National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

A NON-DISRUPTIVE STATUS QUO: THE ABSENT CANADIAN MODEL FOR CYBER FORCE DEVELOPMENT

LCol P.F. Szabunio

JCSP 40

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 40

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 40 – PCEMI 40

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

A NON-DISRUPTIVE STATUS QUO: THE ABSENT CANADIAN MODEL FOR CYBER FORCE DEVELOPMENT

LCol P.F. Szabunio

Word Count: 3803

Compte de mots: 3803

TABLE OF CONTENTS

A NON-DISRUPTIVE STATUS QUO: THE ABSENT CANADIAN MODEL FOR CYBER FORCE DEVELOPMENT

> *There is something about the way decisions get made in successful organizations that sows the seeds of eventual failure.*
>
> — Clayton M. Christensen[1]

Introduction

Just as the sailor must become familiar with the natural rhythm of wind and wave, the soldier with the undulations and features of ground, and the airman with Bernoulli's principles of flight, so too must the cyberwarrior master the implicit laws of cyberspace.[2]

While the concept of *disruptive innovation* is not the sole purview of cyberspace, it is perhaps one of the more fertile mediums through which its effects are readily apparent. Online stock trading and retailing, electronic bourses like the TSX, e-Cards, distance learning programmes, and ever-more sophisticated applets running open-sourced internet-based software, are all examples of disruptive technologies sprouting from the cyber realm.[3] And, just as dual-purpose civil-military technology has held disruptive effect upon the past conduct of warfare (e.g. the tank, powered flight, wireless, etc.), so too will disruptive cyber technologies affect future military operations.

This paper applies Harvard's Clayton Christensen's, and Deloitte Consulting's Michael Raynor's,[4] *Innovator's Dilemma and Innovator's Solution* models (ID/IS)—that

---

[1] Clayton M. Christensen, *The Innovator's Dilemma* (New York: HarperBusiness, 2000), xv.

[2] Throughout this essay, the terms 'cyberwarrior,' 'cyberspace,' etc. are applied within a colloquial meaning: unless explicitly noted otherwise, arguments for or against the domain distinction of cyberspace (as a realm of military operation as distinct as sea, land or sky), fall beyond the scope of this work to develop.

[3] *Ibid*., xxix. A good recent example of the disruptive construct in action is 3-Dimensional Printing, and how it has potential to upend traditional manufacturing across a host of civilian and defence applications, including the arms and weapons trade.

[4] Clayton Christensen is a renowned Harvard Business School professor who pioneered thought on the concept of disruptive innovation in the mid-1990s through his seminal work, *Innovator's Dilemma*. Canadian post-doctoral student Michael Raynor, a research strategist with Deloitte Consulting Canada, and

anticipate and cope with disruptive innovation—to draw holistic insight if the Canadian Force's (CF) current cyber operations organisational strategy and structure can succeed, or not.

This essay is structured in two parts. First, it discusses the ID/IS concept as a model applicable to military thought. Then, it briefly examines open-source information for current and planned CF cyber operating structures in order to discuss the fit or divergence of expressed CF ambitions from the model's theoretic optimum. The initial hypothesis posits that the CF occupies a middling ground, where success will happen only through dint of brute force and command will, and not by any particular deliberate adherence to what ID/IS theory might suggest be done.

The Innovator's Dilemma and Innovator's Solution as Models for Military Thought

Christensen defines *disruptive innovation* as:

> [A] process by which a product or service takes root initially in simple applications at the bottom of a market and then relentlessly moves up market, eventually displacing established competitors . . .. [It] allows a whole new population of . . . [users] at the bottom of a market access to a product or service that was historically only accessible to . . . [upmarket users] with a lot of money or a lot of skill.[5]

---

adjunct professor at the Richard Ivey School of Business (Western), co-partnered with Christensen in follow-up to *Innovator's Dilemma*, with the *Innovator's Solution*.

[5] Clayton Christensen, "Disruptive Innovation – Key Concepts," last accessed 13 May 2015, http://www.claytonchristensen.com/key-concepts/. A 'litmus test' to assess and identify if a disruptive opportunity exists is to ask: Does the product or idea compete against non-consumption – does it underperform existing products or exist in uncertain and ill-defined markets? Does the product or idea help users more easily and effectively do what they are already trying to do? Is there a segment of users that are currently 'overserved' by the existent product or idea; and Can you create a different, low cost, simplified and more responsive business model? Michael Raynor, "Growth and Innovation in Established Firms" (Business 600 course lecture, Richard Ivey School of Business – University of Western Ontario, London, ON, January-February 2003).

In their nascent stages, disruptive technologies offer little functional benefit that established technologies don't already meet or exceed—think of the cumbersome and unreliable nature of early tanks relative to cavalry and horse-drawn guns. As such, the disruptive threat to status quo ideas, structures, and operating norms is not readily discerned, especially to well-established, -regarded, and -run professional organisations and businesses.

However, by exploiting a seemingly uninteresting niche where there is no immediate demand for the good or service provided—by introducing something that is already served by other evident means into an under-served market segment (often with worse performance than incumbent solutions)—the idea *gains* traction to resolve a problem the user never realised it was trying to solve. Through Darwinian emergence, this 'good enough' idea soon nips at the heels of established paradigms or technologies, much to the surprise of stable, long-standing, and well-functioning organisations, as Figure 1 illustrates.

