Canadian Association for Security and Intelligence Studies

THE CYBER CHALLENGE

Highlights from the CASIS 2016 Annual Symposium

September 23, 2016

This report is based on the views expressed during an annual symposium organised by the Canadian Association for Security and Intelligence Studies. Offered as a means to support ongoing discussion on security and intelligence issues, the report does not constitute an analytical document, nor does it represent any formal position of the organisations involved.

http://www.casis-acers.ca/

Report by Adam Chuipka

CANADIAN ASSOCIATION FOR SECURITY AND INTELLIGENCE STUDIES

Who We Are

The Canadian Association for Security and Intelligence Studies (CASIS) is a nonpartisan, voluntary organization established in 1985. Its purpose is to provide informed debate in Canada on security and intelligence issues. A distinguished board of directors comprised of professionals of national and international reputation and status oversee the operations of the association.

Membership is open and currently includes academics, government officials, journalists, lawyers, former intelligence officers, students and interested members of the public committed to the study of intelligence services.

What We Do

For over twenty-five years CASIS has held an annual meeting and has sponsored conferences, symposiums and forums on particular intelligence and security-related themes. The first conference was held at Glendon College in Toronto in June 1984 with others being held in Vancouver, Montreal, Calgary, and Halifax; more recently annual conferences have been held in Ottawa.

As an organization, CASIS was formed in May of 1985 at which time a constitution was adopted. That constitution has been amended and updated through the years, most recently in October 2011. Today CASIS's aims are to:

- To encourage and promote the study of intelligence and security, and the teaching of courses at Canadian universities and colleges in these fields;
- To encourage research in intelligence and security in the interest of higher education, scholarship and an informed public opinion;
- To provide an interdisciplinary forum through which interested academics, and other interested persons may engage in matters relating to intelligence and security;
- To provide a body of resource expertise to the interested public in order to facilitate awareness and understanding of intelligence and security activities as carried out in various sectors, disciplines and organizations;
- To electronically publish regular information about the Association and its activities and other matters pertinent to the Association's mandate;
- To study the role of security and intelligence services in society, to foster the accumulation of knowledge about such activities, and to study the relationships between security and intelligence agencies and the governmental institutions and constitutional values of society.

THE CYBER CHALLENGE

Highlights from the CASIS 2016 Annual Symposium

September 23, 2016

Table of Contents

A Canadian Perspective on Cyber Challenges

The Communications Security Establishment Canada (CSE) is Canada's national cryptologic agency and has a long history of protecting Canada and Canadians from threats. CSE has three key roles under its mandate:

1. To acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with the Government of Canada intelligence priorities;
2. To provide advice, guidance and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada; and
3. To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Increased reliance on digital information has necessitated a heightened focus on cybersecurity. More and more of the world's, and Canada's, government operations, business, military systems and citizen's lives are conducted online. This increased prevalence of digital information and electronic systems represents a tremendous opportunity for Canada to collaborate, innovate, and drive economic prosperity.

- Canada has one of the world's most connected populations. Out of a population of approximately 36 million people, as of July 2016, there are an estimated 32 million Internet users in Canada.
- Canadian citizens can access over 200 federal government services online. Almost every aspect of Canadian life – whether it's finance, electricity, education, research and development, transportation, entertainment or social interaction depends in some way, shape or form on the Internet. Almost 4% of Canada's Gross Domestic Product is directly dependent on the Internet.

This increased prevalence of digital information and electronic systems also presents risks and threats to our governments systems, to Canadian industry, and ultimately to Canadians.

- The Internet was designed to be reliable; it was not designed with security in mind. Computer technology used to be self-contained, and fairly simple. Security vulnerabilities arise from new technology being layered on top of, rather than replacing, older common components which has created complexity in a system that can have widespread impacts.
- While the Internet used to be the exclusive domain of states, it has become much easier to acquire the tools and knowledge required to obtain and create cyber weapons. In addition to the 100 cyber capable countries, there are a growing number of non-state actors that pose a threat.
- Already, federal computer systems are probed more than 100 million times a day by suspected malicious actors searching for vulnerabilities. The National Research Council hack of 2014 was an expensive lesson.

