**Cybersecurity: What Parliamentarians Need to Know and Do**

**Monday, March 9, 2015 – 4:45 p.m.**

**1 Wellington Street**

**Panelists:**

- Jane Holl Lute, President and CEO of the Council on Cybersecurity

and former Deputy Secretary of Homeland Security

- Paul Milkman, Senior Vice President, Technology Risk Management

and Information Security, TD Bank Group

- Peter Hammerschmidt, Director General, National Cyber Security Directorate,

Public Safety Canada

- John Proctor, Vice-President, Global Cyber Security, CGI

**Moderator:**

Fen Hampson, Co-Director of the Global Commission

on Internet Governance and Chancellor’s Professor, Carleton University

**Opening remarks:**

Maureen Boyd, Director of the Carleton Initiative for Parliamentary and Diplomatic Engagement

**Presentation:\***

Eric Miller, Vice-President, Canadian Council of Chief Executives

\*- see power point presentation

**Notes by Anaïs Voski**

Section I – Until 5:30 p.m.

* The shadow-war: we’re in the third age of computing. Firewalls used to work but now in a world of billions of users and apps we have to change our strategy
* We’ve gone from a mini-warfare scenario to an urban warfare scenario

Four main areas of cyberthreats:

1. Fraud: everyone likes to steal money
2. National security: Russia has used cyber attacks on Estonia
3. Theft of intellectual property: Finance / DRDC 2011
4. Hackivism: Anonymous, ISIS
* There’s a new technical complexity: it’s incredibly sophisticated and takes technological sophistication to understand. In order to formulate policy we therefore have to understand the language first.
* The Dark Web (which one cannot find in Google) is used, for example, for trading drugs or stolen passports
* Everything networked is hackable, and everything is networked
* This means a whole new level of security, and how we fit it into this new reality is the question
* We need collaboration. Public and private sector cannot do this alone
* The private sector owns 90% of critical infrastructure, but it cannot be done alone because governments have the capacity, they’re the ones passing laws and making regulations, so both have to work together.

Three main questions:

1. How de we as a country get ahead of this fast evolving threat?
2. Are there better ways that we can work with our allies?
3. What is the role of Parliament of addressing these challenges?

**Moderated Questions and Answer Session:**

**Fen Hampson:**

* The CIGI poll is interesting, we found that when it comes to individual citizens, trust in the internet is fast eroding.
* 63% more concerned about their online privacy compared to a year ago
* Everyone worries about their online security being compromised. Is that fear justified?
* What do we really mean by cybersecurity? What is the challenge?

**Jane Holl Lute:**

* Thanks for overview, most of which I will disagree with.
* When it comes to cybersecurity we’re telling ourselves a story
* Three interesting questions:
	+ 1) how do we make systems we trust from systems we can’t?
	+ 2) how do we ensure the integrity of information and identities in an open internet?
	+ 3) and what will the role of government be?
* This is what society has assigned to our governments to handle. Governments are used to being big players and monopolists in security, but it’s not true in cyberspace. No two countries in the UN are stepping up to challenge in same way.

**John Proctor:**

* The role of government is one of systems and architect: how to deal with security in design
* Consumers are demanding to be connected, society is like that, systems designed to spread info far and wide
* We might be at the tipping point. People are asking: how connected do I want to be?
* Every time you innovate, you become more vulnerable
* Integrity: how do we define online integrity? That’s become a key problem. How does the system demand integrity? Challenging the system architecture. Who built the actual architecture? Who designed it? If it is unstable, why trust it?

**Peter Hammerschmidt:**

* The Government of Canada is finding that other countries are developing cybersecurity strategies
* Vast majority of infrastructure is in the private sector, however, and not controlled by the government
* Ultimately it’s a private sector responsibility, but government has been helping to protect and facilitate protection, there’s a safety and security and economic imperative
* Areas looked at: information sharing, trying to share new ways to share information with private sector, and using some of the existing services, such as business you have with shareholders, customers, etc. and shaping how companies are responding to cybersecurity issues.

