Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson,
Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

> *"There is one quality which one must possess to win, and that is definiteness of purpose, the knowledge of what one wants, and a burning desire to possess it.*
>
> Napoleon Hill (1883–1970)
> Writer and advisor to President Franklin D. Roosevelt

An engine designed to convert innovation into a country's global leadership position in a specific product market is examined in this article, using Canada and cybersecurity as an example. Five entities are core to the innovation engine: an ecosystem, a project community, an external community, a platform, and a corporation. The ecosystem is the focus of innovation in firm-specific factors that determine outcomes in global competition; the project community is the focus of innovation in research and development; and the external community is the focus of innovation in resources produced and used by economic actors that operate outside of the focal product market. Strategic intent, governance, resource flows, and organizational agreements bind the five entities together. Operating the innovation engine in Canada is expected to improve the level and quality of prosperity, security, and capacity of Canadians, increase the number of Canadian-based companies that successfully compete globally in cybersecurity product markets, and better protect Canada's critical infrastructure. Researchers interested in learning how to create, implement, improve, and grow innovation engines will find this article interesting. The article will also be of interest to senior management teams in industry and government, chief information and technology officers, social and policy analysts, academics, and individual citizens who wish to learn how to secure cyberspace.

Introduction

How can a country become a global leader in a product market and contribute to its own prosperity, security, and capacity? The objective of this article is to examine one response to this research question: the establishment of an engine (i.e., a structure, processes, and values) that converts innovation into system-level results (e.g., prosperity, security, and capacity) that cannot be delivered by a single organization or individual working on its own.

The innovation engine examined in this article cultivates innovation in: i) firm-specific advantages to compete globally; ii) research and development (R&D); and iii) linking with external communities. This engine converts innovation into four system-level 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.

We use the authors' experience and knowledge gained designing and growing business ecosystems to offer a generic approach to make a country a global leader in a specific product market. Table 1 list articles published in this journal since 2008, organized on the basis of the nature of their contribution to our understanding of innovation engines and their entities.

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

Table 1. Contributions that increased our understanding of innovation engines and their key entities

A. Innovation engines	
Engines to convert innovation into desired system-level results	Bailetti and Bot (2013; timreview.ca/article/658)
Models for innovation engines and business ecosystems	Muegge (2011; 495) Muegge (2013; 655) Quinn (2009; 279)
B. Business ecosystems	
Examples of how new technology ventures use business ecosystems to create value	Bailetti (2010; timreview.ca/article/355) Low and Muegge (2013; 703) Rosenblum (2010; 381)
Lessons learned building real-life business ecosystems	Dixon (2011; 441) Milinkovich (2008; 200)
Overview of business ecosystems and identification of distinguishing features	Carbone (2009; 227) Hurley (2009; 276)
Approaches to visualize characteristics of business ecosystems and their evolution	Weiss (2009; 242) Weiss, Sari, and Noori (2013; 683)
C. Projects in business ecosystems	
Examples of projects that co-create value in a business ecosystem	Bailetti and Hudson (2009; timreview.ca/article/308) Westerlund and Leminen (2011; 489) Weiss (2011a; 488) Weiss (2011b; 436)
D. Platforms	
Motivation to use a platform	Makienko (2010; timreview.ca/article/382)
Examples of platform operators and their strategies	Bailetti (2010; 377) Leminen, Westerlund, and Nyström (2012; 602) Mahendran (2008; 114) Majic (2010; 379) Misaka (2013; 684) Muegge and Milev (2009; 245) Noori and Weiss (2013; 647) O'Halloran (2010; 350) Poole (2010; 391) Poole (2011; 446)
E. Foundations	
Examples and characteristics of non-profit organizations that anchor business ecosystems	Prattico (2012; timreview.ca/article/636) Xie (2008; 194) Weiss (2010; 376)

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

We use the experience and knowledge gained protecting Canada's critical infrastructures and managing R&D portfolios (Craigen et al., 2013a: timreview.ca/article/704; Craigen et al., 2013b: timreview.ca/article/705) to use Canada and cybersecurity as an example of an application of the innovation engine.

