Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

> *"Cybersecurity is perhaps the most difficult intellectual profession on the planet."*
>
> Dan Geer
> Computer security and
> risk management specialist

In this article, we seek to identify the important challenges preventing security in cyberspace and to identify the key questions that nations should set out to answer to play a leading role in securing cyberspace. An important assertion is that the challenge of securing cyberspace transcends the abilities of any single entity and requires a radical shift in our approach in how: i) research is conducted, ii) cybersecurity researchers are educated, iii) new defendable systems are developed, and iv) effective defensive countermeasures are deployed. Our response draws upon extensive source material and our personal experiences as cybersecurity professionals contributing to the establishment of the VENUS Cybersecurity Corporation, a not-for-profit corporation that aims to make Canada a global leader in cybersecurity. We view the challenge to be global and transdisciplinary in nature and this article to be of relevance world-wide to senior decision makers, policy makers, managers, educators, strategists, futurists, scientists, technologists, and others interested in shaping the online world of the future.

Introduction

The explosive growth of the Internet has radically transformed the way we interact as a society. It underpins all facets of our critical infrastructure, enables global commerce, and affords us unparalleled near-real time access to information. It has also made us information-dependant in both our professional and personal lives. With the advent of the Internet of Things (IoT), we now live in a digital era that has rapidly transitioned society from a state best described by the term "always connected" to a new reality of "everything connected".

An unintended consequence of this connectivity is that it has introduced new vulnerabilities, adversarial threats, and challenges to our society. Network boundaries are becoming both blurred and porous. In fact, the overall "attack surface" of modern networks is increasing at an exponential rate. Cisco estimates that 15 billion devices will be connected to the Internet this year, increasing to 50 billion devices by 2020 (Macaulay et al., 2015). Each new device represents a new connection into the network and yet another potentially exploitable entry vector for an adversary. Perhaps most worrisome is that studies have shown that approximately 70% of these devices contain serious vulnerabilities (HP, 2014). Here, the asymmetric nature of cybersecurity comes into focus, namely the work factor for an attacker is the "cost" of finding a new attack vector while the defender bears a cumulative cost of all known attacks. Put more plainly, a defender has to stop all entry vectors into a network whereas an attacker only has to find one way in (Geer, 2015).

Although we can argue that the IoT represents a revolution of connectivity, the Industrial Internet of Things (IIoT) – the use of IoT technology in manufacturing – represents a steady evolution of structured connectivity. Anxious to reduce operational costs and increase industrial automation, the very "system of systems" that composes our critical infrastructure (e.g., the smart

Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

grid, water treatment, transportation, financial services) are all moving away from communicating over air-gapped enclaves to leverage the connectivity provided from information technology (IT) networks. Operational technology (OT) and IT networks have converged and, as a result, systems and architectures everywhere are at risk because they are being tasked to perform in unintended ways. In fact, recent high profile cyber-attacks against cyber-physical networks all highlight the fact that digital attacks are bridging from the virtual world to cause major damage in the physical world:

1. The Stuxnet computer worm was designed to infect and replicate using Windows operating systems in order to overwrite Siemens Step 7 software. It targeted the Iranian nuclear program and, once installed, Stuxnet, allowed for both surveillance of enrichment activities and sabotage by causing centrifuges to spin out of control (Langer, 2011).

2. The self-replicating virus dubbed "Shamoon" operated in three distinct phases to attack Saudi Aramco, a national petroleum and natural gas company in Saudi Arabia. The first phase was used to infect a system in order to steal data. In the second phase, the virus attempted to infect connected systems within the local network in order to maintain persistence in the target network. Finally, in the last phase, the virus attempted to hide its "tracks" using destructive techniques that include overwriting accessed files and the system's master boot record (Bronk, 2013).

3. In 2008, intruders exploited the software running on surveillance cameras along the Baku–Tbilisi–Ceyhan (BTC) crude oil pipeline in Azerbaijan, Georgia, and Turkey. The exploit allowed them to gain access to software that provided operational control of the pipeline so they could increase pipeline pressure without raising alarms, ultimately causing an explosion that shut down the pipeline (Robertson, 2014).

4. Germany's Federal Office for Information Security (BSI) reported massive damage to an unnamed steel mill in Germany. The mill suffered an intrusion through malicious software attached to an email that allowed for unauthorized access to critical plant components. The threat actor showed knowledge of industrial control systems and caused cascading system failures that resulted in a massive explosion (Zetter, 2015).

