Institute X

Ottawa, ON

Cyber Security

Protection, Progress, Prosperity

Submission to the Federal Consultation on Cyber Security

October 2016

INSTITUTE X

Institute X is a transformation change consultancy and think tank with expertise in the areas of cybersecurity, digital identity, and Cloud computing.

Timothy Grayson is a creative expert in digital transformation and trust, with a robust body of work. He is also a novelist, most recently of *Internet Exodus*, the story of a global systems hack and the turmoil it unleashes.

Cyber Security
Protection, Progress, Prosperity

Executive Summary

This Consultation on Cyber Security is sure to draw extensive contribution. Those institutional and private contributors, from academia and the private sector, are sure to be deep of detail about this rapidly evolving field. They will represent every corner of cyber security: defense, protection, innovation, opportunity exploitation, and such. The richness of the data brought forth is likely to be unsurpassable.

This submission focuses on *Canada's Way Forward*, making concrete policy proposals to accommodate the vast number of constraints and pressures on the Government of Canada. The three foundational sections: *Evolution of Cyber Threat*, *Economic Significance of Cyber Security*, and *Expanding Frontiers* will narrate the context and implications of the information and data insights.

Principle concerns are:

- The cyber threat growing over decades is unending. It has—typically—taken a trajectory from prank, to petty harm, to criminal larceny of all sorts, and on to social and international weaponization. As capabilities morph, they spawn new vectors of development.
- Cyber threat, maturing beyond relatively benign monetary harms into various forms of weapon, originating in secret and specifically or indiscriminately targeted at Canadians will become ever more terrorizing.
- Cyber threat evolves along the same path as the underlying technology. As such, a high-probability area is quantum computing, set to be the next step of computing evolution. In this domain, particularly quantum cryptography, Canada has material advantage in research and development activity.
- The economic significance, as stolen/extorted money and reparation, is substantial. These costs will become both more unquantifiable and vastly larger. There will be impacts to intangible assets such as brand value and trust (itself impacting transaction costs), as reduced confidence in Canada and Canadian business (as credit rating impacts).
- There is also economic opportunity. Every, accelerating threat evolution brings along an equally important evolution in protections. This unlikely-to-abate game of cat and mouse innovation presents substantial economic opportunity. Abundant businesses and research organizations in Canada are ready to capitalize on that global opportunity.

The Government of Canada must forge a way forward that addresses both the national costs and revenues while concerning itself with the nation's safety at all levels. It is probable that most responses will focus on the "protection" intent of the consultation with suggestions to do certain things: support specific forms of

protection, support Canadian vendors, and so on. There is nothing inherently wrong with any such choice. All have value. But, they ought to be individually undertaken in full recognition of the conditions and the limitations on what government can do.

Within an overall strategy that embraces the goals of (1) enhancing levels of Canadian cyber security and (2) enhancing Canada's cyber security industry, the following recommendations provide maximum leverage to accomplish both goals.

1. Set, institute, and implement "unrealistically" high requirements for cyber security for all government entities. These should apply equally to all who interact digitally with government at any level for any purpose.
2. Through regulation or legislation if necessary, extend "unrealistically" high cyber security standards to a set of key industrial sectors.
3. To facilitate upgrade to these high levels of cyber security, government should underwrite a portion of costs borne by non-government participants. Support could be structured to encourage faster uptake.
4. To support the domestic cyber security industry, particularly for innovation of products and services that are scalable and exportable, industrial policy to complement these upgrade activities must favour Canadian firms.
    a. Extension of existing early buyer programs such as BCIP[1]
    b. National security exemptions on procurement of Canadian products/services
5. Foster persistent investment into R&D through some combination of direct grant or tax credit schemes based not solely on currently invested capital but future investment of capital to incent longer term research/innovation.
6. To expand internationally, target export development support for Canadian-owned cyber security businesses operating in Canada collectively and harmoniously with provincial and municipal efforts.
7. Lead a national action plan for cyber through the creation or fostering of a non-governmental directing entity that would focus and orchestrate the activities of the diverse and distributed players in the cyber security domain, including academic, government, and private research organizations, private sector firms, government entities, and so forth.
8. Act. Cyber threat is metastasizing geometrically and every week of hesitation allows uncoordinated action to diminish in strength and potential.

[1] Build in Canada Innovation Program

Cyber Security
Protection, Progress, Prosperity

While security is the underlying reason for this consultation, it is readily apparent that this great challenge is intrinsically tied to an equivalent opportunity for industrial development. Canada has many of the resources needed to raise the public safety profile and defense standing viz. cyber. As such, coordinated policy and action on cyber security could be doubly beneficially enabling their world-class growth.

Detailed consideration of every facet of cyber security (e.g., role and effectiveness of CCIRC), while important, is not this submission's focus. This paper addresses the four topic areas as a comprehensive strategic argument and recommendation to use thoughtful action on cyber security to:

i. raise Canada's level of cyber protection and defense; and
ii. support an industrial policy that capitalizes on the growth of cyber security to Canada's economic benefit.

Evolution of Cyber Threat

Cyber threat is part of popular culture, its impact reaching from personal stalking to commercial infiltration and national defrauding. Known by titillating exposures like the Ashley-Madison breach and the Democratic National Committee's machinations, these are but the top of the iceberg. Without them though, the exponentially larger, out-of-sight threat below the surface would be out-of-mind except to experts and cyber *cognoscenti*. So, if what is revealed in popular media is large and expanding, exactly how big and dangerous is that which is hidden from view? Unfathomably.

Cyber threat in all its manifestations is neither sudden nor unanticipated. It has been around as long as "cyber" has been a domain, which depends on how one pegs its start. Phreaking (stealing telecomm capacity) in the early 1980s was arguably a watershed in cyber threat development, spawning as it did the first generation of personal computer/communications network entrepreneurs as hackers. Today, we tend to restrict ourselves to Internet-based threat, which dates to the popularization of the World Wide Web in the early 1990s.

The starting point is immaterial, as is nuanced historical assessment of cyber threat evolution. Overlapping and diverging threat vectors predictably followed the money, evolving closely with underlying technological development. ***Cyber threats are simple crimes in complex environments using (sometimes) sophisticated tools***.

Cyber threat is simple crime

Without diminishing its impact or gravity, cyber threat arrived at its current state predictably, as a combination of trespass, vandalism, larceny, and extortion. ***The objective is always to achieve—acquire or create—value for the perpetrator.*** Often the value is money; other times, it is control of a valuable thing, wreaking havoc, or notoriety.