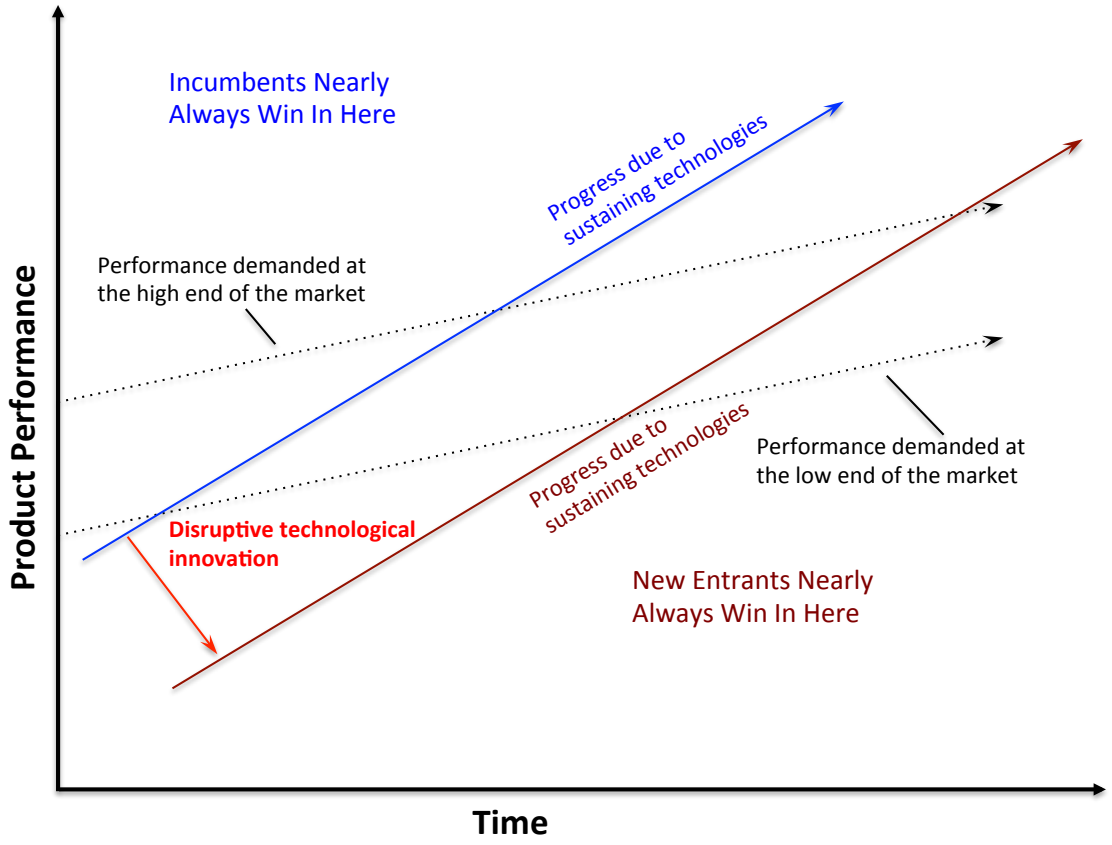

Figure 1 – The Impact of Sustaining and Disruptive Technological Change
Source: Adapted from Christensen, "The Innovator's Dilemma . . .," xix.

The somewhat insidious nature of disruptive innovation drives the *innovator's dilemma*, where "the logical, competent decisions of management that are critical to the success of their [organisations] . . . are also the reasons why they lose their positions of leadership."[6] This assumption is particularly true as both institutionalised and informal systems, by which established entities prioritise their energies and resources, simply do not allow them to pay attention to niche ideas, despite logic saying these ideas "might be big someday."[7]

It is not lack of will or intellect to deal with these emergent threats to the established status quo that undermines the leading idea or structure's dominance; it is

[6] Christensen, "The Innovator's Dilemma . . .," xvi.
[7] *Ibid*., xxv.

merely that organisations can rarely succeed at doing two antithetical things at once—they are good at what they do plainly because that is what they are good at; not easily does the leopard change its spots, so being something other than what drives the very heart of their success simply cannot work.[8] This precept applies as much to those who provide the new technology or idea, as it does to those who *consume* that idea or service.[9]

The Innovator's Solution

This dilemma created by organisational confinement—i.e. how the structures that made an incumbent highly successful within existent operating conditions, but now inhibit disruptive responsiveness—is resolved through an "*Innovator's Solution* that espouses independent action, and a vibrant cultural dynamic . . ., [aspects that are] anathema to most military structures."[10] Within the narrow scope of this essay, the aspects of IS theory most militarily relevant relate to organisational Resources, Processes and Values (RPV); strategic adaptation; and the criticality of executive influence, as discussed next.

IS theory first considers organisational capability to exploit or absorb the emergence and effects of a disruptive technology through the adaptability of its endemic

---

[8] *Ibid.*, 131-132.

[9] For example, consider the military's role as a *consumer*, and how the simpler and lesser quality VHS video format eventually came to dominate the qualitatively superior Betamax format in the 1980s. Had the CF made decision to invest primarily in the higher-end Betamax technology to the exclusion of VHS, the subsequent conversion costs back to the widely-adopted (lower-market) VHS standard would have been astronomical. Similar effects are evident today, for example, Canadian military computers as possibly being one of the last working refuges of 3.5" floppy disc drives, now rendered obsolete by flash drive technology.

[10] Lieutenant-Colonel Paul A. Szabunio, "Military Responses to Malicious Cyber Activities," (Joint Command and Staff Programme (Distance Learning) CF549DL – Advanced Topics in Campaign Design Forum Discussion, Canadian Forces College, April 2015). Emphasis in original.