However, there are also many examples of success stories in the quest to secure cyberspace:

1. Operation Tovar was an international collaborative effort among law enforcement agencies to counter the Gameover Zeus botnet used by cybercriminals to perpetrate bank fraud and distribute the malware referred to as CryptoLocker ransomware (Dawda, 2014). CryptoLocker was a Trojan horse program that would encrypt files on a hard drive and would display a message stating that a ransom or payment would have to be made in order to decrypt them. After the botnet's command and control infrastructure was taken down, the decryption keys were recovered and made available to victims free of charge.

2. The Australian Signals Directorate has released a list of the top 35 mitigation strategies to against targeted intrusions. Those organizations that followed the mitigation strategies have shown a dramatic improvement in terms of lowering the number of successful intrusions (Stilgherrian, 2015).

3. Level 3 Communications and Cisco teamed up to shut down a major malicious network that targeted approximately 90,000 systems with the Angler Exploit Kit malware. Command and control servers were identified and shutdown, thereby denying the botnet operators $30 to $60 million a year in criminal proceeds from bank fraud and ransomware (Avery, 2015).

Nonetheless, the security of cyberspace is a problem domain where there are more questions than answers. As implied by the opening quotation, it is a challenge that is incredibly intellectually demanding. According to Geer (2015), a key reason is that "there is no real ability to perform controlled experiments, yet uncontrolled natural experiments are all round us all the time even though data quality from those natural experiments is constantly confounding the issue". These "uncontrolled natural experiments" are a reference to real-world impacts on an increasingly online interconnected global society of man and machines.

As this article will show, the threat environment is rife with challenges. However, with these challenges comes opportunity. In aiming for a goal of cybersafety, there is the possibility of profoundly increased productivity and creativity (Bailetti et al., 2014; Nagger, 2015). This perspective emphasizes cybersafety as an important ena-

Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

bler of a globally connected future society that functions at a different level and pace than today's world.

Within this broad domain, our perspective emphasizes the opportunities for Canada and similarly positioned countries to thrive in the future if they can earn leadership positions in securing cyberspace. In this journal, Bailetti and co-authors (2013) proposed a not-for-profit corporation – what became the VENUS Cybersecurity Corporation (venuscyber.com) – as an innovation engine to make Canada a global leader in cybersecurity. The overall system-level intent of this effort is to convert innovation into the following results: i) new knowledge jobs; ii) addressed gaps in cybersecurity R&D and in operational limitations; iii) new highly qualified people operating in the cybersecurity space; and iv) sustainable income for the operator of the innovation engine (Bailetti et al., 2013). The resulting effort expended to launch and operate the VENUS Cybersecurity Corporation has further informed our view on the nature of the problem and how to address the challenge in Canada, but there remain many issues to be resolved and many open problems to be addressed. In particular, through our contributions to the establishment of the VENUS Cybersecurity Corporation, we have learned that:

1. Industry leadership is lacking. Canada's Cyber Security Strategy (Government of Canada, 2010) has the stated goal "to protect critical infrastructure". This simply cannot be accomplished without the direct involvement of critical infrastructure industries. Sadly, although these industries must deal with cybersecurity issues, given that the potential negative impact on their bottom line is enormous, they have still not found a way to monetize these efforts, which are seen only as an expense as opposed to an investment opportunity, a market differentiator, or simply a de-risking investment to protect their brand.

2. Critical mass is lacking across all sectors. Because cybersecurity is a systemic problem, it can only be efficiently addressed through concerted efforts that involve the supply chain of this same critical infrastructure industry. It is a "weakest link in the chain" issue and individual vendors are not willing to invest unless they are explicitly compelled by mandatory standards, which do not exist. Compounding the issue, the government sector has not effectively facilitated an appropriate level of engagement from all sectors in a unified and coordinated way.

3. Securing cyberspace is a societal concern that has no easy or obvious solution. Like health, cybersecurity cannot be addressed and resolved once and for all. Unlike the health domain however society has simply not yet reached a level of consciousness where it decides to generate the policies required to create a global response that has a chance to potentially match the global risk.

There are other jurisdictions that have solved some of these concerns or at least are more advanced than Canada. For example, the United States has been able to leverage its vast research and development capacity, including a network of national labs, not-for-profits, and high-end academic research programs, to better address the breadth and depth of the challenge. The United Kingdom has just announced a national cybersecurity plan, which includes the establishment of a National Cyber Centre to provide "economic security, national security and the opportunity that comes to a country that provides that security" (Osborne, 2015), which builds upon their more mature research and innovation programs.

