Securing Canada’s Information-Technology Infrastructure: Context, Principles, and Focus Areas of Cybersecurity Research

Dan Craigen, D’Arcy Walsh, and David Whyte

> “*I don’t want to make the wrong mistake.*”
>
> Lawrence (Yogi) Berra
> Major League Baseball player and manager

This article addresses the challenges of cybersecurity and ultimately the provision of a stable and resilient information-technology infrastructure for Canada and, more broadly, the world. We describe the context of current cybersecurity challenges by synthesizing key source material whose importance was informed by our own real-world experiences. Furthermore, we present a checklist of guiding principles to a unified response, complete with a set of action-oriented research topics that are linked to known operational limitations. The focus areas are used to drive the formulation of a unified and relevant research and experimental development program, thereby moving us towards a stable and resilient cyber-infrastructure. When cybersecurity is viewed as an inherently interdisciplinary problem of societal concern, we expect that fundamentally new research perspectives will emerge in direct response to domain-specific protection requirements for information-technology infrastructure. Purely technical responses to cybersecurity challenges will be inadequate because human factors are an inherent aspect of the problem.

This article will interest managers and entrepreneurs. Senior management teams can assess new technical developments and product releases to fortify their current security solutions, while entrepreneurs can harness new opportunities to commercialize novel technology to solve a high-impact cybersecurity problem.

Introduction

The explosive growth, complexity, adoption, and dynamism of cyberspace that have enhanced social interaction and expanded our ability to productively utilize our environment have also introduced new adversarial threats and challenges to the institutions and individuals that make up our society. Ongoing threats to our critical infrastructure have resulted in substantial loss of competitive advantage and have deleteriously impacted our way of life. Cyberbullying, cybercrime, cyberterrorism, and adversarial state-sponsored activities are all examples of malevolent attributes of cyberspace. Mitigating these malevolent attributes requires an agile, legal and ethically compliant, interdisciplinary and scientifically based research and exploratory development program in cybersecurity.

The overall cybersecurity research challenge resides within a particularly complex area, being at the intersection of behavioural sciences, formal sciences, and the natural sciences. The significant adversarial component of cyberspace has led to a view that the science of cybersecurity is a science that must support reasoning about adversaries, the core components being operations research, cybernetics, and game theory. Consistent with this perspective are “nature inspired” approaches that draw upon analogies arising from immunological and biological systems. Other areas that could usefully inform a science of cybersecurity include cryptography, formal reasoning, machine learning, and composition. Our core tenant is that the cybersecurity challenge is inherently interdisciplinary and demands coordinated attention from new perspectives for the public good.

In response to Canada's Cybersecurity Strategy (2010; tinyurl.com/md7qchf), we published a report in May 2013 for the Communications Security Establishment Canada (CSEC; cse-cst.gc.ca). Our report (Craigen et al., 2013; tinyurl.com/k6khgr6), upon which this article is based, described what is required to establish a secure, stable, and resilient information-technology infrastructure. Informed by national and international strategies, roadmaps, and problem books, we presented a research context for investigating the cybersecurity challenge. In addition, we formulated a set of guiding principles to ensure the cybersecurity research program addresses the desired improvements, outcomes, and guidance stated in Canada's Cybersecurity Strategy. Constrained by the context, and satisfying the principles, we then described the specific research focus areas. Although we were specifically responding to Canada's Cybersecurity Strategy, it is our view that the context, guidelines, and focus areas are of global consequence.

Addressing the inherently interdisciplinary challenge of cybersecurity and ultimately establishing a secure, stable, and resilient information-technology infrastructure for Canada and, potentially, the world, should also be of direct interest to managers and entrepreneurs. Being a consumer or producer of enhanced cybersecurity capability presents emerging business opportunities and demands state-of-the-art management methods to ensure a diverse ecosystem is coordinated in manner that progressively addresses operational limitations and builds wealth for the collective good.

Beyond research and experimental development, we believe the context, principles, and research focus areas presented in this article are also a useful starting point for assessing and evolving management regimes that will be required to address the challenge. We also believe the material is a useful orientation for identifying new business opportunities that will arise as new interdisciplinary perspectives related to cybersecurity are better understood.

The main body of this article is composed of three complementary sections. The first section provides a summary of related work and a description of a research context for cybersecurity in order to scope the problem domain. The second section articulates a set of guiding principles that inform the nature and kinds of specific research initiatives that should be pursued. The third section identifies particular focus areas for research and experimental development that are linked to operational limitations. Note that the core components of this article (i.e., the three complementary sections) essentially capture the current contextual state within which the nine focus areas are derived and presented. The guiding principles provide suggestions on how to progress the focus areas in a productive, action-oriented manner. Finally, the conclusion summarizes important key considerations going forward when addressing the interdisciplinary cybersecurity challenge as a whole.