RPV, with the human resource being foremost.[11] When selecting the leadership for disruptively competitive operational units, too often the choice is based on a sequential record of "right stuff" successes (i.e. good communicator, decisive, personable), rather than experiential determinants of success.[12] In military parlance, this criterion implicitly speaks to annual performance assessment measures focused on career ascension within the narrow confines of a trade-directed path, rather than a broader view of successes and lessons from *failure* that might be more relevant to the new disruptive paradigm.

These same managers, now leading organisations within disruptive contexts, then rely on using the operating processes most familiar to them, that well-served their previous career-driven ascendency. While it seems intuitive to apply what one already knows to a new environment, "very often the cause of a new venture's failure is that the wrong processes were used to build it."[13] An example is the annual budgetary funding priority allocations to organisational elements where the default value-for-money equation is *prima facie* evident, rather than to uncertain projects where more innovative (and disruptively relevant) thought may be present.

Leadership values bias the structural worldview within which decisions and actions are prioritised, ranging from organisational ethics and behaviours, to determining which high payoff targets we attack or bypass. In the disruptive context, this factor

---

[11] "Of all the resource choices required to . . . [be successful], the one that most often trips a venture up is the choice of its managers . . .. We have examined innumerable failed efforts to create new-growth businesses [or to compete in such a dynamic] and would estimate that in as many as half of these cases, those close to the situation judge that . . . the wrong people had been chosen to lead the venture." Clayton M. Christensen, and Michael E. Raynor, *The Innovator's Solution* (Boston: Harvard Business Review Press, 2003), 178.

[12] Christensen and Raynor, "The Innovator's Solution . . .," 179-180.

[13] *Ibid*., 184. "Managers can only do what makes sense to them, given the context in which they work." *Ibid*., 203.

drives the question of which ambiguous areas of interest are attractive to pursue or not.[14] The leader of any disruptive (or counter-disruptive) venture is judged on success and is emulated by those within the organisation who see such, so organisational culture becomes a "powerful management tool . . . [that] enables employees to act autonomously and . . . consistently."[15] The goal thus becomes to define where this culture can be fully realised, and where the disruptive element fits within the overall organisational structure, as Figure 2 illustrates:

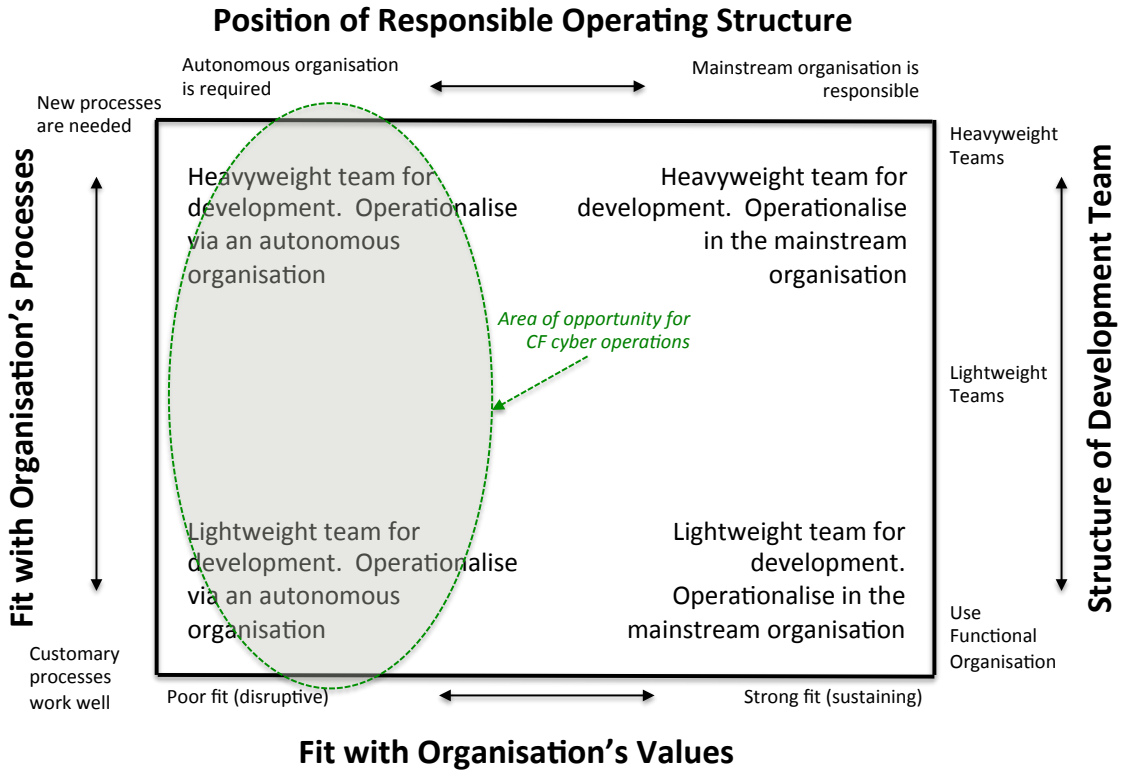

Figure 2 – Framework for Finding the Right Organisational Structure and Home
Source: Adapted from Christensen, "The Innovator's Dilemma . . .," 203; Christensen and Raynor, "The Innovator's Solution . . .," 191; and Raynor, "Growth and Innovation . . ."

