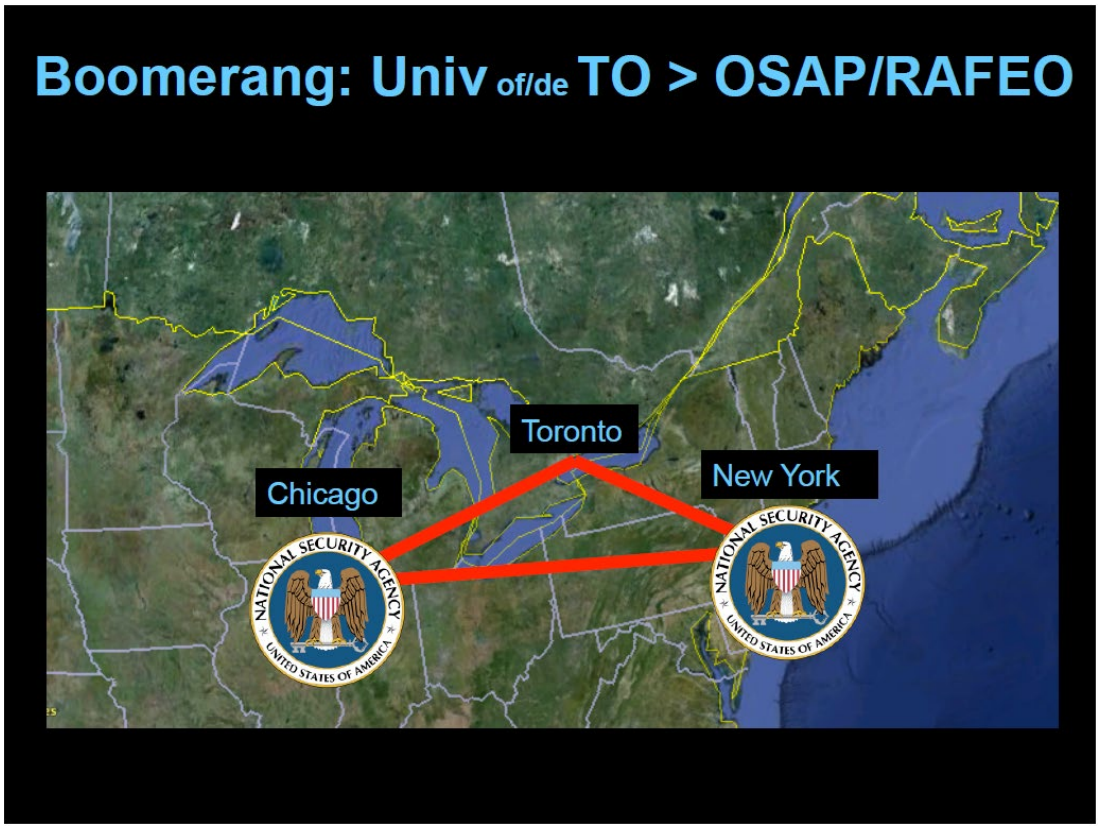
134 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Andrew Clement, Professor emeritus, Faculty of Information, University of Toronto), 42nd Parliament, 1st Session, 18 March 2019.

At least one quarter of Internet communications between persons located in Canada end up being routed through the United States, he said. Referring to this as "boomerang routing," Professor Clement explained how his group first discovered this phenomenon, stating that:

> Early in our research we generated a trace route, … which shows the data path between my office at the University of Toronto and the website of the Ontario student assistance program that is hosted in the provincial government complex a short walk away.
>
> This route surprised us, especially since the route to and from the U.S. went through the same building in Toronto, Canada's largest Internet exchange, at 151 Front Street. At the very least it challenged presumptions of maximal efficiency of Internet routing, prompting our further investigations into how widespread this phenomenon was as well as into the reasons for this counterintuitive behaviour.… It turns out to be quite common. We estimate at least 25% of Canadian domestic traffic boomerangs to the U.S. The Canadian Internet Registration Authority, CIRA, recently put the figure much higher.[135]

135 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Andrew Clement, Professor emeritus, Faculty of Information, University of Toronto), 42nd Parliament, 1st Session, 18 March 2019.

Figure 1: Boomerang Routing Map:
Sending an Email Across the Street in Toronto Via the United States



As the witness describes above, the image shows a map of Canada and the United States overlaid by a triangle that has Toronto at the apex and New York and Chicago at the two base angles. Crests of the United States National Security Agency are shown at the two base angles. The image demonstrates how, once it leaves Canadian territory, Canada can lose legal jurisdiction over its data.