Given the dynamic attributes of cyberspace, we take the perspective that the focus areas will need to be updated as circumstances warrant. Through the sharing of the focus areas we hope to generate an ongoing discussion about how to achieve the end state of a secure, stable, and resilient information-technology infrastructure.

Context of Cybersecurity Research

In this section, we provide a concise and selective literature review of the material we used to set the context for establishing an appropriate and relevant research program that addresses challenges that are: i) specific to cybersecurity or ii) shared with other domains, but of particular relevance to the cybersecurity domain. In our opinion, the referenced material provides a well-considered and useful description of the cybersecurity domain.

Recent work by Mulligan and Schneider (2001; tinyurl.com/kt3f3gq) presents the view that cybersecurity should be considered as a public good. Using public health as an example, the notion of "public cybersecurity" is articulated. This is important contextually because new policy and new institutions are implied. Exploring the shift from public health to public cybersecurity, Mulligan and Schneider also provide illustrative examples that are useful for evaluating the nature of the cybersecurity domain as enlightened from this new viewpoint.

From a scientific perspective, the material is also well founded with respect to emerging research focused on the grand challenge of establishing a "science of (cyber)security" (e.g., TRUST: truststc.org; McMorrow, 2010: tinyurl.com/35h74h6; Science of Security Workshop, 2008: sos.cs.virginia.edu; U.S. Department of Homeland Security, 2009: tinyurl.com/y98ohjr). Papers by Denning (1976; tinyurl.com/l8qxamp) and Harrison and colleagues (1976; tinyurl.com/ltnzfoe) are early examples of research that would advance a science of cybersecurity. Through discussion of classes of attacks, policies, and defenses, Schneider (2012; tinyurl.com/luj9pau) references the importance of building upon existing knowledge, particularly formal methods, fault-tolerance, and experimental computer science but Schneider also acknowledges the importance of cryptography, information theory, and game theory. Interestingly, based on safety ("no bad thing") and liveness ("some 'good thing' happens"), Schneider (2012; tinyurl.com/luj9pau) and McMorrow (2010; tinyurl.com/35h74h6) suggest new techniques to express and validate security policy requirements as part of the emerging science of cybersecurity.

With a focus on technical measures for blocking cyberattacks, a U.S. Department of Homeland Security (DHS) report (2011; tinyurl.com/65udd87) adopts the human immune system as a metaphor to motivate the need for automated collective action amongst distributed systems to defend individual computers and networks. The DHS report identifies automation, interoperability, and authentication as the building blocks that underpin a five-level focus and convergence maturity model for networked environments. The DHS also describes the attributes and desired end state of a healthy cyber ecosystem (including participants within the ecosystem).

There is also clearly a strong connection between cybersecurity research and ongoing investigations concerning security analytics and measurements (Cybenko and Landwehr, 2012: tinyurl.com/kc3nm7p; Yee, 2012: tinyurl.com/lokvcs8). As stated by George Cybenko, the founding Editor-in-Chief of *IEEE Security and Privacy* and his first successor, Carl E. Landwehr, "Accordingly, we won't find the appropriate science for understanding the evolving cybersecurity landscape in the logic of formal systems or new software engineering techniques; it's an emerging subarea of game theory that investigates dynamics in adversarial situations and the biases of competing human agents that drive those dynamics." Based upon game theory, partially observable Markov decision processes and other techniques, Carin and colleagues (2007; tinyurl.com/mkf7fyw) describe a computational approach to the quantitative cybersecurity risk assessment of intellectual property in complex systems – we believe this methodology could be augmented/generalized to also address critical infrastructure protection.

Finally, from the perspective of "Reducing Systemic Cybersecurity Risk", Sommer and Brown (2011; tinyurl.com/l2nbn5r) suggest that research responses should adopt a cross-disciplinary approach that combines "hard computer science" with the need to understand social science dimensions because "information system security are achieved only by a fusion of technology and the ways in which people and organizations actually try to deploy them". Further, Dave McMahon and Rafal Rohozinski (Bell Canada and the Secdev Group: "Dark Space Report", December 2012) state that, "Current approaches to cybersecurity are ill-suited to detecting or anticipating threats, which increasingly rely on hybrid socio-technical vectors." An example of a hybrid socio-technical vector would be phishing attacks – they have a technical component, but use sociological/psychological means to induce a user to invoke malware. McMahon and Rohozinski further suggest that, "By identifying and understanding the threat agents as threats themselves, instead of only the technology as threats, we can understand and neutralize other threats before they are created".