**Paul Milkman:**

* It’s a different perspective if you ask a banker. I think it’s interesting, because if you’re a well funded business and dependent on internet, for example as TD Bank Group is, we spend more annually on security than most governments do
* It costs 175-200 million dollars a year and it goes towards security infrastructure
* When we have new technologies that people use for banking transactions, it’s wonderful and enables commerce, but we have to create guarantees to the public as well
* When we speak to our individual 24 million customers, we give them free anti-virus and free web browser monitoring, which stops man-in-the-middle attacks – but takeup is low as the consumer doesn’t value it because doesn’t pay for it. We are yet to find balance with consumer
* There is progress with government; Department of Public Safety and CSEC have led the discussion. The current course and speed is not getting us there yet. We all have a different perspective depending on where you sit on this panel – what’s clear is that this is all of our problem.
* We don’t truly have control of this critical resource.

**Jane Holl Lute:**

* Reaction: a lot of us rely on the internet – that’s not true, we all do. There’s not an enterprise in this economy that doesn’t rely on the internet to deliver value. Cars rely on such infrastructure.
* We need a way to sort through what exactly is going on here. Why imperative? Attacks are going on every single day, but these are not sophisticated attacks. I don’t send my kids to school saying be careful of specific threats, I say wash your hands and cough into your sleeve. It’s a metaphor for our basic hygiene and it’s true about our online activites
* 3 billion are online today. That’s half the population of China
* Governments are not playing the role they’re supposed to because they don’t have the power that matters. The power of government is to protect us, not connect us. But what role do we want them to play? Our reliance is absolute.

**Fen Hampson:**

* How are they going to do it? They’re in the business of collecting and trading data
* It’s easy for the government to say: it’s not our problem. But I think it is our problem, because when bad things happen people look to their government to deal with it.

**Peter Hammerschmidt:**

* You’re absolutely right
* This needs government help, we recognize that in Public Safety, so we have been focused on those enterprises and have been trying to partner with the private sector to expand reach into sectors we haven’t previously had a reach into
* We provide organizations with practical tools and reach out to them, because we see them as being vulnerable. But it’s also a critical point in the economy and critical infrastructure. There’s a role there for government. Is that a regulatory role or other role?
* Regulatory is one way, through guidelines, standards, legislation, etc. There are a number of tools that government can use. If there’s no other option than regulation, even non cyber-savvy organizations will have a lot of interest in those

**John Proctor:**

* Some attacks are very sophisticated
* A lot of companies spend money on being technically sophisticated. How does government assist and help them? One of the challenges: We have a pipeline problem, how are we generating folks who can do it? Everyone needs cyber. Why aren’t we doing that? UK has a cyber apprenticeship program. We need to go down that road as well
* What’s our equipment like? Well-educated people are one thing, we also need well-trained people. Hard to hire and retain those kinds of people, but there’s a demand for them
* What is Canada known for globally? Trust. How do we take that model to the market? We got cyber. We don’t overregulate, because you’ll kill us and small businesses. It becomes a balance of what companies should be doing
* Critical infrastructure in cyber, but what is critical? If police can’t reply to an energy or hospital shuts down, that is critical
* He who tries to defend everything defends nothing
* Regulation has to be more specific
* What’s critical infrastructure? Transportation systems, health, etc. As North Americans, we’re not doing enough to protect those against cyber attacks.
* Cyber warfare will be directed at critical warfare in the future.

**Jane Holl Lute:**

* What is the fact? If it’s a warzone, how big do you think it is?
* We’re not going to manage cyber space as if it were a warzone, we’re not managing it as a military.
* We need to think about how to protect ourselves in this environment. A lot of attacks are preventable. Why haven’t we done more? Why aren’t we doing more to help people understand?
* Until recently this was an intelligence subject, but those days are over.
* Questions:
	+ 1) Do you know what’s connected to your networks?
	+ 2) Do you know who has administrative authority and who can override?
	+ 3) Can you patch it before the bad guys do bad things? It’s about the 80-90% that we can do in terms of protection so that military action doesn’t become necessary.