From this base understanding of RPV, strategic adaptation then occurs in one of two ways: either as top-down command-vision directed through a process of deliberate

[14] *Ibid*., 185.
[15] *Ibid*., 189.

analysis and planning (like the military's Strategic or Operational Planning Processes); or as bottom-up, innocuous, free-form initiatives that hold the seeds for disruptive potential (see Figure 3). The dilemma thus becomes to recognise disruptive opportunity (very difficult to predict by definition) by selecting a proper strategic tack, while not starving such emergent ideas from proper structures to nurture them.[16]

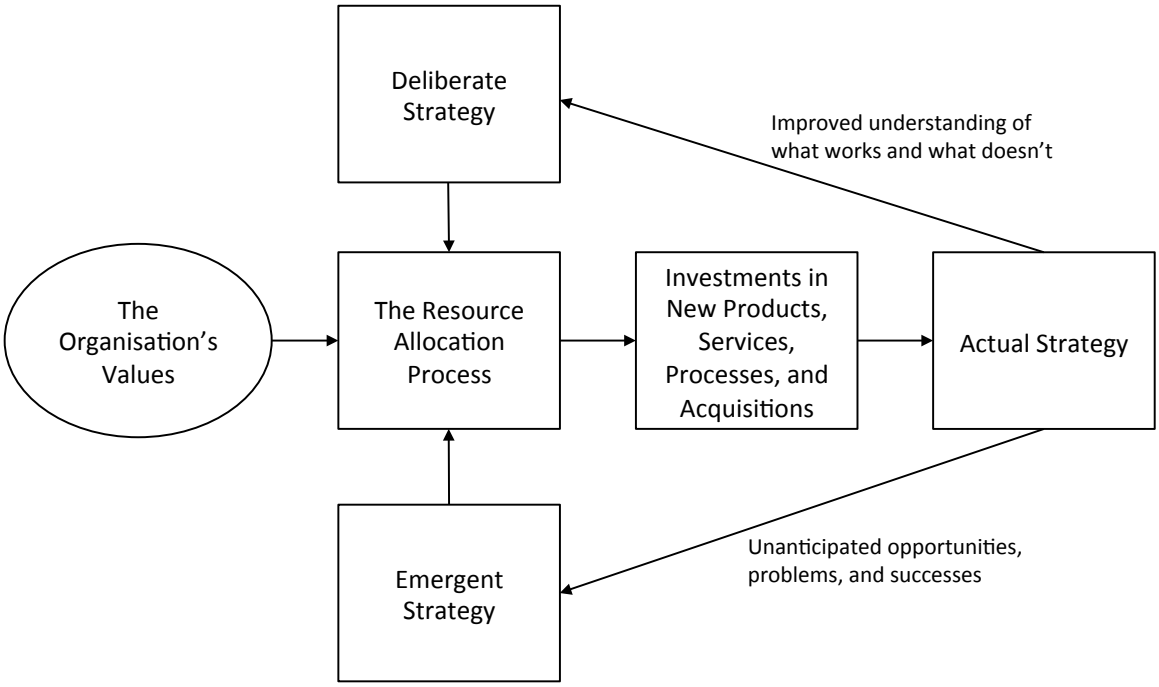

Figure 3 –The Process by Which Strategy is Defined and Implemented
Source: Christensen and Raynor, "The Innovator's Solution . . .," 215.

Complex adaptive systems (CAS) theory suggests how to resolve this dilemma:

> Those seeking to enable success of integrated teams . . . should shift their focus from attempting to structure and control individuals' duties and functions to providing the conditions for emergent evolutions and, in particular, to reframe the managerial role as one who scans the adaptive social system to detect self-organization and the establishment of the few simple rules that explain the teams' interactions.[17]

[16] *Ibid*., 216.
[17] Alan Okros, John Verdun, and Paul Chouinard, "Complex Adaptive Systems," in *The Meta-Organization* (Toronto, ON: Defence Research and Development Canada, 2011), 44-45.

In other words, ID/IS theory operationalises CAS perspective by offering insight as to how the deliberate vs. emergent process dichotomy can be managed (Table 1). The leadership challenge is thus to implement process conditions through which viable strategy can emerge, be sustained, and motivate behaviours within the considerations of cost structures, discovery-driven planning, and an appropriate fusion of deliberate with emergent strategic planning.[18]

Sustaining Innovations: Deliberate Planning	**Disruptive Innovations: Discovery-Driven Planning**
(Note: decisions to initiate these projects can be grounded on numbers and rules).	(Note: decisions to initiate these projects should be based on pattern recognition).
1. Make assumptions about the future.	1. Make the targeted financial projections.
2. Define a strategy based on those assumptions, and build financial projections based on that strategy.	2. What assumptions must prove true in order for these projections to materialise?
3. Make decisions to invest based on those financial projections.	3. Implement a plan to *learn* – to test whether the critical assumptions are reasonable
4. Implement the strategy in order to achieve the projected financial results.	4. Invest to implement the strategy.

Preference for Predictability Within an Understood Status Quo ⟷ Willingness to Assume Risk and Uncertain Outcomes

Table 1 – A Discovery-Driven Method for Managing the Emergent Strategy Process
Source: Adapted from Christensen and Raynor, "The Innovator's Solution . . .," 228.