Source: Image submitted by Professor Andrew Clement during his testimony.

Given Canada's lack of sovereign control over its data flows, Professor Clement asked the Committee to consider what would happen if the United States experiences a cyber attack and decides to shut down its external connections. He said,

> If, for whatever reason, our connection with the U.S. was cut, even in its own legitimate self-defence, how resilient would Canada's Internet prove to be? We should know the answer, but we don't. However, the evidence available suggests very poorly.[136]

To remedy this situation, Professor Clement made several recommendations. Among these, he recommended that "all sensitive and critical Canadian domestic data be stored, routed and processed within Canada." He also recommended that the government "support the development and use of Canada's Internet exchange points for direct inter-network data exchange to avoid U.S. routing" and promulgate cybersecurity standards requiring financial institutions and telecommunications service providers to report on their routing practices.[137]

Regarding Professor Clement's recommendation about Canada asserting data sovereignty over all sensitive and critical domestic data, it is noteworthy that the Canadian Bankers Association confirmed to the Committee that Canadian data is potentially exposed when a Canadian financial institution outsources some of its services to a company located in a foreign jurisdiction.[138] PayPal, was one of those financial sector entities that confirmed that Canadian data is stored in the United States. The same appears to be the case for Mastercard, which informed the Committee that "the majority of transactions take place at our St. Louis or Kansas City facility."[139] Mastercard's Chief Security Officer, Mr. Ron Green, went on to say the drive for data localization might hinder his efforts, saying,

> From where I sit globally I can see threat actors attempt to work against the payment system no matter where they are. But as countries localize or look for localization of data, and that data can't be used in other places, the ability for me to analyze and see where the threat actor moves becomes more difficult.[140]

By contrast, Interac Corporation's Chief Risk Officer, Terri O'Brien, said that her company keeps Canadian data firmly on Canadian soil. She stated that:

---

136 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Andrew Clement, Professor emeritus, Faculty of Information, University of Toronto), 42nd Parliament, 1st Session, 18 March 2019.

137 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Andrew Clement, Professor emeritus, Faculty of Information, University of Toronto), 42nd Parliament, 1st Session, 18 March 2019.

138 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Charles Docherty, Assistant General Counsel, Canadian Bankers Association), 42nd Parliament, 1st Session, 18 March 2019.

139 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Ron Green, Executive Vice-President, Chief Security Officer, Mastercard Canada), 42nd Parliament, 1st Session, 1 April 2019.

140 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Ron Green, Executive Vice-President, Chief Security Officer, Mastercard Canada), 42nd Parliament, 1st Session, 1 April 2019.

> We are not prepared to allow data or anything outside of our Canadian constitution and Canadian roots. Our incorporation—we became a corporation about a year ago—is quite strongly grounded in Canada. All of our data is to reside in Canada. We also use Canadian vendors and Canadian suppliers in any of the delivery of our services, but we build our own technologies.[141]

If executed thoughtfully, the Committee believes efforts to build out Canada's digital infrastructure can serve economic and national security interests concurrently. One important objective would be for Canada to enhance its connectivity with Europe and Asia, while reducing its reliance on the United States. Canada's Arctic region may offer possibilities in this regard. For instance, the Committee heard about one initiative which proposed to increase broadband connectivity in Canada's north by joining up with an international telecommunications cable located in international waters off Alaska, and to develop the James Bay region as a cloud hub.[142] Such initiatives could contribute to Canada's claims of sovereignty in the north and to its data sovereignty more generally.

Recommendation 9

The Committee recommends that the Government of Canada explore ways to ensure all sensitive data moved within Canada has a domestically routed path, ensuring data packets are not exposed to foreign network infrastructure.

CONCLUSION

Canada should ensure it pursues every opportunity to compete in the international digital economy, while maximizing its ability to enforce the privacy rights and security of its citizens in this domain. Those that rely upon the financial sector to secure their savings and to pursue their livelihoods need to know that their trust and confidence in its cybersecurity practices are well placed.

141 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Terri O'Brien, Chief Risk Officer, Interac Corporation), 42nd Parliament, 1st Session, 8 April 2019.