The advent of quantum computing will bring tremendous opportunities for science, medicine and engineering. However, protecting systems will prove much more challenging.

- Once Quantum technology becomes a commercial reality, it will render current encryption methods ineffective for securing sensitive government, business, and personal information.
- Cryptologists at CSE and around the world are racing to find new cryptographic standards before quantum computing power advances within this decade.
- Waterloo's Institute for Quantum Computing has been doing some incredible work in that area (see *Presentation: Cybersecurity in a Quantum World*).

> For Canada to realize all of the benefits that Internet technology can offer, it also has to offer trust and confidence.
>
> — Greta Bossenmaier, Chief, CSE

To effectively tackle these challenges and realize the benefits and potential that the Internet brings to our society, we need to innovate. There are three important building blocks that have helped CSE add value in its important cyber security role – people, technology, and partnerships.

- Shared Services Canada (SSC): Prior to the establishment of SSC, CSE worked with 43 different government organizations to protect their individual networks. With all these organizations now under one network, CSE can detect and react to malicious activity much more efficiently.
- Public Safety: The Canadian Cyber Incident Response Centre (CCIRC) is Canada's national coordination centre responsible for reducing the cyber risks faced by Canada's key systems and services. CCIRC works within Public Safety in partnership with provinces, territories, municipalities, private sector organizations and international counterparts. It also coordinates the national response to any serious cyber security incident. CSE serves as a technical adviser to the Centre.
- Canadian Cyber Threat Exchange (CCTX): Through the CCTX, CSE shares unclassified cyber threat information gathered through their unique capabilities as well as some of their cyber defence tools to help companies better defend themselves.
- Academia: The Tutte Institute for Mathematics and Computing (TIMC) is a Canadian government research institute programme of CSE responsible for conducting classified research in fundamental mathematics and computer science, with a research focus in cryptology and knowledge discovery/data mining. Tutte has already established key partnerships with learning institutions, including Carleton University and the University of Calgary.
- CSE IT Security Learning Centre: The Centre provides relevant Government of Canada IT security knowledge and skills that security practitioners can apply to their own departmental practices.
- The Government's Cyber Security Review: The Review will examine how Canada can remain secure, resilient and economically prosperous in the face of an evolving cyber threat environment. Consultations are a critical part of the review process.

A Perspective on the Cyber Threat

With more than 100 cyber capable countries and an increasing number of cyber capable non-state actors, cyber threats are growing on a daily basis. There is not one country or business that hasn't been penetrated, whether it is political activism, organized crime, espionage – government and industrial, disruption of service, or destruction of property.

- There is an alarming trend that critical infrastructure and major corporations are the target. Malware is widespread and well-placed and there is no regulatory requirement to hunt and eradicate it – there should be. The United States should institute a national cleanup given the ubiquity of malware already in its networks.
- We need to increase information sharing, enhance guidelines, strengthen pattern recognition to see where the trends are, and implement third party requirements. Best practices are not being followed.

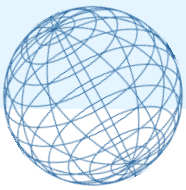
> We must have an honest conversation about the state of our cyber *insecurity*.
>
> — Melissa Hathaway, Senior Advisor, Cyber Security Project, Harvard Kennedy School's Belfer Center

Focus should be placed on the most critical infrastructure such as power, telecommunications and finance rather than spreading across all sectors. Everything else depends on these three.