The catalysing influence of executive leadership is critical to set the operational tone within disruptive environments. Generals play a three-fold role here: to personally adjudicate between sustaining and disruptive opportunities and choose which to exploit;

[18] Christensen and Raynor, "The Innovator's Solution . . .," 230-231.

to create and grow the 'disruptive growth engine' that identifies and exploits such opportunities (see Figure 4); and to maintain sufficient situational awareness to react to changing circumstance.[19] This growth engine, which provides essential organisational capability to identify and/or exploit disruptive opportunity (or counter against hostile external disruption), requires an individual with sufficient political clout to challenge status quo processes and lead change.[20]

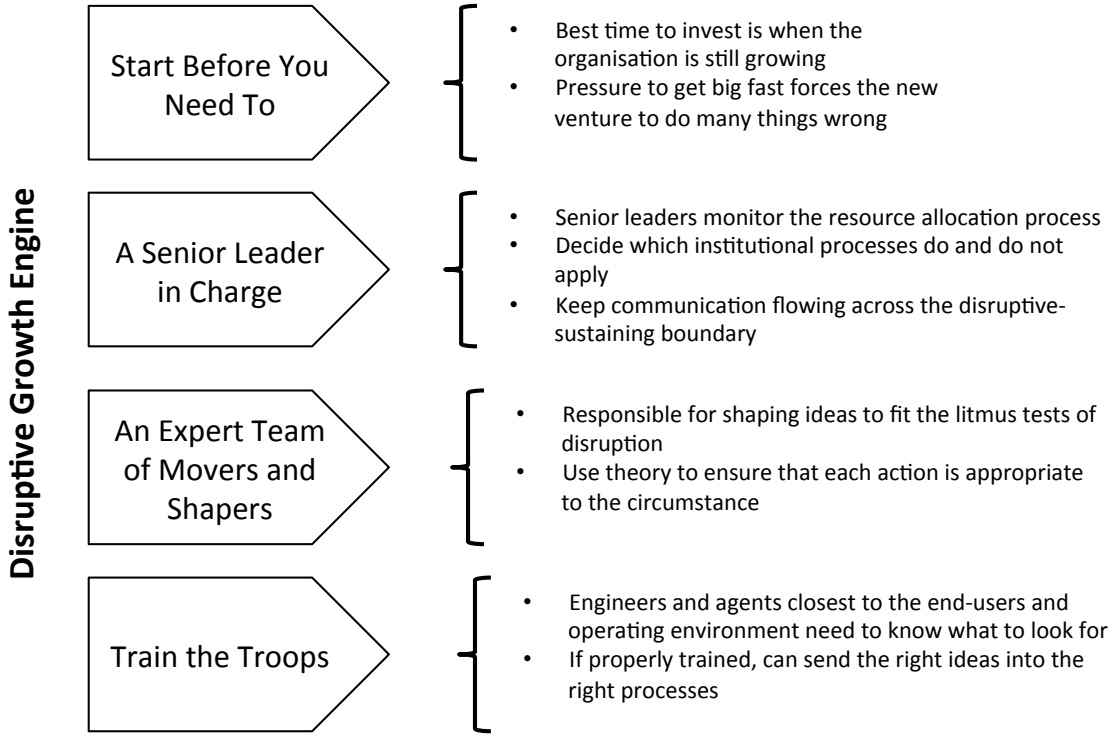

Figure 4 –The Disruptive Growth Engine
Source: Adapted from Christensen and Raynor, "The Innovator's Solution . . .," 279.

In other words, managing disruptive change, or conducting military operations within an environment ripe with such, is as much about leading change as it is about

[19] *Ibid*., 267.
[20] *Ibid*., 277.

kinetic targeting.[21] Senior executives managing the complexity of innovation must: actively coordinate decision-action processes where none otherwise exist; break free of status quo processes when new patterns of communication and thought are needed; impose new process discipline where sensible; and they must cultivate a learning environment where reasoned failure is seen as *opportunity* to support disruption, and not as something to be viewed as career-limiting.[22]

Relevance to Military Cyberoperations

In closing the first half of this essay—where ID/IS theory was introduced as a model for military thought—it is important to acknowledge that some may criticise it as irrelevant to contemporary warfare or military organisational design strategy. For example, Libicki speaks to centralising and standardising interoperability, protocols, technology, and knowledge sharing within the United States military as part of its overall information management (i.e. cyber) strategy.[23] While Libicki acknowledges the benefits to information management within the military being de-centrally organised via an "Internet-like [distributed-cum-disruptive] approach,"[24] he also plays devil's advocate, noting that market logic (from which ID/IS theory is derived), may not readily apply to the military context, where orientation toward a common command-based goal takes precedent over the individualist, and money-driven, capitalist desires.[25]

---

[21] See: John P. Kotter, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review* 73, no. 2 (March/April 1995): 59-67.

[22] Christensen and Raynor, "The Innovator's Solution . . .," 282. Arguably, traditional military progression models tend to penalise, not reward, such behaviours.

[23] Martin C. Libicki, *Who Runs What in the Global Information Grid: Ways to Share Local and Global Responsibility* (Santa Monica, CA: RAND Corporation, 2000).

[24] *Ibid*., iii.

[25] *Ibid*., 15. Libicki questions if market influences are the best way to assess and equip military forces, and that market logic cannot readily superimpose to military needs: "Markets do not work unless

Laudable as this view may be, it is naïve to pretend capitalism's 'invisible hand' has any less influence on the military than it does over any other aspect of global society. Military structures do not operate in island-like isolation from the economic sea of the nation state within which they float. Many other forms of intangible capital exist, such as goodwill, political favour, and self-serving agendas, all of which are amenable in permutation to the ID/IS framework. Information, including disruptive information, like any other good, is subject to the same principles of supply and user demand that drives most human interests.