- Hacking a financial network/system or credit card database is to steal money.
- Locking a computer/phone (system) is to ransom and extort release.
- Hacking an email server to acquire information is for control, possibly for ransom or to embarrass.
- Hacking a car's functional systems is for control and to sow panic, and/or to extort and steal.
- Hacking critical systems is for control leading to chaos, destruction, or ransom.

And so it goes. The objectives are ancient and understandable. Cyber threat does not exist as an end in itself *except* as an egotistical display of capability and skill.

Cyber threat: innovation's dark art

Recalling that the objective of acquiring value underwrites cyber crime and threat, its unfolding has followed an common trajectory. It is the path of all innovation, as cyber threat is nothing if not criminal innovation.

Innovation arises out of unfulfilled need or desire. Ignoring for a moment the myriad other ways innovations germinate (e.g., recombination, domain-switching), cyber threat innovation has simply tracked information and communications technology development.[2] Like other innovations that arise from novelties created by new technologies and structures, cyber threat cycles through typical phases.

Cyber threat evolves to take advantage of novelty in and ignorance of new structures and circumstances just as common innovation explodes out of basic invention. That is, a discovery or invention is revealed for some good purpose. It is the product (and victim) of single-minded thinking and vision. The mind that found it was bounded by a particular creative view. Released to other similarly creative but unrestricted minds, the invention is exposed not merely for its benefits but also its shortcomings. Were it not for the unsavoury pornography, gambling, and other underground industries, the Utopian World Wide Web (especially eCommerce—and maybe cyber currency) would never have developed for good or bad purpose as fast as it did. Exploits paved the way.

> In Ottawa, over Labour Day weekend 2016, a hacker breached a road sign to post vulgar messages. Such annoyances are capability proofs that presage wider, more troubling criminality.
>
> Apply this on Hwy 401 signs or to metropolitan auto/rail traffic and see what dangerous hilarity(!) ensues.

[2] This leading indicator—as broad as it is—must be distinguished from narrower, tactically-driven evolution of cyber threat based on direct cyber security development. When cyber threat changes in apposition to the activities to thwart it (cyber security), these are marginal cat and mouse iterations mostly inconsequential to policy considerations.

It is easy to trace cyber threat evolution through dark phases of cyber *annoyance*, cyber *irritation*, *petty* cyber *crime*, *organized* cyber *crime*, and ultimately to cyber *weaponization*.

In 2016, Hollywood Presbyterian Medical Center reported its computer systems were hacked and locked. The hacker attempted to extort US$34-million (9,000 Bitcoins), ultimately getting only US$17,000 (40 Bitcoins).

The questions are: How many go unreported? What will organized criminals demand—and get?

- Hacks of institutional websites to deface with unflattering imagery or commentary are trespass. It is petty and equivalent to vandalism.
- Malware that corrupts personal computers leads to the kind that steals credit card information or, more creatively, to ransom; hallmarks of criminal enterprise.
- Malware designed by a state to damage another state's infrastructure is cyber weaponry. Using cyber tools to meddle in other states' affairs weaponizes the tool.

This excludes cyber crimes that seem benign at first such as cyber stalking, social media defamation, and contraband retailing in the Deep Web (all afforded by the inherent anonymity of cyber structures). ***The organized and hence efficient use of cyber tools for criminality and its weaponization—at all levels and in all ways—makes for fearsome cyber threat.*** This nascent actual weaponizing of cyber space, perhaps especially through social media, is the most unnerving.

Cyber weaponry

A common if not inevitable endpoint is the unleashing of weaponry based on a usually well-intentioned initial innovation. Cyber is no different, as proven by what has already happened.

Consider:

- Anonymous communication becomes a weapon to destroy reputation, credibility, and trust, ruining individual and organizational lives.
- The broad, globalizing reach of the Web as a social medium becomes a weapon/tool of terrorist radicalization and indoctrination.
- Social exposure of personal information, together with connected home/car/etc., turns the convenience of distant control into break and enter tools.
- Broad, cheap transmission over the Internet and distributed, networked computing enables delivery of malignant instructions that turn devices into legions of zombie robots.

Fictional Scenario 1: Fit to die

Many GPS mapping applications were fraught with calibration errors early on, misdirecting the unaware into rivers and buildings. What if an artificial flaw was distributed to the personal level? What if the step-count metric on Fitbits were altered? Would competitive people drive themselves to injury… goaded by a digital coach? Could it overexert coronary recuperants? The example is silly compared to critical system take-over, but could it happen? What would the effect be on health care? **How would it guide the next idea?** The point is we don't know nor are we motivated to pursue the thought. It's small and ridiculous. But, so was arming Amazon-purchased drones.

- Commercially available drones with connected high resolution cameras expand espionage even to the individual level; with explosives as flying bombs.
- Connected financial systems magnify value and secrets, increasing risk of attack, making individual and institutional impacts from "success" of a hack unimaginably broad.
- Connected and dominantly software-based transportation systems and devices are compromised and repurposed—turning a car into urban missile.

So much of what we consider banal and safe is, by virtue of being computer- or chip-embedded and software driven, at risk of being used against us in ways *we cannot even imagine*.[3]

Cyber threat construction

Cyber threat depend on three things, none of which is going away or containable.

1. The creative criminal mind with a goal.
2. The unthinking processing power and speed of software.
3. Networked information transmission.

To some extent, the first factor has been considered. While a human actor is implied, given the pace of Artificial Intelligence (AI) development and the obvious shortcomings of software (e.g., trading programs that led to economic cataclysms), the "malcontent with intent" could readily be a machine. A machine probably set on this path by a human actor, mind you.

Fictional Scenario 2: Untrustable Systems

We are accustomed to stability and predictability. Machines and computing systems are designed for it and for the most part, are so. We tend to trust them. Malfunctioning systems are brought down to correct the problem and restore stability. But what if the executed cyber threat injected malware to alter a high-leverage instruction to be "off" at random intervals. That is, on some irrational frequency an innocuous calculation output a tiny error before immediately returning to normal? The error might not be replicable; the system rendered unreliable. What if the output affected financial transactions or enterprise resource planning, or air traffic control, or any of the many boring but critical uses of signals and the GPS? How much inefficiency (cost) could such noise introduce?

Software is fundamental to cyber threat. Irrespective of the ultimate goal, exploiting software is essential to execute a material cyber threat. Software enables because it is an amoral, rule-following instruction set; for software, the Nuremberg defense holds. The threat, presuming it is not a straight-forward take-over of controls (itself a problem with authenticity and authorization), is either injection of new code that enacts the threatening mission directly or code that corrupts existing software so it enacts the mission itself.