In this section, we have provided a context for our establishing an appropriate and relevant cybersecurity research program. Next, informed by the context, a set of guiding principles is presented for responding to the cybersecurity challenge in a productive action-oriented manner.

Principles of Cybersecurity Research

This section summarizes a set of 13 guiding principles of cybersecurity research. How was this particular set of principles determined? Firstly, the IT-security best practices (tinyurl.com/l42xht7) promulgated by our organization, the CSEC, were used as a baseline to validate these principles, as they were determined. Secondly, each principle was linked to at least one key information source first cited in the research context description. These sources are produced by recognized subject matter experts and provide more detailed explanatory material. Finally, the principles were appraised collectively as a concise but comprehensive set of principles that are anchored in a careful estimation of our own experiences, baseline best practices, the context, and ongoing engagement with cybersecurity stakeholders. The principles also provide a starting point for deliberating about the multi-dimensionality of the problem domain and its interdisciplinary nature.

The following are the guiding principles we have identified:

1. Coordinate research activities to systematically progress towards achieving the attributes and desired end state of a healthy cyberecosystem (including participants within the system) (DHS, 2011; tinyurl.com/65udd87).

2. Engage social-science research labs to understand the social-science dimensions of cybersecurity, thereby augmenting "hard", computer science research (Mulligan and Schneider, 2001: tinyurl.com/kt3f3gq; Sommer and Brown, 2011: tinyurl.com/l2nbn5r).

3. Focus research on promising scientific approaches that comprehensively and rigorously underpin required security policy (Schneider, 2012: tinyurl.com/luj9pau; McMorrow, 2010: tinyurl.com/35h74h6).

4. Focus research on promising scientific approaches that comprehensively and rigorously underpin the quantitative cybersecurity risk assessment of complex systems (especially critical infrastructure) (Cybenko and Landwehr, 2012: tinyurl.com/kc3nm7p; Carin et al., 2007: tinyurl.com/mkf7fyw).

5. Focus research on promising scientific approaches to automate collective action amongst distributed systems to defend individual computers and networks (DHS, 2011; tinyurl.com/65udd87).

6. Focus on research that incorporates adversaries in models and analyses of cyberspace (McMorrow, 2010; tinyurl.com/35h74h6).

7. Engage research labs to investigate cybersecurity-related research gaps and to de-risk scientific approaches and emerging technological solutions (Schneider, 2012: tinyurl.com/luj9pau; McMorrow, 2010: tinyurl.com/35h74h6; Science of Security Workshop, 2008: sos.cs.virginia.edu; DHS, 2009: tinyurl.com/y98ohjr).

8. Leverage and influence cybersecurity-related maturity models and standards when investigating difficult problems (DHS, 2011; tinyurl.com/65udd87).

9. Build upon existing knowledge that is relevant to cybersecurity (McMorrow, 2010: tinyurl.com/35h74h6; Science of Security Workshop, 2008: sos.cs.virginia.edu; DHS, 2009: tinyurl.com/y98ohjr).

10. Leverage research that addresses the challenges of "big data" as well as domain-specific challenges (U.S. Office of Science and Technology, 2012: tinyurl.com/l2pucpt; PREDICT: predict.org).

11. Leverage research that addresses the question: "What does a data scientist do? " (IBM InfoSphere; tinyurl.com/bwupcuh)

12. Leverage existing knowledge regarding ways of working, as discussed in our full report (Craigen et al., 2013; tinyurl.com/k6khgr6).

13. Carefully address the myriad of considerations (such as those pertaining to ethics) that influence and are influenced by cybersecurity (Menlo Report, 2011; tinyurl.com/mk9b44a).

In this section, we summarized a set of 13 guiding principles of cybersecurity research. In the next section, we present the focus areas of cybersecurity research that are constrained by the context outlined in the previous section and satisfy the principles outlined above.

Focus Areas of Cybersecurity Research

The following sub-sections describe nine focus areas for cybersecurity research. To identify these focus areas, the authors assessed key research-program descriptions related to cybersecurity, which we used as a baseline to validate each focus area. Next, based upon our own expertise and experience, we ensured that each focus area corresponds to operational limitations. Finally, the focus areas were appraised by organizational stakeholders as a concise but comprehensive set of focus areas that are anchored in a careful estimation of our own experiences and ongoing engagement with cybersecurity stakeholders. Further details and a more complete list of challenges and research topics, can be found in our full report to the CSEC (Craigen et al., 2013; tinyurl.com/k6khgr6). In the sub-sections that follow, we briefly describe each of these nine focus areas as action-oriented statements accompanied with a short explanation and example challenges.