**Paul Milkman:**

* If you have a limited number of sophisticated institutions, most of the population doesn’t know.
* Most of the world is immature in its ability to protect itself. The reality is that the bad guy has stolen enough money from us, he operates efficiently, and cooperates well with other bad guys, sometimes they’re even protected under another country’s policy. Who’s going to do something about it?
* I don’t think it’s about money. Institutions would contribute to shared services, but those need to be provided by a government or mandated by a government. Not by regulation, but shared capabilities. I don’t know how we get there.
* If we don’t have a lot of time to improve this, then what do we collectively do about it?

**Fen Hampson:**

* We’re seeing a move towards encryption.
* It’s interesting that the American, Australian, and Chinese presidents have suggested that companies should not produce IT products so secure that governments cannot gain access to them. They need to have access for intelligence gathering, law enforcement, national security, etc.
* What are your views about the encryption revolution? Should there be regulatory response to open up back doors?
* Last week the Globe and Mail created a sophisticated network to communicate sensitive information concerning their investigative journalism. It seems like the government has lost trust.
* Creating the balance is the hardest part.
* PNR: stands for Passenger Name Record. It’s the gold standard of protection for the individual’s privacy.
* We look at privacy quite differently from Europeans than Americans. It’s all about ownership in Europe, in the US it’s about limiting government’s ability to intrude into our lives.
* Privacy: I don’t care if you know my blood type, I care if you can change it

**Notes by Stephen Power**

Section II --- From 5:30 PM

**Fen Hampson:**

- Are North Americans doing enough to harden critical infrastructure against cyberattacks? Are we on the cusp of a new frontier of cyberwarfare?

**Jane Holl Lute:**

- We aren’t going to manage cyberspace as if it is a warzone, or manage cybersecurity as a military operation

- We need to think about how to protect ourselves in online environment

- Many attacks are not sophisticated, are easily preventable

Why isn’t government and industry doing more to help promote “basic hygiene” regarding cybersecurity?

- Up until now government has treated cybersecurity as a problem for the intelligence community, and industry has treated it as an unavoidable nuisance

- This approach is no longer acceptable

Four questions that can be asked to help understand how secure an organization is:

- Do you know what’s connected to your networks?

- Do you know what’s running on those networks?

- Do you know who has admin privileges to change, override, or alter security settings?

- Do you have an alert system set up to allow you to patch holes before they can be exploited?

 - These four questions can prevent 80-90% percent of cyber threats

**Paul Milkman:**

- The vast majority of people and organizations aren’t sophisticated enough to protect themselves against cyberattacks

- In these cases you need to seek out shared services from government or the private sector

- “Bad guys” are operating very efficiently and often operate in other jurisdictions where they can’t be stopped or identified. Small and medium businesses aren’t evolving fast enough to defend against this

Who is going to do something about this?

- Shared services are an option but there needs to be government backing in providing them since industry can’t pull this together on its own although the population is asking for these services

- If we don’t have too much time to improve this situation, what do we collectively do about it?

**Fen Hampson:**

- What are your views on the “encryption revolution?” Do we need a response, possibly regulatory, to create backdoors in encryption programs so that those responsible for public safety and national security can go after “bad guys” using encryption to conceal their activities?

**Paul Hammerschmidt:**

- Need to balance these concerns against privacy concerns

- Don’t know the answer or where the balance lies

- There needs to be a broader discussion in society around this issue

- no country is going to take a firm position on this so not much to add

- security imperative exists; government at the end of day is expected to step in and provide protection

**John Proctor:**

- Notes that people are losing confidence in what they can do on the internet privately

- Interest growing in privacy solutions to defend against government intrusion

- Solutions provided by industry are steered partly by consumer choice

- Government has lost trust, including the commercial world

Some people could care less about who reads their e-mails; Snowden revelations did not impact internet usage

- No win scenario for government

- If government doesn’t use surveillance to stop a terrorist attack, fault lies with government

- But if they get caught snooping, fault also lies with government

- It will be hard to find a balance but demanding encryption keys are not the answer

**Jane Holl Lute:**

- People are asking the government if it is working to keep everyone safe

- What are the rules the government is operating in?