---

[3] Cyber threat evolution has not, is not, and will not be anything the civilized, law-abiding world will be prepared to deal with in advance. (Except, of course, for those parts of government dedicated to borderline criminality in the service of the greater good.) The civilized, moral, creative mind has boundaries from which it recoils that do not inhibit the criminally creative with a goal.

Software, particularly the kind of comprehensive applications that make operations efficient, is a complex system. The applicable feature of complexity is asymmetry. A threat, executed, may be unnoticeably trifling while its effects are disproportionally large. Asymmetry is, of course, the essence of guerrilla warfare and terrorism.

Networked connectivity is equally important though not essential, as infection of air gapped systems proves. (Internet) Connectivity is the essence and a prime value of the Web. With Cloud computing and mobility structures, it is a foundation of all cyber value, development, and innovation. There is, inherently, nothing wrong and much right with this situation: recent history proves Scott McNeely's prescience and Metcalfe's Law of network value.[4]

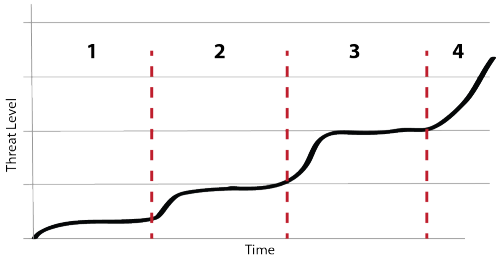
Less popularly considered by (technology) optimists with an eye on network value is that risk is also amplified at a similarly exponential pace. Every endpoint is a threat surface and endpoints now include thermostats and cars and millions of other banal devices. Multiplying communicating devices have multiplying access conduits for information—and for breach. It makes for the inevitability of Black Swan catastrophic cyber threat succeeding.[5] How are these billions, if not trillions of endpoints to be protected and monitored to an unimpeachable degree?

This consultation has to acknowledge state leadership in cyber weaponization.[6] Whether this condition is unacknowledged as a problem is mostly a political and moral stance. Still, its effect cannot be ignored. State/military weaponization of anything *always* escapes into the hands of unsavoury actors of all sorts so that cyber weaponization is the overriding source of dire threat from all manner of player.

Patterns of cyber threat evolution

Cyber threat growth has conformed to a predictable set of innovation steps.

1. *Invention* – technological advance presents new opportunities for (positive and negative) exploit
2. *Exploration* – opportunities and constraints in the new technology are tested for exploit
    a. Annoyance and Irritation
    b. Petty larceny and criminality
3. *Organization* – non-state activity to exploit weakness is organized
4. *Weaponization* – typically states lead advances in the use of the innovation for offensive/defensive combat purpose.



[4] Scott McNeely was CEO of Sun Microsystems and uttered, "The network is the computer." Metcalfe's Law states: the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2).

[5] Taleb, Nassim. *The Black Swan: The Impact of the Highly Improbable*. Random House: New York. 2007.

[6] Cozy Bear (APT 29) hacked the White House, and Fancy Bear (APT 28) hacked the Democratic National Committee and World Anti-Doping Agency. Both are allegedly tied to the Russian state. China (NRC hack) and North Korea (Sony hack) sponsor hacking of Western government and commercial systems. The NSA created Stuxnet and the Snowden Papers have laid bare the intent of US cyber hacking and weaponization.

It should also be evident that the specific domains susceptible and giving rise to cyber threat correlate and track the expansions of information communications technology and computing, including networking. ***Where software and connectivity have gone so goes cyber threat.*** This ought to most directly inform planning and policy particularly for anticipating areas at risk of cyber threat.

Economic Significance of Cyber Security

This submission does not estimate economic loss or gain attributable to cyber security because reasonable assessments are largely unconstrainable. ***It can be validly argued that economic impacts of cyber security would be felt in every part of the Canadian economy that has made any foray into "e" anything (eCommerce, B2B integration, etc.)***. In other words: everywhere. As such, specific estimates may be informative but unreliable. Sunnier representations are likely to show levered expansion and increasing positive value. Others may focus on the negative impact to the Canadian economy from the same leverage applied to risks.

This section seeks only to illuminate the ways:

- Cyber as an economic sector is relatively more valuable and has relatively more potential for gain than many other sectors of the Canadian economy.
- Cyber threat has indeterminately large costs.
- Cyber security is a sector where actions on the cost or the revenue side of the ledger can have material beneficial effect on the other side as well.

Revenue and Cost

There are two interdependent but divergent dimensions to cyber security for Canada. One is the positive economic opportunity presented to the Canadian cyber security industry. Globally, immediate and ongoing spending to secure and sustain cyber protections against evolving threats represents an enormous and rapidly growing market. Canada has a number of advantages in this domain that position Canadian industry for significant export-based gain. The other is the cost of cyber security in Canada, which splits into two primary areas. (1) Immediate investment by Canada and Canadian business/individuals to upgrade and enhance cyber security measures to repel attack. (2) Potential cost of sustaining successful cyber attacks.

Upside (Revenue)

In active cyber security clusters in Fredericton, Ottawa, Toronto, and Waterloo, is an inchoate ecosystem of commercial organizations and research institutions. They work in cyber security subdomains ranging from cryptography to fintech and services. Expansion to niche development beyond the common domains of cyber security (e.g., protection of chips and communication in cargo transport or the many areas of military-directed cyber security) makes the full breadth of cyber security commercial and research activity in Canada a moving target.

Within this industrial sector are Canadian-bred and owned entities at all stages from start-up to enterprise, many of which fall to acquisition by larger foreign firms. There are also Canadian outposts of foreign firms. The obvious value of globally successful Canadian-owned and based firms is the significantly larger overall contribution to government revenue and GDP. Even foreign-owned firms make economic contribution directly and by virtue of employment. Knowledge employees in

this tech sector are in high demand, commanding high compensation. Exactly the labour force desired for an economy shifting from natural resources.

Most individual firms and research labs engaged in this area are innovators. They must be. Viability in the face of changing cyber threat demands it. Small firms in this domain, of which Canada has many, are the seedlings of global economic impact and value to Canada. Maximum economic potential and impact comes from innovation and successful commercialization through the growth stage of a firm's existence, let alone from a category's development. This makes a cyber security industrial policy that shepherds small firms through this stage urgent. Here ***the cyber security consultation is inextricably tied to innovation efforts and policies*** of Innovation, Science, and Economic Development Canada.