1. Improve the management and quality of signatures
A signature is a distillation of a pre-configured malicious pattern. Signatures are widely used, for example, to tersely identify cyberthreats and thereby identify and detect the activity of known malicious networks and hosts (e.g., viruses). Challenges include prioritization

and arbitration of generated events from computer network operations, false-positive reduction, and automated signature generation based on a corpus of data. Responding to the challenges will improve the detection, quality, effectiveness, complexity, fidelity, and timeliness of signature-based techniques.

2. Increase effort on anomaly detection and support discovery of new threats
Anomaly detection refers to activity that does not conform to expected behaviour or usage patterns. From a cybersecurity perspective, for example, anomalous traffic patterns in a network could suggest that a system has been penetrated and sensitive data is being exfiltrated. Challenges include specification-based intrusion techniques, data mining to support anomaly-based detection hypotheses, and mimicry-attack detection. Responding to the challenges will target new areas where anomaly detection and discovery can be explored (e.g., protocol semantics, applied mathematics, statistics, machine learning), coupled with novel techniques to minimize post-detection analysis requirements, etc., thus materially improving this field.

3. Reduce time to action through streaming and event-driven analytics
Streaming analytics refers to the inline analysis of data (e.g., Internet protocol packets, stock trades, currency trading, health monitoring) to rapidly and intelligently respond to evolving situations, potentially in near real-time. There is a spectrum of algorithms, ranging from near real-time algorithms supporting almost instant response to adversarial situations, through to longer-term algorithms that require an almost forensics-like, perspective. Identifying this algorithmic taxonomy is a research challenge in its own right. Example challenges include automated, machine-driven signature detection and near real-time correlation of events.

4. Provide dynamic defence at the network edge and beyond
A network edge is the location where the processing and enforcement of organizational policies commences. This challenging problem focuses on developing dynamic defence techniques that can rapidly interdict network attacks, using both network and host-based capabilities. The "end goal" for dynamic defence can, in fact, be two-fold: i) to mitigate the degree of damage attributed to a detected compromise by adapting the network or host environment in a timely fashion to actively resist or repel an ongoing attack, and ii) to ensure that mission-critical services are available to clients even when the network or hosts are under attack.

5. Investigate secure cloud-based systems including virtualization
Cloud computing is the delivery of computing resources over a network. Cloud computing brings challenges pertaining to scale, security, and privacy. Challenges arise from the evaluation, architecture, and design of such systems. Furthermore, there are specific concerns about contagion of malware infections across virtual instances and into the underlying base image. Virtualization is a key technology underpinning cloud computing. Accordingly, software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) present both attractive cost savings in addition to potential security concerns (e.g., separation of virtual machines, secure application programming interfaces, authentication, secure auditing, as well as multi-latency and hypervisor vulnerabilities).

6. Investigate secure supply chains
Commercial off-the-shelf (COTS) products are those products that are commercially available, leased, licensed, or sold and do not require specific maintenance/modification. COTS products tend to vary in quality, yet also evolve quicker and more usefully in response to broader market forces. The challenges pertain to evaluation, architecture, and design, identification of security requirements, and the specification of such systems. There is a significant challenge to scale system evaluation and design to mitigate threats arising from specific products. The supply chain is of particular concern with COTS products.

7. Investigate practical enterprise-level metrics
Enterprise-level metrics allow us to answer questions that are fundamental to investment and deployment decisions, such as: "How secure is my organization?" and "How has my security posture improved through the last set of updates?" To properly manage our systems, scientifically based metrics and measures are required. Any underpinning "science of cybersecurity" will require a family of justified measures and metrics. Currently, there are no universally agreed-upon methodologies to address the fundamental questions of how to quantify system security.

8. Investigate secure mobility (including wireless)
Mobile devices are trending towards ubiquity and there is a strong desire to use capabilities available at home within the workplace, as in "bring your own device" (tinyurl.com/k5mc7th). Mobility raises unique questions from the perspective of threat risk assessment and adds potential attack vectors due to the use of wireless and

other over-the-air communication mechanisms. Challenges pertaining to evaluation, architecture, and design, identification of security requirements, and the specification of such systems once again arise, although within a different context.