Based on these lessons, this article proposes to identify the key questions that can be answered by building intellectual and industrial capacity in a coordinated fashion and by better leveraging existing talent to secure cyberspace for the greater prosperity of all. We present our analysis within the Canadian context, although much of the discussion can apply to other countries.

First, we provide necessary background information about the challenges of the threat environment. Next, we describe the key drivers to securing cyberspace. Finally, we identify the key questions that will form the basis of an agenda for research and practice. Finally, we offer conclusions.

Background: Challenges in the Threat Environment

Keeping pace with the constantly evolving cyber-threat landscape is a daunting task. This is coupled with the fact that IT security systems and architectures, everywhere, are being tasked to perform in ways they were never intended to operate. Specifically, the Internet is a complex globally distributed system that was initially designed for maximizing connectivity with very little thought about security. Geer (2015) highlights that "the security of cyberspace means responding to sentient opponents", while Wechsler (2015) argues that securing cyberspace is first and foremost about all-encompassing recognition to detect cyberspace intrusions that are adversarial in nature. The key point is that, in

Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

the face of sophisticated adversarial threats, the world simply does not know how to secure cyberspace.

With this context in mind, we identify a set of seven observations based on practical knowledge of both the threat environment and state-of-the art cyber-defence countermeasures, gained during our professional work and contributions to the establishment of the VENUS Cybersecurity Corporation:

1. Tractable network defence postures focus on understanding the interaction/correlation of both internal and external network behaviours: modelling the Internet at an enterprise network edge is not a tractable security approach. Recent cyber-threats have shown that even state-of-the-art commercial security products are not sufficient to block intrusion attempts from sophisticated threat actors referred to colloquially as advanced persistent threats (APT). Well-financed criminal enterprises and nation states with modest budgets can purchase, configure, and automate malware detection test suites comprised of the latest ant-virus software, personal security products (PSPs), firewalls, etc. To rise to the challenge, we must expect that the adversary has a copy of the commercial product(s) we employ to defend our networks for their own in-house malware testing and adapt our defensive tactics accordingly.

2. Detection techniques must have the necessary fidelity to enable non-human-in-the-loop automated defences. Current intrusion detection approaches are flawed because they focus on incoming network traffic looking for malicious behaviour. The issue with this approach is that the volume, velocity, and variety of Internet traffic are increasing at an exponential rate – the current coping strategy is bound to fail. Couple this with the fact that novel intrusions can exploit publically unknown vulnerabilities (i.e., zero-day exploits) and thus have no observable a priori pattern. More effort is needed to exploit the temporal advantage enjoyed by the network defender (e.g., observation of subtle changes in the network using network/host baselines over time) to develop techniques to observe abnormal lateral networks movements and command and control (C&C) patterns within the network.

3. The threat landscape has outpaced our quantification of the threat – sophisticated exploits are becoming democratized while sophisticated threat actors are interested in low value information and compute resources. We must address the negative causal link between false positives and false negatives (i.e., the fidelity of detection has to improve to a point where sophisticated automated defensive actions are the norm). Generating an "incident report" or requiring an analyst to investigate a suspected intrusion is akin to "admiring the problem". Although the initial suspected infected system may be identified and remediated, other systems inside the network may now also be compromised (e.g., lateral adversarial movements in the network to establish persistence). "Time to action" must be minimized by identifying and eliminating (where possible) human-in-the-loop decisions/bottlenecks/transforms. The work force is finite; acceleration of the analytic workflow needs to be leveraged by using systems/processes that are scalable and repeatable.

4. A state-of-the-art network defence posture must borrow from an attacker's playbook and invoke a "weird machine" paradigm, for example, a heterogeneous deployment of commercial products or non-standard deployments to enable a non-standard and thus "best of breed" detection approach. Traditional threat risk assessments (TRAs) are broken. Standard TRA methodologies typically underestimate the threat and, although the process serves to indicate some measure of due diligence has been taken to assess the network security posture, it can amount to a form of "security theatre". Recent high-profile attacks have shown us that: i) sophisticated adversaries are interested in "low value information"; ii) sophisticated exploit tools/frameworks are widely promulgated at no or low cost, thus removing the requirement of high technical skill as a barrier to entry; and iii) outsourcing of vulnerabilities research means that zero-day exploits are commoditized and available for sale.