The most important feature of this industrial domain viz. positive economic impact is that ***cyber security is a broad industrial domain only now beginning to reach growth toward mass consumption and use in business and consumer markets***. It is also an industry unlikely to slow for decades, if ever, because of two key factors driving it: (1) ongoing digitization and technology evolution, and (2) the increasing value of what is being digitized and made accessible digitally. Cyber security could ultimately have an impact in the order of the resource sectors. A parallel might be the boost personal computing gave the likes of Microsoft, IBM, Oracle, and "Silicon Valley" generally in the 1980s, and the Web gave Google eighteen years ago.

Downside (Cost)

The other side of the economic ledger is the cost impact of changes to the demand for and degree of cyber security. Particularly for the contingent liability elements, the scope of risk and cost could be crippling to individual victims and to the nation at large. Some proactive and reactive costs are considered separately.

Implementation of upgrades

Any meaningful action by the Government of Canada with regard to cyber security ought to entail a mandate to enhance cyber security. This should apply not only to government itself, but to every other threat surface (i.e., owners/operators of all connected devices and networks). Such a mandate, if effective, could mean material and costly cyber security upgrade to allegedly inadequate systems protections across the land.

Such a directive would impact commercial interests in a number of ways, not least of which would be raising investment and maintenance costs for cyber security. Business people, some operating on razor-thin margins, will undoubtedly claim it is unnecessary in their circumstance and that if implemented, costs will be passed on to the consumer of their goods. Business lobbies will rally economists and actuaries to dispute and invalidate the need for these costs relative to the devastating economic impact on immediate commercial affairs. ("This is just another unfair and anti-competitive tax… businesses will be hampered and move out of the country…," one can already hear.)

Clearly any meaningful imposition of enhancements to the national state of cyber security will have a short-term negative financial impact on those forced to upgrade. As suggested in the *Canada's Way Forward* section, some of this negative impact can be offset.

Consider a parallel with Y2K (without the loudly-ticking deadline). In 1999, anyone that depended on computers faced substantial upgrade costs. Nobody liked it. The upgrade activity did, however, generate enormous offsetting economic benefit in the technology sector. Ultimately January 1, 2000 was anti-climactic. But the forced upgrade enhanced productivity afterward *and* there was the immediate positive offset. So the New Year's technology/economic hangover was minimal.

Cost of failure

Canadian businesses and governments—perhaps Canadians generally—notoriously delay and defer investment to upgrade and enhance (commercial input) assets. Mechanized equipment and rolling stock is used well beyond useful life; the Prime Minister's home is left to unseemly decay; geriatric helicopters fall from the sky; governments and business rely on antiquated, counter-productive information technology systems. ***While the Canadian productivity challenge is not the subject of this consultation, it factors into the economic impacts of cyber security.***

Be that as it may, cyber security failure presents quantifiable loss to the owner of the breached system, be it a smartphone, personal computer, substantial system, critical infrastructure, or connected door lock. In the case of *commercial* breaches that become public, remedy costs are high and climbing. These include notifications to impacted consumers, system repair (after the damage is done), payment for credit and identity monitoring/protection services for impacted consumers, and rising potential for class action damages assignment. Never mind the increasing likelihood of ransom and reputation (brand) fallout.

The insurance industry must come to terms with the calculus of cyber risk and premiums that earn a profit. But the nature of the risk remains too unpredictable to be accurately evaluated. Besides, the downside risk has yet to find a floor. On the other hand, risk of cyber security failure is regarded as improbable by those who: (i) have not been close to failure; (2) have an interest in devaluing investment for enhanced security; and (3) are unclear on the nature of asymmetries. Cyber intrusions and their associated costs are evermore common, but remain a Black Swan consideration. (Unlikely to affect me/my business!) Without a large policyholder base over which to spread the risk, cyber insurance costs remain high—disincenting buyers. For policy and direction, the real and potential negative economic impacts of failure must be considered without illusion.

Expanding Frontiers of Cyber Security

As sophistication and impact radius persistently expand, the present extent and nature of cyber security is far from the fullness of what it will be as a requirement, practice, and industry. Obviously the cyber security *domain* directly affects the cyber security *industry*. It also affects other industries where security is a paramount interest: critical systems, military, financial, and e-commerce, among others. So the relevant impact locus includes all users of systems and devices that represent an attack surface for cyber threat, including home and personal computing, mobility, and countless evolving computer structures. That relevant area also includes commercial operations that have exposed and maintain networked (operational) systems, especially using the Internet. Farming, for instance, is within this risk space where operational plans and activity, implements, automated irrigation and/or livestock maintenance is to any extent software supported and networked.

More important may be nascent and even unconsidered areas. That could mean everything, which is not to overstate the case because, as we know, the frontiers of cyber security expand in direct correlation to the expansion of digitization. The drive to direct more and more processes of every sort to the lower cost digital domain propels the expanding frontiers of cyber threat/security.

That which is in play or clearly evident but yet to be popularly appreciated as a threat vector, ought to be the most vivid guide. A select, small but critical set of frontiers is presented below. It is no accident or coincidence that these techno-commercial areas tend to be those broadly identified as being most valuable to organizations: only that which is valuable can be threatened.

Mobility

Ubiquitous wireless communications through voice, email, text message, and the Web (not least, social media) is a strong enabling force for rapid expansion of computing technology. Portability and always-on accessibility impels exposure of evermore value. Formerly fortified information (technology) assets have to be exposed, typically through the Internet and eventually through wireless networks.

To accomplish this and satisfy that demand, perimeter security "walls" are rendered necessarily more porous. So the wall metaphor/approach becomes increasingly incompatible with the new reality. Mobile access from anywhere is, however, but one part of the equation. Another part is: once the ability to access applications and data remotely is universal, the next demand is to add value by connecting to information resident in multiple disparate locations. This is one of the factors that has led to the rise of Cloud computing.

The Cloud

The Cloud is shared computing resources; mainly a business model change. That said, by its very nature as networked resources with relationship dependencies, Cloud structures present an expanded threat surface. Cloud structures depend upon standard interconnection among information *sources*, applications, and information *users* irrespective of where in the world any one of those might be located.

The good news is that Cloud providers are aware of the threats and (the good ones) are proactive about security. The cold water is that every customer and user represents a point of failure, which may or may not be closely monitored. Moreover, the heightened vigilance required and usually provided may yet prove insufficient because of the exponentially increasing value of succeeding at breaching security. With many more eggs in each basket, Clouds' value as a target guarantees that as they grow (and they are), they will draw increasingly aggressive cyber attack.