- Power: First and by far the most important, without power nothing else functions. The energy sector – both nuclear and electric – is constantly being probed and disrupted. In 2014, malware was discovered in the core of operations systems of multiple nuclear systems in South Korea. In December 2015, Ukraine electric power was targeted and disrupted. In this case, Ukraine still had old systems in place to bring the power back. Most Western systems, including the United States and Canada, no longer have those systems in place to fall back on.
- Telecommunications: Enabling the free flow of goods, services, data, and capital, telecommunications is the second most important critical infrastructure. Without telecommunication systems, nothing else works. Telecommunication providers are constantly experiencing distributed denial-of-service (DDoS) attacks reaching destructive levels.
- Finance: We cannot afford to lose trust and confidence in the global financial system; we are wholly dependent on it. Recently, the Society for Worldwide Interbank Financial Telecommunication messaging system has been bombarded with cyber-attacks. In March 2016, $81 million was stolen from a bank in Bangladesh. Banks in Ecuador, Vietnam, Japan, South Korea, China, Singapore, Philippines, and Italy have all faced attacks as well.

The Internet of Things on the horizon will lead to challenges in securing networks as embedded devices come online.

- Everything from embedded medical systems, to autonomous vehicles, to smart grids and smart cities are driven by technologies which will become commonplace over the next 5 years. We must anticipate and mitigate the next generation of threats to internet-connected devices or we will be left even more vulnerable than before.



Global Security Implications

The Stability-Instability Paradox in Cyberspace

The cyber realm can be very complex - not because it creates new modes of force, but because it provides for interesting alternatives that expand the range between traditional conflict and traditional peace. Two perspectives:

- Pessimistic – Offensive Advantage: The cyber realm is highly asymmetric giving a strong advantage to the attacker. There are a growing number of threats and many non-state actors now have a way to gain an advantage. Defending everywhere at once is highly impractical. Furthermore, there is a problem of attribution in cyberspace – without evidence of who the attacker is deterrence, justice, retaliation, or a counter-strike is not possible.
- Optimistic – Defensive Advantage: Intrusions at the high end require a great deal of expertise, intelligence, and are the result of years of planning. Coding bugs in a cyber weapon used in a large operation can prevent the successful execution of an attack. From the attacker's side, there is a lot that can go wrong.

There is a lot we can learn from concepts developed during the Cold War. The Stability-Instability Paradox can help explain cyber behaviour today.

- Nuclear weapons were not good weapons; they were, however, good for deterrence. Mutually Assured Destruction (MAD) created a delicate balance of terror: a contest of resolve with the introduction of an element of chance where things might get out of control. This created an interesting situation. There was stability at the nuclear level because states would not risk threatening MAD, but instability at the conventional or subconventional level, as proxy wars were the alternative to nuclear confrontation.
- In cyberspace, the ability to engage depends entirely on cooperatively produced infrastructure and a willingness of both sides to stay connected. Therefore, deterrence is still a factor. Concealment in cyberspace is harder to maintain at higher-level cyber operations. This risk of attribution could equate to the risk in a shift of domains where cyber aggression can be punished. This creates stability at the truly dangerous and destructive levels in cyberspace, and instability at the lower levels where we see minor aggressions with social and economic value, such as espionage, covert influence, and symbolic protest as more common. Of course, deterrence is not always effective against certain actors.

Casus Belli: Can Cyber War Lead to Real War?

Cyberspace is fundamentally changing decision makers' perspectives on what the threat is and how to address it. Cyber operations are more covert than traditional operations, which can lead to hacking in peacetime.

- The problem of attribution in cyberspace proves a challenge for military commanders who are faced with cyber-attacks that are more covert action than traditional military action. Deterring and responding to these threats is a challenge if the assailant's identify and motive for attacking is unknown.
- With regards to chemical weapons, there are 5000 facilities around the globe that can be inspected at any time. How is it possible to achieve a similar inspection access to cyber weapons?
- Cyberwarfare is real - militaries will need to prepare the battlefield for wars that may never happen by undermining networks around the world. Attacks on infrastructure to prepare the battlefield would have very real consequences for civilians depending on the same infrastructure.
- Can a country be coerced into doing something through cyber-attacks? The example of cyber-attacks on Estonian networks resulted in the networks going offline for a few hours. If this extended to a few days, the damage could be staggering. However this hasn't dissuaded Estonia from further deepening its technological dependence.
- Cyber-enabled propaganda and information operations prove to be a challenge as well. Cyberspace introduces a lot of uncertainty; digital information – whether true or not – can be disseminated across the globe instantly and have an impact on those viewing it. Taking it down in one place will not prevent it from being posted in another.