5. Convergence of IT and OT networks has exposed critical components to a wide range of cyber-threats that are not traditionally monitored by IT staff and existing cybersecurity technologies. With increased Internet connectivity and the advent of the industrial Internet, physical systems are increasingly being targeted by cyber-attacks. The critical infrastructure that underpins our society, such as electric and water utilities, manufacturers, and oil and gas operators all use industrial control systems (ICSs) to support these industrial processes. Perhaps the most prevalent ICS is SCADA (i.e., supervisory control and data acquisition). ICS/SCADA systems are part of the OT networks comprised of electromagnetic systems (i.e., physical

Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

systems) that were designed to operate in an environment largely separate from conventional IT networks (i.e., cyberspace). These converged IT/OT networks are now being connected to the Internet (directly or indirectly through corporate networks), thereby increasing their exposure to a wide range of cyber-threats. This is coupled with the fact that OT networks are not traditionally monitored by IT security staff and existing cybersecurity technologies. As a result, the merging of the cyber-physical networks has been done in an ad hoc manner with very little thought about inherent vulnerabilities, secure network topologies, and state-of-the-art protection mechanisms.

6. Access to highly qualified personnel (HQP) is limited and significant training and experience is required to transform new recruits into cybersecurity professionals. In fact, the need for seasoned, well-trained cybersecurity researchers and professionals has outpaced supply: over the last five years, the demand for cybersecurity professionals has grown approximately 3.5 times faster than demand for other IT positions (Burning Glass, 2015). One might argue that this skills gap could be addressed by using a transdisciplinary approach to hiring by targeting individuals with a high degree of technical aptitude and "trainability" versus the requirement for a STEM background. However, this approach would not obviate the time delay caused by the significant amount of training and practical experience required to transform a new recruit into a cybersecurity professional.

7. The profound lack of shared meaningful data sets limits the repeatability and reproducibility of experimental results for new cybersecurity tools and techniques. Cybersecurity researchers are often relegated to using data sets obtained from lab or synthetically manufactured datasets that skew the experimental outcomes as a result of having a lack of naturally occurring abnormal network behaviour, or *crud,* that is regularly seen in real networks (Paxson, 1999). Conversely, some researchers have the advantage of having access to large "real world" networks for testing but due to privacy and legal concerns cannot share the data with the broader community. A balance has to be struck between privacy concerns and the lack of available curated datasets.

Key Drivers to Securing Cyberspace

When assessing the need for anticipatory intelligence, O'Connell (2015) suggests that "analysis will deepen decision-maker understanding of what is *driving* an issue so as to better and more deliberately prepare for it". When assessing the nature of the challenge of securing cyberspace, we identified three key drivers:

1. Complexity of the problem space

2. Accelerated pace of change

3. Finite internal capacity

Key driver 1: Complexity of the problem space
The first key driver to securing cyberspace is the complexity of the problem domain (Geer, 2015; Wechsler, 2015), which is illustrated by the nature of the challenges in the threat environment, as described in the previous section. Geer (2015) notes the possibility of introducing irreversible and unintended effects that are permanently incompatible with fundamental values when responding to sentient opponents. To accommodate these kinds of concerns, Douba and colleagues (2014) introduced a weak transdisciplinary framework that explicitly accommodates a value level (theology, ethics, and philosophy) along with normative (intent, risk-based decision making), capacity (technical disciplines), and empirical (real-time manifestation of phenomena) levels when contemplating the nature of "cybersafety of the online world of the future".

Key driver 2: Accelerated pace of change
The second key driver is the exponentially increasing rate of scientific and technological change. Using a retrospective analysis, Urban (2015) provides a convincing description of the Law of Accelerating Returns – the informal law that advances are becoming bigger and bigger and happening more and more quickly. Urban (2015) directly conveys how fast things will change in the future: "All in all, because of the Law of Accelerating Returns, [Ray] Kurzweil believes that the 21st century will achieve 1,000 times the progress of the 20th century." Assuming that a weak transdisciplinary framework is useful when representing and analyzing the problem domain, we argue that it is important to introduce the increasing rate of change to the framework. The value level may change more slowly than the capacity or empirical levels but a deeper understanding of securing cyberspace may mean a deeper understanding of how the different levels of the framework interact given that change happens faster at different levels.