Identity federation and broad single sign-on

Digital identity lags as a practically implemented capability despite at least fifteen years of technology industry activity. Too many systems remain protected by simple passwords (to which too few people give adequate care), and popular expectation is that biometric technology will solve the problem.[7] With *authentication* and *authorization*, there is an unhealthy level of ignorance among too many executives

[7] Biometrics is not the core issue, and in this instance it's optimistic to believe a technological *tool* will address the problem.

charged to make decisions about it. That leads to delays to or outright ignoring of upgrade with concurrent desire for "single sign-on" and other interoperability capacities. Credit card security/fraud experience explicitly reveals that success securing one area of attack serves to redirect attackers to the next most vulnerable point. Mostly, there is a willful disregard for the essential, fundamental need to sufficiently authenticate. As time goes on, the current risk of not being certain about who or what one is transacting with may move to the level of critical and mortal. If a credential representing keys to the kingdom is to be available, it is valuable, making it a target for attack by hack after the fact or by compromising initial proofing.

Particularly for non-employee access, single sign-on demands some form of federation. As with underlying identity, this is woefully undeveloped. The technology exists and performs; the very slowly developing structures for interoperation and commercial acceptance of the risks and obligations of genuine, broad federation does not. Expanding Cloud-based interoperation will critically require strong digital ID and federation. This situation bodes well as driving force behind cyber security activity for decades.

Experience v. authentication

As much as ignorance of identity and credentials leads to poor cyber security decisions, so does the fashionable fetish of "user experience." This drive by online service providers to make every possible customer interaction painless, simple, undemanding, and non-invasive to the extent of compromising security is not bad in principle. It *is* a bad—crippling—thing where unchecked by a pragmatic wisdom counterbalancing for practical security, especially identity.[8]

Among others that ought to know better, Web staple, Yahoo! opted to ignore the need to maintain enhanced security on its flagship email service. Eventually (six-years later) media reported that Yahoo! was hacked by Chinese military hackers, exposing about 500-million individual user accounts (Cybersecurity not a priority at Yahoo, insiders say). Why? Doing so might make Yahoo! mail slower and more difficult to use, so its executive demurred. If an organization as sophisticated and central to the cyber world as Yahoo! is this cavalier, what chance is there an organization whose core business is NOT cyber will act smarter?

Too many (mostly consumer-directed) businesses believe they need single sign-on and anything else that retains the customer they "own." This diminishes or eliminates measures that would ensure they know who the customer is because it could adversely affect the experience.[9]

As long as Canadian online service providers are reluctant to embrace and join a high authenticity digital identity process and protocol *at the consumer level*, alternative cyber security measures and/or a counterbalancing policy/operating model will be needed. Either way, part(s) of the cyber security economy will benefit from a prolonged growth period.

---

[8] Examples of progress on such cooperation, collaboration, and standardization are ongoing in British Columbia and reflected in the capabilities, if not use of the federation model provided to the federal Government by SecureKey.

[9] "Experience" is code for unfettered and unhindered ability to do anything without having to undergo anything undesired on the path to online purchase or otherwise transacting. Note that this idea extends to where the consumer is not even paying; when the consumer is only being "monetized" as value to secure payment from others such as advertisers.

The Internet of Things

By expanding the number of endpoints on the network exponentially and generating even larger explosion of data, the Internet of Things (IoT) adds obvious scale challenges to cyber security. Because the IoT represents the inclusion of computing capability in an expanding array of connected things, it means more opportunity for more kinds of threat in more places. Thus scope of relevant, applied cyber security will dramatically broaden as well. In some cases these will be variations of existing themes. In others, new threat vectors will represent novel opportunities for attack: more takeovers of not just systems but individual and multiple individual devices and things. What might be done with that opportunity by motivated cyberpunks or state-sponsored hackers is anybody's guess.

Artificial Intelligence and robotics

Artificial Intelligence and robotics present a cyber threat risk straight from science fiction. These generally derive from takeover. There are many issues, every one of which demands extensive assessment. Suffice to say that mobile robots—not assembly line machinery—have the capacity to perform a variety of tasks, the extreme variant of which effectively to weaponize the machine (itself).

The science fiction of artificial intelligence as a threat is well trod: sentient machines become aware and take over from humans. With the exception of Stephen Hawking, Steve Wozniak, and about 100 deep thinkers, nobody believes that harm can come of AI. It may be that the AI created and allowed to become sentient will not evolve in our destructive human image.[10] But, what if some sociopathic human introduced a virus to corrupt that AI's "morals" and development so that the initial good intentions and precautions were defeated? AI development will not stop. So like nuclear facilities and capabilities, it will need rigorous protection. That protection will be significantly in the form of cyber security. And because the growth cycle of robotics and AI is at an early stage, this represents another half-century or better of derived demand for and evolution of cyber security.

Other

There are many other forces pointing to sustained growth for cyber security. One is quantum computing: a step-function change to how computing is performed. It will force similar step-function changes to all parts of the ecosystem, resetting cyber growth curves to zero. This ought to make for decades of explosive, overlapping (i.e., simultaneous development of traditional and quantum variants) growth for cyber security. It is, however, farther toward the horizon. The following are two other clear and present developments of significant import to cyber security.

Health care and genetic manipulation

Healthcare represents two clear vectors for cyber attack: stealing health records and attacking connected medical (hospital) equipment. The value we place on information privacy, particularly about our money and health, ensures continuing focus on protecting stores of information in the healthcare system. This, at the same time as personal and institutional healthcare data volume explodes. The industry is not immune to the forces of progress—toward wireless, connected, computerized

[10] Encoding Asimov's *Three Laws of Robotics* into the machine's software ought to be foolproof in preventing that.

equipment from iPads to dialysis equipment. Moreover, many devices, such as pacemakers are digital and connectable. These become targets, perhaps for pure malice (ransom) toward individuals or for terrorism, and will require increasing degrees of cyber security. What is less clear is the potential for immediate and long-term damage from misappropriated cyber access to leading edge medical and health research like that on genetic manipulation.

Software-based transportation, including driverless vehicles

We have seen hackers take over mid-2010s cars. The documented takeover of moving automobiles in Summer 2015 and Fall 2016 was done by accessing the vehicle wirelessly and taking remote control.[11] The amount of software in the typical vehicle is substantial but a far cry from the software-based operation of a Tesla, hacked in late 2016. There is no magic behind why this evolution is an ongoing force for cyber security development: the more software, the more opportunity for (mass) corruption. With software-based control of driverless and auto-piloted vehicles, the potential for less frequent (maybe) but catastrophic disaster grows.