> Cyberwar might lead to real war if the national security decision maker decides it to be so.
>
> — Kenneth Geers, Senior Research Scientist, Comodo

In terms of strategy, we should be focused on mastering the technology rather than fearing it.

- Canada and the United States have enormous strategic depth in cyberspace that Russia and China do not possess. The more authoritarian regimes are, the more they fear cyberspace. We need to invest in infrastructure and bolster the Internet as a force for good.
- The China-United States cyber accord is seen as an example of how diplomatic efforts can reduce cyber-attacks between states. However, due to the attribution problem, deterrence efforts are never fully realized, as cyber-attacks can be pushed to a lower, less traceable level.

Cybersecurity in a Quantum World

Quantum computing is based on quantum mechanics, the branch of physics that explores the set of laws governing the atomic and subatomic level of atoms, electrons, photons and other particles. While traditional computers use long strings of bits to encode either a zero or a one, quantum computers use quantum bits, or qubits. Qubits have two distinct properties:

1) Superposition: the ability to be in multiple states at the same time – that is, something can be "here" and "there," or "up" and "down" at the same time.

2) Entanglement: the phenomenon in which two or more quantum particles can be inextricably linked in perfect unison, even if separated by great distances.

These two properties allow quantum computing to easily factor very large numbers very quickly, which is considered impossible for even today's best computers. Modern cryptology practice takes advantage of this mathematical problem to prevent "eavesdropping" of encrypted information.

> Everything you are going to send or have sent on the internet today or in the past will be decrypted.
>
> – Ray Laflamme, Executive Director, Institute for Quantum Computing, University of Waterloo

The immense processing power of quantum computers will someday render the most widely-deployed cryptosystems in security products today (including RSA & Elliptic Curve Cryptography) ineffective. However, this technology is yet to be realized and there is ongoing research on new ways to make "quantum-safe" cryptosystems.

- Quantum cryptography requires the control and manipulation of a few million qubits. As of today, the record in Canada for controlled qubits is 12, with a high frequency of error. In the next 5 years it is predicted 100 qubits will be reached. It won't be until we have reached 40 qubits that it will become possible for us to simulate quantum dynamics that are currently inaccessible on today's hardware.
- Quantum-Safe Cryptography (QSC) refers to efforts to create cryptosystems based on problems that neither classical nor quantum computers can effectively solve. ISARA is developing Quantum-resentment solutions for classical computer systems.
- Quantum Key Distribution (QKD) refers to cryptosystems that make use of quantum mechanics to exchange cryptographic keys known only to the communicating parties. These can then be used to encrypt and decrypt messages allowing guaranteed secure communication. Any attempt of eavesdropping from an outside party would be known by those communicating. However, current fiber optics networks would need updating for its use because every 20 km needs a repeater, which is essentially an "eavesdropper". These repeaters would require a quantum equivalent to maintain a direct connection. There are currently some small QKD networks around the world, there just needs to be a willingness to make them smaller and more useful.

The Threat to the Private Sector

Private Sector and Critical Infrastructure

At 85 per cent, the bulk of critical infrastructure in Canada is in the hands of the private sector. The cyber challenge necessitates collaboration between the public and private sector to ensure they can effectively address this challenge.

- Critical infrastructures are described by the Canadian government as processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.
- Canada recognizes ten critical infrastructures including: energy and utilities, finance, food, transportation, government, information and communication technology, health, water, safety, and manufacturing.
- The National Cross-Sector Forum was created to promote information sharing across the sector networks and address cross-jurisdictional and cross-sectoral interdependencies in order to facilitate resilience.