Key driver 3: Finite internal capacity
The third key driver is a recognition that any individual, organizational, national, or even global initiative will

Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

have limited resources to make cyberspace secure, whether the resources are people, money, infrastructure, and so on. In terms of the transdisciplinary framework introduced by Douba and colleagues (2014), this driver primarily manifests itself at the capacity and empirical levels, but there would clearly be manifestations at the value and normative levels too. Society needs the higher levels of the model to provide guiding principles as opposed to constantly lagging behind and reacting to technological innovation. In general, there is also an important interplay with the second key driver, because one of the characteristics of the accelerated pace of change is the potentially exponential ability to do more with less or to accomplish previous, or new tasks, in completely new ways in response to limited resources.

Focus Areas and Key Questions

In our judgement, although each driver is distinct, these three drivers together represent the primary forces that drive an organizational, national, or global strategy that intends to address the challenge of making cyberspace safer. In contrast with the current state of affairs, which is comprised of many disconnected cybersecurity research and practice agendas, we advocate an approach that provides a unified response to these primary forces.

For Canada, we believe attention should be given to three focus areas, one per driver, to further secure cyberspace in a manner that is to Canada's advantage. For each focus area, we also identify the outstanding questions that, if answered, could allow a nation such as Canada to earn a global leadership position in securing cyberspace. Although the security of cyberspace is a problem domain where there are more questions than answers, this article presents "the big questions" that should be addressed first.

1. Focus on establishing a deep understanding of securing cyberspace by engaging the right brain on the right problem at the right time. This focus area should leverage Canada's existing cadre of highly qualified experts, important relationships, and a unique society that is attractive to external expertise. However, there is currently a lack of coherent long-term vision (which anticipates the evolution of the problem domain) and a lack of internal expertise to engage external experts (due to the breadth and complexity of the domain or an inability to establish local expertise in a timely fashion). Thus, our key "big questions" in this focus area are:

   - *What is an appropriate knowledge and learning framework to address the challenge of securing cyberspace?*
   - *What is the best way to make systematic breakthroughs?*
   - *How can Canada best leverage its limited human capital and also improve the productivity of this limited resource?*

2. Focus on "surfing the wave of change" by understanding what kind of change must happen and adapting constantly to secure cyberspace. Currently, Canada is not recognized as a global centre of innovation nor is it considered to be at the forefront of science and technology. Because of a poor strategic position, there is a danger Canada will be overwhelmed by the force of accelerating global change. However, given the opportunity to ride the wave of change to gain competitive advantage, Canada's relatively sophisticated but small-scale society means it has the structural make-up to support agility – there is the real possibility that Canada has the acumen to understand what kind of change must happen and to enact change. The implication is Canada will become more and more prosperous by harnessing specific scientific and technological breakthroughs in a timely fashion. Thus, our key "big questions" in this focus area are:

   - *What is the best way to understand what kind of change must happen?*
   - *What is the best way to keep pace?*
   - *What is the best way to adapt to change that must happen?*

3. Focus on leading global initiatives that are significant to enhancing Canadian expertise and capacity to secure cyberspace. In our view, Canada is currently too constrained by rigid management processes, organizational boundaries, and budgets to coordinate public, private, academic, and non-governmental sectors. However, Canada does have world-class practical cyber-expertise that could evolve to lead global initiatives that are significant to securing cyberspace to Canada's advantage. If Canada can lead or leverage external initiatives while augmenting its internal expertise and capability, it can make a greater impact within the globally connected world of the future and effectively address the challenge of securing cyberspace to its advantage. Thus, our key "big questions" in this focus area are:

Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

- *What is the best way to indirectly scale Canada's limited resources?*
- *What is the best way to directly extend or augment Canada's finite capacity?*
- *What is the best way for Canada to establish credibility and have influence on a global scale?*

The challenge of securing cyberspace is perhaps never-ending and it is certainly daunting. However, we believe that progress can be made using an approach that features sustained vigilance and adaptable tools, which are as important as the tactical fixes that currently dominate the domain. Our intention here is for these focus areas and questions to become a starting point in developing an agenda for research and practice to secure cyberspace.