Cyberattacks threaten and limit the benefits that Canadians, as well as citizens of other countries, currently derive from cyberspace. Cyberattacks include, but are not limited to, stealing intellectual property, disrupting critical infrastructure, usurping identity, compromising online bank accounts, creating and distributing viruses, posting confidential information, and encrypting systems to demand ransom. Increasingly, cyberattacks use sophisticated software designed to defeat or bypass security systems. These attacks are criminally or politically motivated, and are executed by very persistent, skilled, and well-funded individuals and organizations.

Cyberattacks that steal intellectual property and disrupt critical infrastructure are particularly damaging. Hard data on the extent of intellectual property theft are difficult to obtain and validate. According to the Canadian Labour Congress, intellectual property theft costs the Canadian economy $22 billion each year (Geist, 2009; tinyurl.com/ptmx2l5). Frontier Economics (2011; tinyurl.com/nauah4a), a research organization based in the United Kingdom, estimates that the theft of intellectual property prevents the world's 20 major economies from collecting €100 billion in tax revenues each year and has "destroyed" 2.5 million legitimate jobs. The Symantec Corporation estimated that companies in the United States lose some $250 billion to intellectual property theft every year; however, this figure has been questioned (Maass and Rajagopalan, 2012; tinyurl.com/c73fp6d).

Critical infrastructure consists of physical and information-technology assets such as energy distribution networks, telecommunications networks, banking systems, manufacturing and transportation systems, and services that support the effective functioning of the private and public sector. Examples of cyberattacks on critical infrastructure include: i) the cyberattacks on Estonia (Ottis, 2013; tinyurl.com/p3juxde) and Georgia (Korns and Kastenberg, 2009; tinyurl.com/oj5ok57); ii) the attack on the Saudi Arabian Oil Company (Bronk and Tikk-Ringas, 2013; tinyurl.com/pegavx8); and iii) brute force attacks on Internet-facing control systems (Industrial Control Systems Cyber Emergency Response Team, 2013; tinyurl.com/q98sqxf).

Cybersecurity will remain a rapidly evolving and significant challenge for the foreseeable future. Protecting cyberspace is a global as well as a domestic priority. There is a sense of urgency for industry, government, academic institutions, not-for-profits, and individuals to work together to ensure that Canadians and citizens of other nations enjoy a secure cyberspace (Auditor General of Canada, 2012; tinyurl.com/otuqxgb). This is easy to say, but very difficult to do. Therein resides the opportunity for Canada to become a leader in cybersecurity.

The global cybersecurity environment presents an increasingly complex set of challenges for Canada (Gendron, 2013; tinyurl.com/p3ela8n). Every adversity, however, has an opportunity couched within. We argue that Canada should act decisively and proactively to become a global leader in cybersecurity. Leadership in this undertaking encompasses the R&D projects; ventures of existing and new companies; content and training; and infrastructures that protect information and information systems.

In this article, we first present the main cybersecurity challenges facing Canada and the ways proposed to improve cybersecurity practice. We then discuss the features of an innovation engine designed to make Canada a global leader in cybersecurity. A unique corporation called the Venus Cybersecurity Corporation anchors the proposed innovation engine. The next section describes the responsibilities and desired results of the corporation. The last section provides the conclusions.

Main Cybersecurity Challenges for Canada

Based on the authors' experience gained protecting electronic information and information infrastructures for the government of Canada, we identify the current challenges faced by those responsible for securing Canada's critical infrastructure. These challenges are:

1. Traditional and ineffective cybersecurity approaches, which focus on prevention, risk management, and deterrence through accountability

2. Uncoordinated approaches between industry, academia, and government

3. Daunting and fractured list of cybersecurity research and development requirements

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

4. Silo mentality of research disciplines that prevents the development of an interdisciplinary science of cybersecurity

5. Overemphasis on the technical aspects of cybersecurity at the expense of social aspects

6. Chasms between classified and unclassified industry, academia, and government domains

7. Lack of education and training programs in cybersecurity

8. A paucity of Canadian companies operating in the global cybersecurity space

9. An under-investment in cybersecurity-related research and commercialization compared to other jurisdictions

10. Slow and uncoordinated government responses to addressing the root causes of cyberattacks

11. Innovation-stifling contracting processes and procedural requirements of governments (e.g., $25,000 contract limits)

Ways to Improve Cybersecurity Practice

Craigen, Walsh, and Whyte (2013; timreview.ca/article/704) and Craigen, Vandeth, and Walsh (2013; timreview.ca/article/705) offer various suggestions on how to improve the investment in research and experimental development programs in Canada. Their suggestions can be summarized as follows:

1. Establish a healthy ecosystem to incorporate continuously evolving operational concerns into available cybersecurity systems, researchers, and practitioners.