9. Continuously leverage research related to the science of cybersecurity
Here, science is viewed as knowledge that results in correct predictions or reliable outcomes. Successful progress on this capability gap will provide significant science-based foundations for our cybersecurity techniques, including a deeper understanding of the interdisciplinary nature of cybersecurity. Though there are sub-areas that are solidly grounded in mathematics (e.g., formal methods and cryptography), much of cybersecurity is based on pre-scientific reasoning. Nicol and colleagues (2012: tinyurl.com/m7ufltk) have identified five hard problems relating to the science of cybersecurity: i) scalability and composability; ii) policy-governed secure collaboration; iii) security-metrics-driven evaluation, design, development and deployment; iv) resilient architectures; and v) understanding and accounting for human behaviour.

These nine focus areas have been informed by our specific experiences, but also by other international research programs. The first four focus areas concern the detection, analysis, tracking, and mitigation of cyberthreats; the subsequent four focus areas concern the means to create trustworthy systems. The last focus area effectively underpins the previous eight by arguing for a science of cybersecurity. We believe that, together, these nine focus areas provide a grounded and useful starting point for establishing a mature and unified research program that effectively addresses the overall cybersecurity challenge.

Conclusion

Here and in our full report to the CSEC (Craigen et al., 2013; tinyurl.com/k6khgr6), we have described the major components of a cybersecurity research program to secure Canada's information-technology infrastructure. Other relevant considerations that are outside the scope of this article include legal and ethical concerns, required skill sets, methods of assessing progress in science, and technology transfer within the cybersecurity domain.

Making the cybersecurity research program public offers benefits to entrepreneurs and managers of existing organizations, both large and small. Entrepreneurs can use the information to identify and act upon gap-filling and disruptive opportunities for the purpose of creating wealth. Managers of existing organizations will be able to search for ways to reduce risk and answer a myriad of questions about how to reduce costs, increase revenue, and enable their organizations to do things they cannot do today.

Moving forward, what is an appropriate path to take, given that cybersecurity must be achieved for the public good and that the challenge itself transcends any one organization? Given the key considerations just mentioned and the interdisciplinary nature of cybersecurity, we hope to establish a not-for-profit institute to bring together cybersecurity venture stakeholders and fully integrate a national research and commercialization program. The research context, principles, and focus areas described in this article will form the basis of the institute's combined research and commercialization program. And, with the help of the institute, innovative companies will be launched to provide cybersecurity solutions that address domain-specific information-technology infrastructure protection requirements that have been identified by cybersecurity stakeholders who are part of the ecosystem. The instute will function as a state-of-the-art social enterprise, ensuring that priority requirements are addressed incrementally for the public good.

In this article, we have presented a collection of cybersecurity research focus areas. Although these focus areas are well-informed by our own expertise, experiences, research, and engagement with cybersecurity stakeholders, they should be viewed as a starting point for a unified cybersecurity research and experimental development program. Given the complex aspects of cybersecurity research – due to it residing in the intersection of behavioural sciences, formal sciences, and natural sciences – it is impossible for any one organization, no matter how well informed, to fully grasp the challenges and potential opportunities. We hope that, by publishing this article and the full report, a discussion will ensue within government, academia, and industry, leading to an evolving set of cybersecurity focus areas where discoveries will result in meaningful advances towards a stable and resilient information-technology infrastructure.

Context, Principles, and Focus Areas of Cybersecurity Research

Dan Craigen, D'Arcy Walsh, and David Whyte

About the Authors

Dan Craigen is a Science Advisor at the Communications Security Establishment Canada (CSEC). Previously, he was President of ORA Canada, a company that focused on High Assurance/Formal Methods and distributed its technology to over 60 countries. His research interests include formal methods, the science of cybersecurity, and technology transfer. He was the chair of two NATO research task groups pertaining to validation, verification, and certification of embedded systems and high-assurance technologies. He received his BScH in Math and his MSc in Math from Carleton University in Ottawa, Canada.

D'Arcy Walsh is a Science Advisor at the Communications Security Establishment Canada (CSEC). 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 Canada (CSEC). He is CSEC'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 CSEC 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.

Citation: Craigen, D., D. Walsh, and D. Whyte. 2013. Securing Canada's Information-Technology Infrastructure: Context, Principles, and Focus Areas of Cybersecurity Research. *Technology Innovation Management Review.* July 2013: 12–18.

Keywords: cybersecurity, cyberinfrastructure, cyberdefence, research, information-technology infrastructure, experimental development program, management, entrepreneurship, Canada