Critical infrastructure in Canada is growingly dependent in one way or another on information technology to operate. Many critical infrastructure sectors are interdependent, meaning a problem in one could have a cascading effect on the others.

- When an entertainment company gets hacked, company and company employee information may be stolen, there may be a drop in market capitalization, and perhaps the resignation of a company chair or CEO.
- However, when any number of critical infrastructures are faced with a devastating cyber-attack, the damage is much greater and can potentially affect millions of people. In December 2015, Ukraine experienced such a cyber-attack, demonstrating that cybersecurity should be taken very seriously.
- These interconnected parts of some critical infrastructures are dependent on preceding parts, without which successive parts cannot operate. Without power, telecommunication systems cannot function. Without telecommunication systems, a number of industrial control systems (ICS) that depend on telecoms can no longer operate, including electricity systems that are moving more and more towards the use of ICS with no fallback alternative.
- As demonstrated by the Stuxnet virus, even “air-gapping” ICS does not fully protect critical infrastructures from infiltration. Many of these companies are taking measures to ensure they are educated and protected as can be, as well as ensuring the proper separation between information and operation technologies.

Managing Risk and the Internet of Things

The Internet of Things (IoT) is essentially everything connected to the Internet that can communicate with us, with other programs, and other devices and "things" without the need for human input. "Things" ranging from industrial control systems, to operation technology, to smartphones, to appliances, to health monitors, to enterprise information technology, to smart grids. While this results in improved efficiency, accuracy, and economic benefit, it also exposes us to new risks and security challenges as interdependencies and complexity arise.

- Threat agents in the IoT include more well-understood agents that have operated in the Internet or enterprise information technology systems, such as criminals, hacktivists, industrial spies, nation states, terrorists, and insiders. However, the IoT also presents new threats, such as chaotic actors, vigilantes, and regulators.

  - Chaotic actors simply aren't looking for anything logical, like money. They can't be deterred, bought, negotiated or reasoned with – they simply want to see things burn.
  - Vigilantes are only narrowly looking to right a wrong and don't necessarily think or care about the interdependencies that could be affected from their actions, whether they are technical, political or personal (ex. Panama papers, Ashley Madison hacks).
  - Regulators may lack awareness of the interdependencies at play in the IoT. Their actions, while well-considered, may have unintended consequences and cascading effects that could not have been predicted.

Using Machine Learning to Detect Cyber Threats

It's impossible to fully secure your enterprise network; sophisticated threats always find a way in. The threat of insiders is equally important. A new era of cyber threats has emerged. Algorithms are fighting other algorithms and attacks are moving at computer speed. Human security teams can't keep up. Cybersecurity automation is required to keep up with the cybersecurity threats of today.

- Machines are needed to fight back against other machines. New machines that are automated to detect and contain threats are essential to continue fighting the cyber threat. Humans cannot keep up with the speed of threats.
- Unsupervised machine learning is critical for cyber solutions. These machines learn the network they are assigned and are able to instantly detect anomalies. By letting these machines do the heavy lifting, they can then alert us to where we need to go and resolve the problem if it hasn't already taken care of it.

Cyber & Foreign Policy: Mitigating the Dangers

Developing International Norms

Currently the United Nations is trying to develop norms, rules or principles for the responsible behaviour of states in cyberspace. The ultimate objective is strategic stability in cyberspace.

- In 2012-2013, the UN arrived at an understanding that international humanitarian law applies in cyberspace. Also known as the law of armed conflict, this law regulates the conduct of war (*jus in bello*) and applies when there is a use of force. This was a big step forward, because this includes the P5 and other major cyber actors.
- Furthermore, under Article 51 of the UN Charter, the threshold for self-defense is "armed attack". This means if a state is attacked with cyber measures that equates to an armed attack, a response to a cyber-attack may be a kinetic attack. This ultimately allows for more options of deterrence.
- The G7 and G20 have endorsed these norms. They have been supported under bilateral understandings between a number of different states as confidence-building measures. While norms are not binding, by creating these understandings we can slowly begin legitimizing certain actions – such as self-defence – which has a strong deterrence effect. The China-United States cyber accord is seen as an example of how diplomatic efforts can reduce cyber-attacks between states.