2. Engage social scientists in cybersecurity research.

3. Focus on approaches that: i) are consistent with federal cybersecurity policy; ii) quantitatively assess the cybersecurity risk of complex systems; iii) automate collective action amongst distributed systems to defend individual computers and networks; iv) de-risk emerging technological solutions; v) are ethical and respect privacy concerns; and vi) focus on cyberadversaries, maturity models and standards, "big data", data scientists, and ways of working and collaborating.

Mulligan and Schneider (2011; tinyurl.com/kt3f3gq) argue that lack of security is the obstacle to success of the information age. Though the problem resides in technologies, the solution requires policies and practices that focus more on the collective than on technology.

Schneier (2008: tinyurl.com/ps78x3y; 2012: tinyurl.com/ousf4cn) argues that understanding the mechanisms of trust is crucial in a connected society. He is a proponent of full disclosure and making security issues public to shed light on the threat as well as encourage its mitigation. According to Schneier, "If researchers don't go public, things don't get fixed. Companies don't see it as a security problem; they see it as a public relations problem" (Smith, 2011; tinyurl.com/c34hlbc). Cybersecurity issues as well as their resolutions are community challenges.

The broad set of challenges, the range of stakeholders, and the relationship between the opportunity and national economic well-being suggest that the required response is beyond the capability of any one individual or organization.

Business ecosystems are used to achieve results that no single member can achieve on its own. Business ecosystems provide a networked approach to innovation and commercialization where members act cooperatively for private benefit as well as systemwide benefit (Moore, 2006; tinyurl.com/5rtbj6u). Ecosystems are deeply interlinked. In an ecosystem, a fundamental tension exists between acting in the group's interest and acting in one's own self-interest (Moore, 2006: tinyurl.com/5rtbj6u; Muegge, 2011: timreview.ca/article/495; Schneier 2012: tinyurl.com/oko37dd).

An Engine to Convert Innovation into Desired System-Level Results

We reason that Canada is a country that has the talent, geographical advantage, and political environment to become a global leader in cybersecurity and that an engine that converts innovation into compelling system-level results can be cost-effectively built using the cyclical relationship conceptualization proposed by Muegge (2011; timreview.ca/article/495).

We argue that the innovation engine comprises five key entities (described below), which are linked together by strategic intent, governance, resource flows, and organizational agreements. The innovation engine enhances the firm-specific advantages that determine the out-

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

comes of global competition among firms. These firm-specific advantages include: research and development, size, and managerial capability (Oh and Rugman, 2012; tinyurl.com/o86vnsg), strategic intent of competitors (Hamel and Prahalad, 1989; tinyurl.com/o9evsdh), and capability to use distribution and brand positions to leverage revenue generated in one market to subsidize market-share battles in other markets and increase sales volume (Hamel and Prahalad, 2013; tinyurl.com/p4w6xs9).

Key entities

The five key entities of the innovation engine that is core to the strategy designed to make Canada a global leader in cybersecurity are:

1. The Venus Cybersecurity Ecosystem (hereafter "Venus Cyber Ecosystem")

2. The Venus Cybersecurity Project Community (hereafter "Project Community")

3. The External Community

4. The Venus Cybersecurity Platform (hereafter "Platform")

5. The Venus Cybersecurity Corporation

Figure 1 illustrates the key entities in the proposed innovation engine and the system-level results that are desired by 2017. The entities in Figure 1 exist at different levels of abstraction, the higher the level, the lower the detail presented. The five entities in Figure 1 are interdependent, and each entity relies on the other entities for the innovation engine to achieve the desired system-level results.

The Venus Cyber Ecosystem is the entity at the highest level of abstraction. Ecosystem members include: i) users, buyers, suppliers, partners, and channels of cybersecurity research, products, services, infrastructure, and solutions; ii) new ventures; and iii) the organizations and individuals who serve them (e.g., legal, accounting, intellectual property, economic development organizations) and provide them with requisite inputs (e.g., technology, capital).