Canada's Way Forward

The nature of *cyber* threat is substantially incongruous with the understanding of threat at the time territorial nation-states were created. Cyber threat is amorphous and untied to geography. There is no unified, identifiable, and qualifiably large peril. ***It is the essence of digitization to create asymmetries. So, cyber threat is small, distributed, camouflaged, and highly levered***: small "wins" yield dramatic results.

No government could implement an effective strategy, with any amount of money, to directly and comprehensively address the overwhelming number of relatively small challenges and opportunities viz. cyber security. And, while the Government may have specific direct roles to take on, it is far more important to create the structures, incentives, and practices that will lead Canadians at large to advance and succeed in some aspect and area of cyber security.

Above all else, after this consultation and following due thoughtful structuring and planning, the Government of Canada needs to create a cyber security doctrine to permeate the nation. It must comprehend the relevant aspects of what cyber security represents and what it touches. Also, it would not be out of line to have a Cabinet-level, "Cyber Czar" dedicated to cyber as an industry *and* comprehensive national cyber security, cyber defense, and cyber attack capabilities management.

Goals

Overarching goals for Canada in cyber security are few but broad. From each, strategic thrusts and milestones will emerge and evolve. The three goals for the way forward are:

---

[11] Greenberg, Andy. Wired. *Hackers Remotely Kill a Jeep on The Highway—With Me In It*. 21 July 2015 and Heisler, Yoni. BGR. *Researchers show anyone can hack Tesla's Autopilot software and force a crash*. 4 August 2016.

1. Ensure computing and network systems in place and active in the country are sufficiently protected and monitored for intrusion and harm, including upgrade(s) to address evolving threats of data theft and system compromise.
2. Ensure Canada and Canadians with commercial interests in this burgeoning global sector are supported to grow and dominate, creating for Canada both a source of added protection and economic growth.
3. Ensure Canada is sufficiently prepared and able to participate (defend and attack) in the inevitable eclipse of warfare into the cyber realm.

The following sections explore the first two goals individually. The third stands alone and is to some extent derivative. It is, in any case, not the focus of this consultation.

Removing government from managing commercial activities beyond its own scope (e.g., operating a functioning government), government is an influencer with two powerful tools: law and money.

- **Law** – Government retains sole power to set the rules of the game. As regards cyber security, it could compel high levels of applied cyber security with ongoing upgrade requirements based on threat/risk evolution. It could compel cyber insurance, not unlike insurance to drive a car. While treaties may make it challenging, there may be no area better for invoking provisions of national security to direct government procurement toward Canadian businesses. This would include Cloud, data centre, and software providers.
- **Money** – Targeted government investment is politically challenging. It is derided by the private sector even while being demanded. The principle argument against is that government shouldn't pick and bet on technologies because it's not good at it. The argument is nonsense having been disproven at least as frequently as proven. Besides, government's bets should be on tidal swells of long-term change not immediate industrial support. Cyber security satisfies this imperative. Canada can financially support the industry in a number of ways, not least among which are: to prefer Canadian cyber security vendors and suppliers (presuming satisfactory comparable technology) in its procurement; to shape direction through targeted tax incentives and investment in cyber security innovation growth; and so forth.

I. Implement cyber security standards

Implementation of seat belt laws across the country with complementary demands on the auto industry was a critical turning point in national road safety. It forced individual consumers to behave differently (if only to wear a seat belt) and prompted the industry to make safety fundamental. Similarly, anti-dumping and other such environmental protections have been more instrumental than market forces.

Left to their own device, businesses ignore and externalize; faced with regulation, they change. And, despite instant hew and cry, structural changes set in motion rounds of innovation ultimately valuable to the primary purpose of the rules (safety) as well as for second order benefit (the economy).

When it comes to cyber threat and security, most Canadian people and businesses are woefully under-protected. Many would argue they are either not a target or have not been targeted… *because they are unaware they are and have been already*. For consumers and businesses, let alone governments, this must change. While the pain of actual suffering over a breach is usually a good trigger, it is too late. Besides, like everything else, it tends to be "one and done." Updating cyber security in 2015 is insufficient in 2016, let alone in 2017.

What can Canada do viz. cyber security?[12]

1. Legislate or regulate, as appropriate, an "uncomfortably" high standard of cyber security.
2. Legislate or regulate, as appropriate, minimum levels of cyber insurance to be carried by commercial and other entities.
3. Educate the public at large.

There are undoubtedly many other things the Government could do, but these take advantage of its strengths and use leverage for greater results.

1. An "uncomfortably" high standard

The idea of an "uncomfortably" high standard is to achieve the goal of maximum resistance and resilience while stimulating a culture of cyber safety. It would have most certain implementation and greatest effect with the Government holding itself to that high standard; even better if other governments do the same.[13] Implementing the standard will create immediate and compelling demand for update. Fortunately, at the federal level at least, this dovetails with system overhauls already underway. Using national security exemption provisions, government(s) could direct the procurement money back into the Canadian cyber security industrial ecosystem.

In addition to itself, governments should impose consistent high standards on select industrial categories where the impact will be re-directed toward a broad corporate and individual user base by regulation or legislation. Telecommunications carriers and data centre providers are one example. While many providers of these services implement and upgrade cyber security to their systems regularly, and many comply with international cyber security standards for competitive reasons, it is obviously insufficient on the whole. Their customers can choose not to maintain their own connected networks and systems at a similarly secured level, exposing weak links.

Industry will love the procurement opportunity and rail about everything else. Many will decry the added costs. It should all be ignored. Safety and security is a public good that cannot be allowed to fall to the lowest viable standard and shopped out to non-nationals. To soften the blow, mitigate some economic impact, and accelerate the process, government could match funds or provide other incentive protocols for upgrade that meets regulatory guidelines and satisfies other possible requirements.

The nature of this imposition could be system protections such as those embodied in ISO 270001 and SOC1 and 2. A strong stance could also be taken on the demand for implementation and use of a broad-based digital identity structure and federation, which would require collaboration and contribution from all levels of government and

---

[12] These recommendations are directional for shaping. Study and planning are needed.