142 House of Commons Standing Committee on Public Safety and National Security, *Evidence* (Tawich Development Corporation), 42nd Parliament, 1st Session, 15 May 2019.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the Committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the Committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Financial Transactions and Reports Analysis Centre of Canada	2019/01/28	145
Dan Lambert, Assistant Director Intelligence Operations		
Barry MacKillop, Deputy Director Operations		
Royal Canadian Mounted Police	2019/01/28	145
Mark Flynn, Director General Financial Crime and Cybercrime, Federal Policing Criminal Operations		
Chris Lynam, Acting Director General National Cybercrime Coordination		
As an individual	2019/01/30	146
Christian Leuprecht, Professor Department of Political Science, Royal Military College of Canada		
Communications Security Establishment	2019/01/30	146
Eric Belzile, Director General Incident Management and Threat Mitigation, Canadian Centre for Cyber Security		
Scott Jones, Head Canadian Centre for Cyber Security		
Public Policy Forum	2019/01/30	146
Satyamoorthy Kabilan, Vice-President Policy		

Organizations and Individuals	Date	Meeting
As an individual	2019/02/04	147
Steve Waterhouse, Former Information Systems Security Officer Department of National Defence		
HackerOne	2019/02/04	147
Jobert Abma, Founder		
Deborah Chang, Vice-President Policy		
FireEye, Inc.	2019/02/06	148
Christopher Porter, Chief Intelligence Strategist		
Illumio	2019/02/06	148
Jonathan Reiber, Head Cybersecurity Strategy		
As an individual	2019/02/20	149
Yuval Shavitt, Professor, Tel Aviv University		
Jill Slay, Professor La Trobe Optus Chair of Cyber Security, La Trobe University, Melbourne		
Canadian Association of Mutual Insurance Companies	2019/02/27	151
Normand Lafrenière, President		
Citizen Lab	2019/02/27	151
Christopher Parsons, Research Associate Munk School of Global Affairs and Public Policy, University of Toronto		
Quantum-Safe Canada	2019/02/27	151
Michele Mosca, Director		
Brian O'Higgins, Chair		
SkyBridge Strategies	2019/02/27	151
Steve Masnyk, Principal		
As an individual	2019/03/18	152
Andrew Clement, Professor Emeritus Faculty of Information, University of Toronto		

Organizations and Individuals	Date	Meeting
Canadian Bankers Association	2019/03/18	152
Charles Docherty, Assistant General Counsel		
Andrew Ross, Director Payments and Cybersecurity		
Canadian Chamber of Commerce	2019/03/18	152
Scott Smith, Senior Director Intellectual Property and Innovation Policy		
Trevin Stratton, Chief Economist		
Darktrace	2019/03/18	152
David Masson, Director Enterprise Security		
Canadian Cyber Threat Exchange	2019/04/01	154
Robert Gordon, Executive Director		
Cybersecure Catalyst	2019/04/01	154
Charles Finlay, Executive Director		
EY	2019/04/01	154
Thomas Davies, National Financial Services Cyber Leader		
Mastercard Canada	2019/04/01	154
Ron Green, Executive Vice-President and Chief Security Officer		
Office of the Privacy Commissioner of Canada	2019/04/03	155
Leslie Fournier-Dupelle, Strategic Policy and Research Analyst		
Gregory Smolynec, Deputy Commissioner Policy and Promotion Sector		
Toronto Dominion Bank	2019/04/03	155
Glenn Foster, Chief Information Security Officer		
Interac Corp.	2019/04/08	156
Terri O'Brien, Chief Risk Officer		
Payments Canada	2019/04/08	156
Justin Ferrabee, Chief Operating Officer		
Martin Kyle, Chief Information Security Officer		

Organizations and Individuals	Date	Meeting
As an individual	2019/04/10	157
Richard B. Fadden		
ADGA Group	2019/04/10	157
Steve Drennan, Director Cybersecurity		
Amazon Web Services, Inc.	2019/04/10	157
Mark Ryland, Director Office of the Chief Information Officer		
As an individual	2019/05/15	163
Luc Jarry, Senior Advisor Cybersecurity		
Tawich Development Corporation	2019/05/15	163
Tony Gull, President		
Sam W. Gull, Advisor		
Robert Milot, Advisor		
Jean Fernand Schiettekatte, Advisor		
PayPal, Inc.	2019/05/29	165
Brian Johnson, Senior Director Information Security		

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the Committee related to this report. For more information, please consult the Committee's webpage for this study.

Citizen Lab

Cockfield, Arthur

Illumio

In Fidem

In-Sec-M

Jarry, Luc

Leuprecht, Christian

Quantum-Safe Canada

Skillicorn, David

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 145 to 149, 151, 152, 154 to 157, 163, 165, 168 and 170) is tabled.

Respectfully submitted,

Hon. John McKay, P.C., M.P.
Chair