- Many different governments have different cyber concerns

- Really about ownership of data, not just limits on government powers

**Paul Milkman:**

- Hardest thing is that cyber is very polarizing

- Need for sober look at issue

- Not a battle between privacy advocated and government; balance is important

- Media discussion has not been about this balance and this has not helped things

**Question:** How does the government meet security concerns surrounding foreign manufacturers of electronics?

**Hammerschmidt**: Several options exist

- Government can work producers as well as buyers

A tricky area, you need to be sensitive to trade and diplomatic issues

**Question:** Asker would like to hear more about encryption, backdoors and information sharing, generally

**Milkman**: Different levels of cooperation

- Within private sector and certain government ministries there is a lot of information sharing

- There are different kinds of information sharing and it differs from field to field

How do you strike a balance?

- Sharing between governments and within governments deal with different issues

**Lute:** U.S./Canada information sharing is a good example

- Information sharing is at the heart of the debate in the U.S. along with the role of government

- Government structure is anathema to the structure of the internet and a different approach is needed

- Increasing connectivity is changing how we interact and intersecting with decaying trust in public and private institutions

Where do we look to find principle on the issue?

- Government cannot do everything and the private sector must take some responsibility

**Question:** What safeguards can be put into place to defend against insider threats?

**Proctor:** Comments on previous question about foreign manufacturers

- You need different degrees of assurance that security issues have been satisfied depending on the sensitivity and complexity of the technology being produced

- Certification programs and processes can help here

- Looking at a specific manufacturer can be misleading given globalized production and supply chains

Insider threat is insidious, whether you are in a large or small institution

- How do you fund these institutions and help them defend themselves

Insider threat programs ask: what can an insider do, and how can you monitor for that threat

- If you want to monitor employees you need to have to the rationale and policies along with both the technology and workforce to do so.

- Insider threat programs exist but they have privacy and logistical issues

**Lute:** We suffer from “the fog of more”: many checklists, guidance, and programs when it comes to cyber security

- Center for Internet Security has a list of “the 20 critical security controls” to watch on cyber and reduce vulnerability

- Need to know how to do the basic things to reduce vulnerability so that when a threat does arrive you can focus scarce resources

**Question:** Is a Geneva Convention around cybersecurity needed?

**Lute**: Governments need to figure out what their role is in cybersecurity, need the conversation about that principle

- A convention alone won’t be good enough

**Question:** Question asker seeking more information on balance between privacy and security

**Question:** What cybersecurity tools need to be built?

**Proctor:** People looking for the cybersecurity bullet

- There is none, it’s too complicated

Monitoring is key so that you know how to react

- The pieces to build are everything we do day-to-day

- However you need balance so that consumers are comfortable with a certain amount of security

As well, insurance industry may play a role by providing a market indicator in “cyberinsurance”

- However the insurance industry doesn’t have the data to create effective models

**Hammerschmidt:** Insurance industry could potentially play huge role

- Insurers receive data with every claim, important feedback mechanism What is need are people like the question asker

- More innovators need to be trained

**Lute:** Specific rules needed to protect privacy

- Rules are needed to get the balance right. Need to be explicit with these rules

- Need ability to revisit problems and issues down the road

Need to build a dashboard for non-tech to understand principles of cybersecurity – these tools don’t exist but they are necessary

Lack of insurance data means that everyone is treated as a menace

We need to get serious about security collectively.

**Milkman:** Always a need for tools that simplify understanding of cybersecurity

Cybersecurity of Canada needs to be considered

- Canada needs to more definite stance at what it will and will not allow

Some common sense decisions that can be made at the government level

- Real question of government will and ability to build cybersovereignty

- Might happen here earlier than others because of Canadian attitude toward risk management

**Closing remarks:**

 **Dr. Rafik Goubran,** Carleton’s Dean of Engineering and Design,

- Increasing reliance on internet and connectivity creates opportunities and risks

- There are also “smart” devices that are seen positive developments, but they are also sensors that monitor us constantly and can become vulnerabilities

- Sensors can open up new dimensions of vulnerability

Carleton is paying lots of attention to big data

- At one time there wasn’t enough data, now there is so much we need to figure out how to use it properly

- Many avenues and ways to find solutions and to generate personnel

- Carleton working with private and public sector on these files