From the basis this framework link between business theory and military organisational strategy provides, the next section reviews the CF's current state for cyber organisation, and what the ID/IS framework suggests about its chances for success.

Fits and Gaps – How Well does CF Ambition Align to a Theoretic Optimum?

In seeking to assess CF cyberstrategic alignment to the ID/IS disruptive strategy model, this author was challenged by the paucity of open-source information against which to concretely review CF structure, planning, progress, or executive capabilities. While much opinion and conjecture about CF cyberstrategy exists, little is of scientific or academic rigour. The second half of this essay thus acknowledges this limitation, and applies what little is known to draw qualitative inference on the present state of affairs. An evaluative structure echoing the prior *Innovator's Solution* section is used,

---

people have something to spend, which raises the question of who starts off with what resources. [. . .] Having unit commanders bid against each other to receive, for instance, UAV coverage, cannot help but yield results that are bizarre from a military point of view . . .. [T]he moral fit between market forces and militaries is poor. Militaries are hierarchies for a reason. Command relationships have to be unambiguous. Everyone works for a common goal, not individual ones." *Ibid*.

considering the CF cyberstructure's RPV, adaptive capability, and executive stewardship to divine if a sustaining, or disruptively agile, course is seen.

Resources, Processes and Values (RPV)

The Chief of Force Development (CFD), under the Vice Chief of Defence Staff, is responsible for CF cyberstrategy via the recently created role of Director General Cyber (DGC).[26] CFD harmonises, synchronises, and integrates all CF force development activities "to develop the capabilities required to produce strategically relevant, operationally responsive, and tactically decisive military forces."[27]

DGC develops CF capability "to operate more effectively in the cyber environment writ large."[28] Barring a defence of Canada scenario, DGC's activities with other governmental agencies, provinces, or territories remain subordinate to the overall coordination of Public Safety Canada (PSC), or the Communications Security Establishment Canada (which reports separately to the Minister of National Defence).[29] DGC maintains information management and signals intelligence liaison with the

[26] Parliament of Canada, The Standing Senate Committee on National Security and Defence, *Minutes of Proceedings and Evidence*, 05 November 2012, 1/16, last accessed 16 May 2015, http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-e.HTM.

[27] Department of National Defence, "Vice Chief of the Defence Staff," last modified 18 November 2014, http://www.forces.gc.ca/en/about-org-structure/vice-chief-defence-staff.page.

[28] Parliament of Canada, "Minutes of Proceedings and Evidence . . .," 1/16. Following analysis by the ad hoc CF Cyber Task Force stood-to in September 2010—mandated to optimise current cyber capabilities (people, processes, equipment, tools), while setting the conditions for cyber force development, generation and employment—DG Cyber (DGC) was established in April 2011 under the lead of a Brigadier-General military officer. DGC's primary role is to identify and develop future cyber capabilities along four lines of effort: a) Cybersecurity policy support in partnership with Public Safety Canada; b) Developing operational-level cyber command and control capability; c) Resource capability building and synchronisation of the various CF cyber programming; and d) Human Resource training, development, and retention. *Ibid.* 2/16.

[29] *Ibid*., 6,8/16.

Assistant Deputy Minister-Information Management (ADM(IM)), and the operational-level CF Information Operations Group (CFIOG).[30]

Determining a projected funding envelope is a critical start point before playing in a disruptive environment (Table 1). For example, within PSC's *Action Plan 2010-2015*, the consolidation of IT/IM[31] services and management under Shared Services Canada (SSC) is noted as an important first step to enhancing national cybersecurity,[32] inclusive of the CF Cyber Force. But security experts have already claimed that SSC's "seven-year, $245-million [consolidation] plan doesn't set aside anywhere near enough investment to adequately prepare government for the online threats it is facing."[33] In other words, the up-front ID/IS strategy budget piece is short-changed from the start.

Another critical aspect is the Cyber Force Human Resource (HR) attraction and retention processes and strategies. Cyber's volatile and complex networked environment demands that HR techniques "constantly adapt."[34] DGC has acknowledged that a different approach to generate the Cyber Force is needed, and while existent HR systems provide short-term relief, longer-term structural changes to HR are required.[35]

---

[30] Lieutenant-Colonel Jason Walkling, "Considerations: Canadian Forces' Efforts in the Electromagnetic Spectrum and Cyber Operating Environment," (Joint Command and Staff Programme Master of Defence Studies Research Paper, Toronto: Canadian Forces College, 2013), 65.

[31] Information Technology; Information Management.

[32] Public Safety Canada, *Action Plan 2010-2015 for Canada's Cyber Security Strategy* (Ottawa: Queen's Printer, 2013), 1. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx.

[33] Vito Pilieci, "Cyber security a non-stop headache for federal government, conference hears," *Ottawa Citizen*, 29 October 2014, last modified 29 October 2014, http://ottawacitizen.com/business/local-business/cyber-security-a-non-stop-headache-for-federal-government-conference-hears.

[34] Sylvain Leblanc, *Human Resources Issues Currently Affecting the Development of the CAF Cyber Force: Technical Report ECE-2013-01, Computer Science Laboratory* (Kingston: Royal Military College of Canada, January 2013), 6.

[35] Brigadier-General Greg Loos, in Parliament of Canada, "Minutes of Proceedings and Evidence . . .," 5/16.