Through our involvement with the VENUS Cybersecurity Corporation, we are taking some early steps in this direction. As an ecosystem-based initiative, VENUS has to date established a network of core expertise that will incrementally grow to address the transdisciplinary nature of the challenge as understanding deepens. To this end, groundwork is being done to establish an open source foundry to enable the deployment of state-of-the-art capability for securing cyberspace. Interworking arrangements are being established with critical infrastructure providers to address the hardest cybersecurity concerns. Finally, initial partnerships are established or being established with important research and innovation organizations in the United States and the United Kingdom to collaborate with the right brains at the right time on the right problems.

Conclusion

The security, robustness, and stability of our access to electronic information and services are keystone requirements for sovereign economies. Without this assurance, nations are unable to effectively conduct business, deliver goods and services, and ensure uninterrupted operations in the global marketplace. An important assertion is that the challenge of securing cyberspace transcends the abilities of any single entity and requires a radical shift in our approach in how: i) research is conducted, ii) cybersecurity researchers are educated, iii) new defendable systems are developed, and iv) effective defensive countermeasures are deployed.

Accordingly, this article shared and built upon lessons learned from attempting to establish a not-for-profit corporation as an innovation engine to make Canada a global leader in cybersecurity: the VENUS Cybersecurity Corporation. We learned that industry leadership is lacking, critical mass is lacking across all sectors, and securing cyberspace is a societal concern that has no easy or obvious solution. With this context in mind, we identified a set of seven observations based on practical knowledge of both the threat environment and state-of-the-art cyber-defence countermeasures. We determined, at the heart of the problem, there are three key drivers: the complexity of the problem space, an accelerated pace of change and finite internal capacity. Three focus areas and associated questions were then identified to form the foundation of an agenda for research and practice to secure cyberspace.

In Canada, our view is that the status quo is represented by an overly insular Canadian society that attempts to independently "solve" the challenge of securing cyberspace on its own. However, there is an opportunity for Canada to play a leading role in securing cyberspace by engaging with external expertise and capacity using a transdisciplinary, ecosystem approach. By playing a leading role in securing cyberspace, we believe that Canada would benefit by attracting investment, creating high-value jobs, ensuring economic growth, encouraging companies to establish and grow, strengthening supply chains, developing industrial capabilities, fostering innovation and fostering success in export markets as cyberspace is better secured for the benefit of society as a whole. Through building intellectual and industrial capacity in a coordinated fashion, existing talent will be better leveraged and new talent will grow in a manner that enables Canada to gain a leadership position in securing cyberspace. Beyond the Canadian context, there is a need for global contributions to address the key questions identified here so we can better secure and shape the online world of the future.

Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

About the Authors

Renaud Levesque is the Director General of Core Systems at the Communications Security Establishment (CSE) in Ottawa, Canada, where he is responsible for R&D and systems development. He has significant experience in the delivery of capability and organizational change in highly technical environments. His career began at CSE in 1986 as a Systems Engineer, responsible for the development and deployment of numerous systems, including the CSE IP corporate network in 1991. In 2000 Renaud went to work in the private sector as Head of Speech Technologies at Locus Dialogue, and later at Infospace Inc., where he became Director of Speech Solutions Engineering. He rejoined CSE in 2003, where he assumed the lead role in the IT R&D section. Subsequently, as a Director General, he focused efforts towards the emergence of CSE's Joint Research Office and The Tutte Institute for Mathematics and Computing. Renaud holds a Bachelor of Engineering from l'École Polytechnique, Université de Montréal, Canada.

D'Arcy Walsh is a Science Advisor at the Communications Security Establishment (CSE) in Ottawa, Canada. His research interests include software-engineering methods and techniques that support the development and deployment of dynamic systems, including dynamic languages, dynamic configuration, context-aware systems, and autonomic and autonomous systems. He received his BAH from Queen's University in Kingston, Canada, and he received his BCS, his MCS, and his PhD in Computer Science from Carleton University in Ottawa, Canada.

David Whyte is the Technical Director for the Cyber Defence Branch at the Communications Security Establishment (CSE) in Ottawa, Canada. He is CSE's technical lead responsible for overseeing the implementation of the next-generation cyberthreat-detection services for the Government of Canada. He has held many positions over the last 16 years within CSE that span both the Signals Intelligence and Information Technology Security mission lines. David holds a PhD in Computer Science from Carleton University in Ottawa, Canada. The main focus of his research is on the development of network-based behavioural analysis techniques for the detection of rapidly propagating malware.