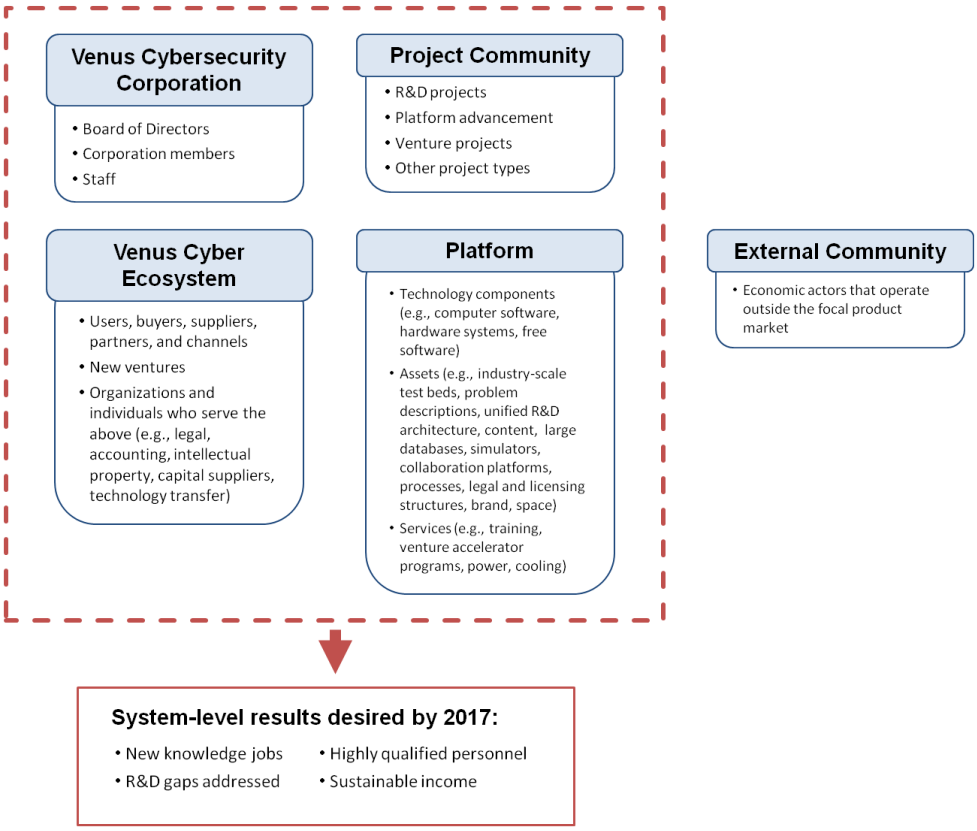

Figure 1. The innovation engine that is core to the strategy designed to make Canada a global leader in cybersecurity

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

The Project Community comprises the individuals working within a project portfolio sanctioned by the Venus Cybersecurity Corporation. Projects are defined and organized by their desired cybersecurity knowledge, technology, and business outcomes. The project portfolio includes R&D projects to reduce gaps and operational limitations, platform advancement projects, venture projects, and so on. Membership in the Project Community provides rights to engage in one or more of the projects launched by members of the Venus Cybersecurity Corporation.

The External Community refers to people who collaborate outside of and with the Venus Cyber Ecosystem and the Project Community. They may contribute to the Platform. People in the External Community can operate inside and outside Canada. The External Community is a source of human capability, technology, relationships, and other resources. The Venus Cyber Ecosystem and the External Community will exchange resources through the identification of important technology and business opportunities, acceleration of members' businesses, open source developments, standards activities, training seminars, and the like.

The Platform comprises a set of technology components (e.g., computer software, hardware systems, free software), infrastructure (e.g., industry-scale test beds, large databases, simulators, and systems to distribute assets, manage contributions, communicate between members, and coordinate work), assets (e.g., descriptions of industry problems, unified R&D architecture, courseware, validation requirements, legal and intellectual property licensing structures, brand) and services (e.g., training, venture accelerator programs). Members of the Venus Cybersecurity Corporation will be able to use and consume these technology components, infrastructure, assets, and services to develop their market offers and carry out R&D projects as well as other projects.

The Venus Cybersecurity Corporation is an organization that: i) supports and structures the collaboration of organizations and individuals in the Venus Cyber Ecosystem; ii) sustains the strategic intent of making Canada a global leader in cybersecurity over the long term; and iii) advances and operates the Platform. The Venus Cybersecurity Corporation comprises the Board of Directors, Members of the Corporation, and employees.