The Cyber Force needs: operators; weapon system and equipment support teams; planning and command staff; and lastly, cyber commanders themselves.[36] With initial seeding from the existent military population itself, the risk is that the same ideational skills the Cyber Force needs to grow are also in direct competition with Canadian industry.[37] Some have posited this 'flight risk' can be mitigated by sourcing candidates well-versed in the necessary competitive market dynamic from the extant Reserve Force community.[38] However, while patriotic commitment is not to be underplayed, it is a leap to expect Reservists to readily leave stable and well-paying positions for a new venture run by a traditionally bureaucratic and compensation-capped employer.[39] To successfully compete against this dynamic, military HR has no alternative but to use financial and career-mobility incentives to attract the necessary talent.[40]

If empirical data is anything to go by, things do not bode well for future Cyber Force recruitment and retention, as the lukewarm ADM(IM) and CFIOG Public Service Employee 'proxy' survey highlights in Table 2:

---

[36] Leblanc, "Human Resources Issues . . .," 7.

[37] *Ibid*., 8.

[38] Walkling, "Considerations: Canadian Forces' Efforts . . .," 101.

[39] Lieutenant-Colonel Paul A. Szabunio, "Developing a Cyberagenda – Vision for Command and Control of Cyber Operations," (Joint Command and Staff Programme (Distance Learning) CF549DL – Advanced Topics in Campaign Design Forum Discussion, Canadian Forces College, April 2015).

[40] Leblanc, "Human Resources Issues . . .," 17. To enhance Cyber Force force generation, "[f]inancial incentives (such as signing bonuses, specialist pay and allowances) should also be investigated. Those individuals who are selected from within the CF, or those who are recruited into the CF, who already have higher education or work experience directly applicable to the Cyber Force must be able to "leap frog" over portions of the education or training offered by the [formal military programmes of the Cyber Centre of Excellence]." *Ibid*. Culturally, the Cyber Force will differ from the CF mainstream, where hierarchy, is likely to be more in line with the Special Operations Force model, where the lead is based on expertise rather than rank. *Ibid*., 13.

Survey Question	ADM(IM)	CFIOG
Q. 17 – I am encouraged to be innovative or to take initiative in my work. (*somewhat or strongly agree*)	70%	69%
Q. 40 – I have confidence in the senior management of my department or agency. (*somewhat or strongly agree*)	57%	52%
Q. 41 – Senior management in my department or agency makes effective and timely decisions. (*somewhat or strongly agree*)	46%	39%
Q. 45 – My department or agency does a good job of communicating its vision, mission and goals. (*somewhat or strongly agree*)	61%	57%
Q. 61 – Do you intend to leave your current position in the next two years? (*no*)	37%	41%

Table 2 – 2014 Canadian Public Service Employee Survey: ADM(IM) and CFIOG

Source: Adapted from Treasury Board of Canada Secretariat, "2014 Public Service Employee Survey Results by Question for Assistant Deputy Minister (Information Management); and Canadian Forces Information Operations Group (Units & Detachments)," last modified 13 January 2015, http://www.tbs-sct.gc.ca/pses-saff/2014/results-resultats/bq-pq/03/370/org-eng.aspx; and http://www.tbs-sct.gc.ca/pses-saff/2014/results-resultats/bq-pq/03/370/379/org-eng.aspx.

Strategic Adaptation

"[I]nnovation is rarely driven from internal military leadership and is usually derived from civilian intervention within the military structure . . .."[41] Recent industry, academic, and government partner initiatives responding to Canadian cybersecurity concerns bear out this maxim. Innovation to secure and defend critical infrastructure poses a number of daunting challenges to overcome, including:

[41] Stephen Peter Rosen, in Samuel T. Mitchell II, "Identifying Disruptive Technologies Facing the United States in the Next 20 Years," (Master of Military Art and Science Research Paper, Fort Leavenworth, KS: United States Army Command and General Staff College, 2009), 13. "Military planners who spend most of their time considering unanticipated battlefield events are not necessarily worrying about the unanticipated *disruptive* challenges that could cause those forces to be swept off the battlefield." Terry J. Pudas, "Disruptive challenges and accelerating Force transformation," *Joint Force Quarterly* 42 (3rd Quarter 2006): 45.

- Traditional and ineffective approaches focused on prevention, risk management, and deterrence through accountability;
- Lack of coordination between industry, academia, and government;
- Fractured cybersecurity research and development;
- Research silos that hinder interdisciplinary scientific development;
- Overemphasis on cybersecurity's technical aspects over its social aspects;
- Firewalls between classified and unclassified industry, academia, and government information domains;
- Lack of education and training programs in cybersecurity;
- Few Canadian businesses in the global cybersecurity space;
- Under-investment in cybersecurity research and commercialisation relative to other jurisdictions;
- Slow and uncoordinated government responses to addressing cyberattack sources; and
- Stifled innovation through bureaucratic governmental contracting processes and procedures.[42]

One Canadian initiative to emerge to counter these obstacles is "Venus," a multi-agency collaboration, structured similar to what ID/IS theory might suggest appropriate (Figure 5). This initiative recognises that cross-disciplinary collaboration and partnership

[42] Tony Bailetti, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh, "Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity." *Technology Innovation Management Review* 3 no. 8 (August 2013): 7-8, http://timreview.ca/article/711.

is essential as the "cybersecurity challenge transcends the abilities of any single organization or individual to address alone."[43]