Track 1.5 Discussions with Russia

Prior to 1991, Russia was a technological superpower. It had its own independent telecommunications stream, large amounts of research, and an impressive industrial capacity. With the collapse of the Soviet Union, this changed and was replaced by foreign technology.

- This came as a tremendous shock to the Russians, who were now using cyberspace which not only supported Western political and economic systems, but was in a sense "owned" by the West. This "colonization" of cyberspace by a foreign power impacted and drove how Russians view and use cyberspace.
- The Russian approach to cyberspace and how to engage on cyber issues has developed over time by the same group of individuals that is still involved with cyber issues. The Russians have much longer strategic thinking in this area.

Early on, Russians never used the term "cybersecurity" – they used "information security". This is because they realized that they had the least degree of control over the technical networks\ and that the information on these networks was the real concern.

- This has changed in the past few years. Cybersecurity is talked about, but the Russian focus remains on information. Russians are looking at finding a state-based solution for the rules of the road on what happens in cyberspace. They have been more serious about it than the West in track 1.5 negotiations. Finding an agreement to deal with extremists' use of internet has been Russia's biggest concern.

APPENDIX

CASIS 2016 Annual Symposium Agenda (Revised)

The Cyber Challenge

An Annual Symposium of the Canadian Association for Security and Intelligence Studies

September 23, 2016
Barney Danson Theatre, Canadian War Museum

Program

8:50	Opening Remarks: Greg Fyffe, President, CASIS
9:00 – 9:45	Presentation: "A Canadian Perspective on Cyber Challenges" John Tait Memorial Lecture: Greta Bossenmaier, Chief, Communications Security Establishment
9:45 – 10:00	**BREAK**
10:00 – 11:00	Presentation: "A Perspective on the Cyber Threat" Melissa Hathaway, Senior Advisor, Cyber Security Project, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard
11:00 – 12:00	**Panel One: Global Security Implications** Chair: Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security Branch, Public Safety Canada Presentation: "The Stability-Instability Paradox in Cyberspace" Jon Lindsay, Assistant Professor of Digital Media and Global Affairs, Munk School of Global Affairs, University of Toronto Presentation: "Casus belli: Can Cyber War lead to Real War?" Kenneth Geers, ex-NSA, NCIS, NATO, author of *Strategic Cyber Security*
12:00 – 13:00	**LUNCH**
13:00 – 14:00	Presentation: "Cybersecurity in a Quantum World" Ray Laflamme, CIFAR Program Director and Senior Fellow, Quantum Information Science Program and Executive Director, Institute for Quantum Computing, University of Waterloo

14:00 – 15:15 **Panel Two: The Threat to the Private Sector**

Chair: Colleen Merchant, Director General, National Cyber Security, Public Safety Canada

Presentation: "Using Machine Learning to Detect Cyber Threats"
David Masson, Darktrace Inc.

Presentation: "Managing Risk and the Internet of Things"
Tyson Macaulay. Francis Bradley, CEO Canadian Electricity Association

15:15 – 15:30 **BREAK**

15:30 – 16:45 **Panel Three: Cyber and Foreign Policy: Mitigating the Dangers**

Chair: Bob Gordon, Canadian Cyber Threat Exchange

Rafal Rohozinski, Sec Dev

Michael Walma, Cyber Foreign Policy Coordinator, Canada Global Affairs

Melissa Hathaway, Senior Advisor, Cyber Security Project, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard

16:45-17:00 Closing Summary: Jon Lindsay, Munk School, University of Toronto

17:00 **CLOSE**