The Venus Cybersecurity Corporation is a not-for-profit, member-supported corporation. Membership in the Venus Cybersecurity Corporation provides rights to engage in the governance of the corporation to the extent allowed by the various membership levels. Strategic members of the Venus Cybersecurity Corporation pay the highest cash fees and thus will have a significant influence over the direction and strategic intent of the Corporation. Other membership levels can influence the direction of the Corporation through their representation on the Board and through participation at the annual General Meeting.

There are differences between members of the Venus Cybersecurity Corporation and members of the Project Community. For example, members of the Venus Cybersecurity Corporation pay annual (cash) membership fees for which they receive the right to vote on governance matters. Voting rights allow corporation members the ability to shape how the corporation operates and what it achieves relative to its strategic intent. Further, the ability to decide on, and launch, cybersecurity-related projects is the purview of corporate membership. Project Community members can only participate in the specific projects to which they make in-kind contributions or provide cash.

Relationships among the five key entities

Figure 2 illustrates the relationships among the Venus Cyber Ecosystem, the Venus Cybersecurity Corporation, the Platform, the Project Community, and the External Community that produce the desired system-level results. The inner triangle in Figure 2 (shown in heavy red arrows) highlights that the resource cycle of the proposed innovation engine will move from the Platform, to the Venus Cyber Ecosystem, to the Project Community, and back to the Platform.

The Project Community is the focal point of innovation in R&D. Projects leverage their access to the Platform to transform resources received from the Venus Cyber Ecosystem and External Community into technology components, assets, and services that increase the relevance of the Platform.

The Venus Cyber Ecosystem is the focal point of innovation in the factors that determine the outcomes in global competition for Canadian firms and new ventures. Organizations and individuals in this ecosystem leverage the technology components, assets, and services of the Platform to create competitive advantages in the global markets where they operate for their own economic gain and to secure Canada's critical infrastructure.