[13] Uncomfortably high standards is a practical application of a better-argued proposal by Nassim Taleb, entitled The Most Intolerant Wins: The Dictatorship of the Small Minority. Its essence is that a small minority can impose its will on a majority. The determining factors are that the minority be more intransigent while the majority remains more flexible. Applied, in this case, with added incentive of substantial procurement money, an intransigent minority (the Government of Canada insisting on very high cyber security standards) will first bend vendors to provide to its standard. When the standard is common for the vendors it should be better priced than the lower quality alternative. Assuming high standard is more common, at least as well priced, and interoperable with government (and select industries') systems, the flexible majority—the balance of the market—will follow suit. The norm is not uncomfortable.

the private sector. A heavy-handed *demand* to create and implement such a system, respecting privacy while elevating certainty and security in (Canadian) cyberspace would be visionary.

2. Cyber insurance

Because economic incentive is particularly effective, government could continue shaping this area without putting hands on directly by demanding cyber insurance for any that operate (on) a network. In essence, by making insurance an obligatory condition to operate, like for a vehicle or certain businesses, government forces directed action into the system. Alternatively, businesses could be given the freedom to choose insurance or not, upgrade or not.

A key to such a scheme is in the nature of the regulation itself. Perhaps insurance is not compulsory; but there is an equal or larger burden on those without insurance (e.g., perhaps a regime of exempting those systems that meet minimum cyber security compliance). The choice is upgrade or insure. Such a system would need oversight to ensure compliance and prevent insurer gouging, but the market itself would ultimately assign appropriate incentives.

Insurance as a lever may not be practical. As this is provincial jurisdiction, it would require harmonized support of the provinces. The example is, however, instructive for how government need not intervene actively so much as reset the rules to incent action in a particular direction, leaving the market to work out equilibria.

3. Education

As for wearing seat belts, stopping drunk driving, smoking cessation, and so on, government is suited to play a substantial part in suasion through genuine cyber security awareness.[14] This cultural shift would have to be implemented with (educational) messaging and conditioning. Best effect would be achieved through effort and expenditure harmonized with the provinces.

A network, like a chain, is hostage to its weak link(s). In cyber threat surface is large and expanding to everyone and every device touching the network. ***It is government's social responsibility to make sure its citizens are aware of and act on the dangers.*** For cyber security it's doubly important compared to other examples because the impact and effect of damage from negligent behaviour is much broader, more akin to mass immunization.

II. Support the Canadian cyber security industry

Certainly, the commercial and research sectors of the cyber security industry will counsel the Government with how it ought to direct funding and support toward the industry in general or to a part of the industry specifically. Recommendations are sure to include increased funding, probably without strings. These are not without merit. The Government ***must*** support the *Canadian* cyber security industry.

Moral support does not count and the range of government financial support options is complex: as broad as the areas of cyber security that could be supported. At a

[14] "Genuine" cyber security awareness is a creative step up from the anodyne and apparently valueless "(cyber) security day/month" campaigns presently conducted.

minimum, presuming cyber security is recognized as a key growth sector, existing support programs ought to be modified to favour cyber security: EDC's mandate to support Canadian businesses in cyber security, consular and export support in trade and global affairs, science and innovation, etc. Other tax and granting programs should be wired toward cyber security for some period (not to the exclusion of other deserving industries, of course).

If cyber security is a priority, two broad forms of financial support are appropriate:

1. direct and specifically targeted funding through procurement, grants, investments, and tax benefits; and
2. indirect funding to support the structuring and organizing of the industry's capacity and activity.

These are themselves supported by ancillary actions such as funding the means for development of economic activity. Optimal tactics would satisfy the Government's first goal of elevating national cyber security safety and standards.

1. Direct intervention

The most important direct intervention and financial support Canada can provide to the industry is to apply a high new standard for government cyber security and then direct procurement of products and services to achieve those standards toward Canadian firms. This will inject hundreds of millions, if not billions of dollars into the industry *while* addressing the Government's underlying needs from existing budgeted expenditure. This funding will, of course, be returned to Canada as revenue, payroll, and consumption taxes. It will enable the Canadian supplier businesses to scale, become globally competitive, and ultimately turn their attention to export markets.

A word of caution. If successful, these Canadian firms would need more capital to scale for global development. If their technologies are truly valuable, they will be targets for foreign acquirers. This is happening already in this sector and has happened in others. Without a complementary means to support these growing businesses with adequate Canadian capital (private and public), the whole effort could be public risk taken for a foreign acquirer's reward.

Grants that target businesses and, more categorically, research organizations addressing today's and tomorrow's cyber security challenges is critical. Investments by the nation are appropriate where the research is primary and may not have an immediate, direct payback. It is vogue for executives and consultants to opine for *practical* innovation: that with a direct, short path to profit. It has merit, but is terminally short sighted where the (national) goal is long-term dominance in a rapidly evolving sector. There is room for businesses to practically innovate and capture ready markets, and they should be supported. But primary investment programs should ensure Canada gets to and remains at the forefront of the industry (e.g., research into quantum cryptography). This will provide the underlying technology innovation to support "practical" innovation for the future.

For all, but particularly for businesses that take advantage of research grants or other funding, two conditions are appropriate. First is a regime for protection and subsequent exploitation of intellectual property over which the Government of Canada should take some license where it is involved. Second, that the business obtaining funding for research continue to make some relative level of ongoing domestic R&D and innovation investment for a set time (years) *after* the grant. The objective is not to hamstring or penalize the organization with a repayment, but to

ensure that a one-time grant is not exploited in the short-term to the detriment of the long-term goal. Quite simply, to lead the *nation* toward a difficult-to-arrive-at end state, it is government's role to counterbalance immediacy, short-termism, and distraction with measures that weight the balance toward long-term focused decision-making that supports the nation.[15]

2. Indirect support

Indirect support is not spending free. The distinction is that this, possibly substantial expenditure is directed not at individual entities in the industry, but toward the vast network of enablers that create the capacity for a robust cyber security sector. While there are many areas worthy of support, the following two provide leverage.

There are innovation hubs across the country. These appear as accelerators and incubators, or as (non-)university-centred technology clusters. Some have begun to focus on cyber security. Among the values these entities represent are: experience, knowledge, interest, and proximity. They are in the business of helping realize cyber security innovation. These support centres need the resources to graduate the start-ups they support into genuine growth businesses. That typically means subsidized support and access to referral pools of capital. So, (i) increasing their capacity to give their "clients" support and (ii) incenting domestic venture capital in a meaningful way specific to cyber security is essential.