References

Avery, G. 2015. Level 3, Cisco Take Down Major Cybercrime Network. *Denver Business Journal,* October 6, 2015. Accessed November 1, 2015: http://www.bizjournals.com/denver/blog/boosters_bits/2015/10/level-3-cisco-take-down-major-cybercrime-network.html

Bailetti, T., Craigen, D., Hudson, D., Levesque, R., McKeen, S., & Walsh, D'A. 2013. Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity. *Technology Innovation Management Review,* 3(8): 5–14. http://timreview.ca/article/711

Bailleti, T., Levesque, R., & Walsh, D'A. 2014. The Online World of the Future: Safe, Productive, and Creative. *Technology Innovation Management Review,* 4(10): 5–12. http://timreview.ca/article/834

Bronk, C., & Tink-Ringas. E. 2013. The Cyber Attack on Saudi Aramco. *Survival: Global Politics and Strategy,* 55(2): 81–96.

Burning Glass. 2015. *Job Market Intelligence: Cybersecurity Jobs, 2015.* Boston, MA: Burning Glass Technologies.

Dawda, U. 2014. DecryptCryptoLocker – A Success Story. *FireEye Executive Perspective,* September 4, 2014. Accessed November 1, 2015: https://www.fireeye.com/blog/executive-perspective/2014/09/decryptcryptolocker-a-success-story.html

Douba, N., Rütten, B., Scheidl, D., Soble, P., & Walsh, D'A. 2014. Safety in the Online World of the Future. *Technology Innovation Management Review,* 4(11): 41–48. http://timreview.ca/article/849

Geer, D. 2015. Six Key Areas of Investment for the Science of Cyber Security. *The Futurist,* 49(1): 10–15.

Government of Canada. 2010. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada.* Ottawa: Government of Canada.

HP. 2014. *Internet of Things State of the Union Study.* Palo Alto, CA: Hewlett Packard.

Langer, R. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy,* 9(3): 49–51. http://dx.doi.org/10.1109/MSP.2011.67

Macaulay, J., Buckalew, L., & Chung, G. 2015. *Internet of Things in Logistics.* Troisdorf, Germany: DHL Trend Research and Cisco Consulting Services.

Naggar, R. 2015. The Creativity Canvas: A Business Model for Knowledge and Idea Management. *Technology Innovation Management Review,* 5(7): 50–58. http://timreview.ca/article/914

O'Connell, K., & Klubes, D. 2015. *Anticipation: A Top U.S. National Security Priority for 2015.* Washington, DC: Innovative Analytics.

Osborne, G. 2015. Chancellor's Speech to GCHQ on Cyber Security. *Her Majesty's Treasury, Government Communications Headquarters,* November 17, 2015. Accessed November 18, 2015: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

Securing Cyberspace: Towards an Agenda for Research and Practice

Renaud Levesque, D'Arcy Walsh, and David Whyte

Paxson, V. 1999. Bro: A System for Detecting Network Intruders in Real-Time. *Computer Networks,* 31(23-24): 2435–2463. http://dx.doi.org/10.1016/S1389-1286(99)00112-7

Robertson, J., & Riley, M. 2014. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar. *Bloomberg Business,* December 10, 2014. Accessed November 1, 2015: http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

Stilgherrian. 2015. Australia's Cyber Defence 'Pretty Ordinary' before ASD's Top Four. *ZDNet,* June 2, 2015. Accessed November 1, 2015: http://www.zdnet.com/article/australias-cyber-defence-pretty-ordinary-before-asds-top-four/

Urban, T. 2015. The AI Revolution: The Road to Superintelligence. *Wait But Why,* January 22, 2015. Accessed November 1, 2015: http://waitbutwhy.com/2015/01/artificial-intelligence-revolution-1.html

Wechsler, H. 2015. Cyberspace Security using Adversarial Learning and Conformal Prediction. *Intelligent Information Management,* 7(4): 195–222. http://dx.doi.org/10.4236/iim.2015.74016

Zetter, K. 2015. A CyberAttack has Caused Confirmed Physical Damage for the Second Time Ever. *Wired Magazine,* January 8, 2015. Accessed November 1, 2015: http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

Citation: Levesque, R., Walsh, D'A., & Whyte, D. 2015. Securing Cyberspace: Towards an Agenda for Research and Practice. *Technology Innovation Management Review*, 5(11): 26–34. http://timreview.ca/article/943

Keywords: cybersecurity, cyber security, security, cybersafety, cyberspace, challenges, detection, mitigation, countermeasures, Internet of Things, research, leadership, Canada