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

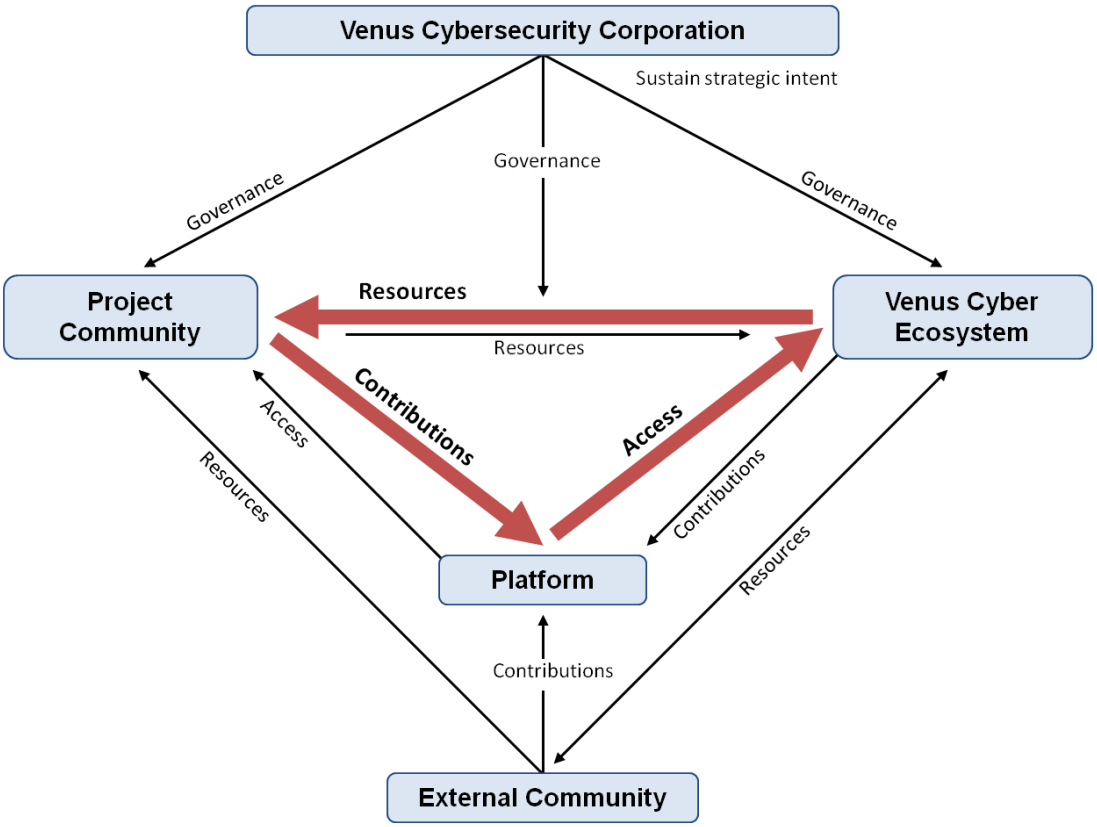

Figure 2. Relationships among the five key entities in the innovation engine

Organizational agreements will enable the following activities:

1. Members of the Venus Cyber Ecosystem will be able to use, extend, and commercialize the assets of the Platform to create and capture economic value.

2. The organizations and individuals in the Venus Cyber Ecosystem and External Community will be able to make the resources required to carry out projects.

3. The Project Community will be able to contribute new technology components and assets to the Platform thereby increasing the Platform's value.

4. Members of the Venus Cyber Ecosystem will be able to contribute technology components and assets acquired from other communities to the Platform.

5. The Project Community will be able to contribute resources such as information, customer leads, and skills to the Venus Cyber Ecosystem.

Venus Cybersecurity Corporation

The Venus Cybersecurity Corporation is the organization that anchors the innovation engine illustrated in Figures 1 and 2. The Venus Cybersecurity Corporation has five important responsibilities:

1. Sustain the strategic intent of the innovation engine over the long term. Strategic intent is an obsession created to attain the desired leadership position and to develop a process that sustains this obsession over the long term. Strategic intent is a vivid picture that captures the essence of winning in cybersecurity and that is stable over time to keep the ecosystem focused. The strategic intent is sufficiently detailed to set targets that deserve personal effort and commitment from members who drive cybersecurity technology and business innovation. Finally, the strategic intent creates a sense of urgency to keep an aggressive pace of ecosystem work and ensures consistency in resource allocation over the long-term (Hamel and Parahalad, 1989; tinyurl.com/o9evsdh).

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

2. Lead the Venus Cyber Ecosystem and the Project Community. By leadership, we mean organizing groups of people to achieve a common goal.

3. Govern. The corporation will make decisions that define expectations, grant power, allocate resources, and verify performance.

4. Increase the relevance of the Platform. The corporation will use contributions from the Project Community, the Venus Cyber Ecosystem, and External Community to advance the Platform. The Project Community contributions may include up front in-kind contributions as well as project outcomes.

5. Provide access to the Platform. The corporation will provide the Project Community and the Venus Cyber Ecosystem with access to a state of-the-art platform.

Iansiti and Levien (2004a: tinyurl.com/7t4xgvn; 2004b: tinyurl.com/nmfpyms) refer to the organization that anchors a business ecosystem as the "keystone." The responsibilities of the Venus Cybersecurity Corporation include the responsibilities that Iansiti and Levien attributed to a keystone plus an additional one: the leadership role described as the second responsibility above.

Not-for-profit versus for profit

In the Canada/cybersecurity example described in this article, the innovation engine is anchored around a not-for-profit corporation. This decision was made to reduce the time required to make and execute decisions; to increase information and resource exchange among industry, government, and academia; to reduce overhead; and to establish strong links with cybersecurity centres in allied countries.

In Canada, a group of private sector firms should lead the proposed not-for-profit organization. There is not one firm that can lead. Government agencies, universities, and other not-for-profits can join as members.

Desired system-level results

Table 2 identifies the four system-level results that differentiate the Venus Cybersecurity Corporation and that will motivate organizations and individuals to become members in the first four years. These system-level results require a business ecosystem, platform, project, and external communities because they are not attainable by any organization or individual working alone. Table 2 also shows the dimensions that will be used to assess the success of the corporation as of December 31, 2017.