Technology clusters are often backed by a local economic development organization. Most directly operate local technology centres and innovation incubators. Particularly where there is already activity, as in Waterloo or Ottawa, the organization has an incentive to direct its attention toward cyber security. Either way, their core value is making connections to local resources and bringing economic development funding policy to the firm. Their local efforts to connect existing businesses and expertise to new businesses and innovation help expand resources and opportunities for both. It is in an economic development agency's interest to attract foreign entities to their jurisdictions, to incent local schools to provide appropriate human resources, and to keep start-up and growth businesses local. All of which makes them an indescribably valuable part of a "hub and spoke" lever of national policy. Above all else, they are close enough to recognize potential for economic development well before it could register nationally.

Educating the public about cyber security is important to change culture. Supporting technical education for those needed to be part of the industry is critical. There is a global dearth of expertise in cyber security. Having and *keeping* human capital in Canada is fundamental to Canadian businesses having and sustaining advantage. The educational support, likely from provincial governments, needs to be directed not only to university level science, technology, engineering, and mathematics (STEM), but more critically at the practical college level. Broad-based trade practise capability, not restricted to the approach of a single vendor, is not valuable; it is essential. And the need is pressing. A ten-fold increase in college graduates with these skills could be sustained for the next decade or more. Canadian students need to be encouraged and guided in this direction. The educational institutions need urgent support to increase capacity to deliver it.

---

[15] If the decision-making does not participate in or support the national good, perhaps that firm could find alternative funding.

3. Ancillary action

Apart from control of monetary and fiscal policy, a government's most valuable role in the economy is indirect. This typically does not require substantial financial intervention.

The ebullience of the cyber security space now is an inevitable outcome of obvious opportunity. In and of itself this is encouraging. It does, however, highlight a problematic reality: there is too much (doomed) activity. Normally, the more activity the better: probabilities become favourable. After the invisible hand has swept the less valuable off the table, the thrivers and global winners will be left. But, the industry system is not closed to Canada. So while Canadian organizations fight and struggle in overlapping, Darwinian activity, supported and coordinated extranational competitors leap ahead. That is free market capitalism—sort of. The problem is when vast amounts of government-underwritten capital disappear. Without clarity of purpose and intense, efficient coordination of support funding, the prevailing conditions lend themselves to vast waste of much needed government largesse.

With a vision extending 30-years hence (at least), the Government does not have to pick individual sectors or, especially, individual firms. In cyber security, the industrial policy the Government chooses defines how much or little the industry advances. What a government can and must do is to set the general direction the industry ought to take, the parameters of engagement, and, until the invisible hand acts more favourably (say, on an *inter*national rather than *intra*national basis), help direct development of the industry by coordinating and backstopping it. Not as a financial guarantor necessarily, but as a "coach" offsetting and limiting (and certainly not capitalizing) the tendency for individual players to pursue similar paths toward similar goals. The national government can be a means to moderate inevitable pendulum swinging that results in lurching, unfulfilled national industrial development. It can also use its heft to pave the way internationally.

National Institutes of CyberSecurity

No government has the necessary insight or skill to implement a directed economy. But every government has abundant skill and capability to constitute and nursemaid an industry *with* that industry.

In many ways the cyber security clusters/regional leaders across the country compete for attention and funding. They compete to be the dominant source of cyber security expertise and economic development. Duplication of activity could be significant. Where there are duplications of assistance/support, such double-investing may be warranted or justified on some level. Or maybe it's just inefficient—at least from a national strategy perspective. For their own, let alone the national strategic good, these Canadian technology clusters need to collaborate and cohere at this juncture.[16] There is a fundamental coordinating role/function, to direct continuity of national purpose, critically needed.

One means to achieve this would be a strategy of coordinated hubs. The National Institutes of Health Research provides an informative structural example. It would

[16] On this front, there appears to be early interest and willingness to do so.

behoove the Government to encourage and sponsor a collaborative round table of interests to loosely coordinate activity and rationally allocate national support for development and commercialization of cyber security. Should there be, say, ten interested research and commercialization centres across the country, they could be represented within a national coalition that agrees on strategies to maximize the national benefit.

Though loosely tied, the interests of these organizations would be aligned by making the organization the dominant means by which federal government support is allocated to the industry, the regions, and the sectors to the ultimate benefit of individual firms. Unfortunately, without a strong, dominant national voice for the strategic national interest, the organization could easily devolve to squabbling (regional and sub-sectoral) interests. The federal government ***cannot*** directly be that national voice at the table. That would not work either. So Government must nominate an institute with national interest as the leader. For instance, a *National Institutes of CyberSecurity* organization with an Ottawa-based entity functioning as first among equals.

It makes sense for the coordinating body to be separate not only from government but also from the interests of the others. Where regional commercial and research organizations would have particular interests, an independent organization with the national interest would be an appropriate administrator. In one formulation, this could be a substantially if not wholly public-funded, not-for-profit organization whose mandate is to provide insight and strategic policy advice and guidance on the current state and future of the industry to all levels of government and even the private sector. With no financial interest in any given sector, technology, geography, or profit-making entity, such an organization could provide impartial guidance to government and administer national interest strategies for cyber security effectively.

Export support and Team Canada

If Canada believes cyber security is an important sector to pursue for national economic growth, the goal should be dominance globally. To oversimplify the impact of that choice: Brand Canada needs cyber security woven through it. Not necessarily at the expense of other industries but with more emphasis and deployed expertise. Select Canadian trade missions have to carry this message along with Canadian businesses to lever the attributes of Canada and Canadian businesses, innovation, research, and experience in this sector to maximum effect.

Programs like those for export development would benefit from a five- or eight-year mandate to focus on cyber security development. This incubation period, given the other activities described herein, ought to be abundant for Canadian industry to find a strongly competitive global footing. As typical for all innovation and technology clustering, whether at a local or national level, widespread success needs ongoing attention but can become self-perpetuating. At that point Canada can redirect export focus onto other key sectors.

Conclusion

There will undoubtedly be much insight and information in the submissions to this Consultation on Cyber Security: data and recommendations that address every relevant area of concern to Canada about the (Canadian) cyber security

environment. With these insights, the Government should be abundantly prepared to make specific decisions about the evolving cyber security world within its purview.

The most important take-away, bar none, is that at this juncture the Government of Canada is in a position to choose a direction and strategy that not only enhances its own protective measures over its own domains, but also:

1. Enhances the practical and cultural state of Canadians' attitudes and behaviours toward cyber security.

2. Supports the Canadian cyber security industry to become a dominant global player.

3. Prepares Canada to participate as warfare evolves farther into cyber.

The choices today are the steppingstones to tomorrow.