Table 2. System-level results and success dimensions of the Venus Cybersecurity Corporation

Desired system-level results	Dimensions used to assess success
1. New knowledge jobs in Canada	• # of jobs created • # companies launched • # and revenue of products delivered to Canadian and international markets
2. R&D gaps and operational limitations in cybersecurity addressed	• # of R&D gaps addressed • # of government programs influenced • # of large industrial programs influenced
3. New highly qualified people operating in the cybersecurity space	• # of academic initiatives generated • # of advanced graduates produced • # of new cyber-related academic disciplines established
4. Income for the corporation	• # of decision makers engaged in the corporation's projects and initiatives • # of jointly sponsored projects in cybersecurity • # of public campaigns recognizing leadership roles of members in the Venus Cybersecurity Corporation

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

Conclusion

In this article, we offer a generic approach to making a country a global leader in a specific product market and use Canada and cybersecurity as an example of its application. The success of the proposed innovation engine relies on properly structuring the collaboration among organizations and individuals in an ecosystem, project community, platform, and a corporation, and creating links to communities external to their sphere of activity.

The cybersecurity opportunity is not exclusive to Canada as a country. Other countries are just as well positioned as Canada to become global leaders in cybersecurity. We use Canada as an example because it is the focus of our work. Our "definiteness of purpose" to make Canada a global leader in cybersecurity may encourage our allies to work towards making their countries global leaders as well. We would welcome this outcome. If Canada and its allies commit to attaining global leadership positions in cybersecurity, the rising tide will lift all boats and the networked world will benefit as a result.

Implementation of the innovation engine to make Canada a global leader in cybersecurity through putting the five entities in place is expected to: i) accelerate and strengthen the process of participation through which organizations and individuals work together to achieve results not possible by any entity working on its own; ii) enable continuous improvement and rapid adjustment to environmental changes; iii) increase the positive impact of the results attained; iv) accelerate learning; and v) identify the salient factors that determine a sustainable global leadership position in cybersecurity.

The cybersecurity challenge transcends the abilities of any single organization or individual to address alone. Consequently, academic, private, and public sector participants must unify their efforts when identifying the relevant issues, finding solutions, informing choices, and educating society in direct response to domain-specific requirements for the protection of information technology. This article contributes a way to unify these efforts.

To implement the approach proposed in this article, a task group has been formed. The task group has assumed responsibility for the embryonic development of the proposed innovation engine, including the launch of the Venus Cybersecurity Corporation. This not-for-profit corporation will be launched by March 31, 2014.

Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity

Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh

About the Authors

Tony Bailetti is an Associate Professor in the Sprott School of Business and the Department of Systems and Computer Engineering at Carleton University, Ottawa, Canada. Professor Bailetti is the Director of Carleton University's Technology Innovation Management (TIM) program. His research, teaching, and community contributions support technology entrepreneurship, regional economic development, and international co-innovation.

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.

David Hudson has recently completed his doctoral studies at Carleton University's Sprott School of Business in Ottawa, Canada. He is a lecturer in information technology innovation in the MBA program at Sprott, a Director of the Lead to Win entrepreneurship program, and Chair of the Ontario Centres of Excellence advisory board for the Information, Communication, and Digital Media sector. David also consults with Fortune 500 firms on innovation management. Previously, he was the Vice President for advanced research and development at a large technology firm and has had an extensive career in technology development and product line management. David received Bachelor's and Master's degrees in Systems Design Engineering from the University of Waterloo, Canada.

Renaud Levesque is the Director General of Core Systems at the Communications Security Establishment Canada (CSEC), 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 CSEC in 1986 as a Systems Engineer, responsible for the development and deployment of numerous systems, including the CSEC 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 CSEC 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 CSEC'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.

Stuart McKeen works for the Ontario Ministry of Research and Innovation (MRI), where he just finished serving a three-year secondment with the Federal Economic Development Agency for Southern Ontario (FedDev). At FedDev, he was both the Agency's Manager of Innovation and the Manager of Entrepreneurship, Internship, and Youth Programs. He has worked in six different ministries of the Ontario Government over the past 30 years. In 2008, he was awarded the Amethyst Award, the Province of Ontario's highest employee recognition award for his pioneering work on prospecting and developing large-scale international research consortiums that have brought jobs and investment to Ontario. Stuart holds a BScH degree in Zoology from the University of Western Ontario, Canada and a BA degree in Economics from the University of Toronto, 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.

Citation: Bailetti, T., D. Craigen, D. Hudson, R. Levesque, S. McKeen, and D. Walsh. 2013. Developiong an Innovation Engine to Make Canada a Global Leader in Cybersecurity. *Technology Innovation Management Review*. August 2013: 5–14.

Keywords: cybersecurity, innovation engine, business ecosystem, innovation in research and development, innovation in commercialization

CC BY