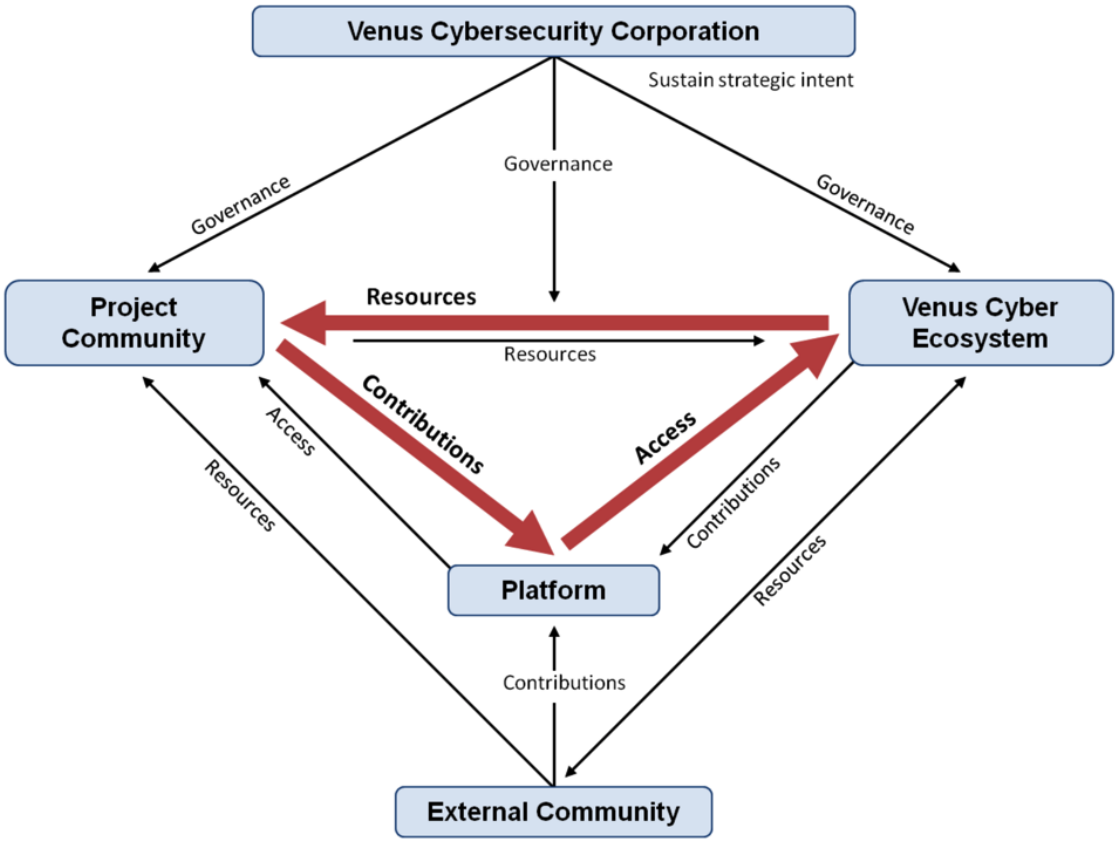

Figure 5 –Relationships Among the Five Key Entities in the Venus Innovation Engine
Source: Bailetti *et al*, "Developing an Innovation Engine . . .," 11.

Regardless if Venus is the appropriate initiative or design to pursue or not, the CF's absence from such innovation-focused partnerships is notable. In the limited scope of this essay, no CF analogue to the Venus project could be found beyond existing and traditional JIMP/other governmental department (OGD) partnerships. This outcome

[43] *Ibid*., 13. Initial partners in the VENUS project included the City of Ottawa, Ontario government, Communications Security Establishment Canada, the National Research Council, and Telus Corporation. Kate Porter, "Cybersecurity non-profit finds home in Ottawa suburb," *CBC News*, 05 November 2013, last updated 05 November 2013, http://www.cbc.ca/news/canada/ottawa/cybersecurity-non-profit-finds-home-in-ottawa-suburb-1.2415303.

regrettably suggests, despite executive rhetoric to the contrary, that the CF's existent operational paradigm is on a *sustaining*, and not a disruptive, trajectory.[44] Recent reports that suggest the military has already been excluded from the Whole of Government cybersecurity table also support this view:

> [I]nternal emails suggests [*sic*] the military recommended a more robust role for itself when the government was finalizing its cyber security strategy about five years ago. But years of a "conciliatory approach" with the National Cyber Security Directorate [NCSD] inside Public Safety has 'gotten us to our current situation. [. . .] Four years of peaceful coexistence and deferring to . . . NCSD has in fact led to us losing ground so that our strategic partner is now the sole recognized lead for dealing with attacks against the nation through cyber. . .. My experience tells me that if you continue down this path, you will drive DND/CF entirely out of the cyber ops business.'[45]

PSC's current strategy to leverage existent JIMP/OGD partnerships suggests, again, pursuit of a sustaining trajectory along a well-worn path.[46] As such, Ottawa's cyberstrategy is ensconced firmly in the upper-right quadrant of Figure 2's *Organisational Home* framework, instead of the upper- or lower-left where it needs to be. DGC's own commentary betrays this potentially flawed positioning, noting the "approach is to avoid treating anything cyber as fundamentally new and instead seek to integrate our cyber activities into existing planning and operational frameworks as fully

---

[44] While recent CDS guidance indicates that Cyber is a priority, there is little open evidence of what has been put into place, beyond 'more of the same:' "*In conjunction with government partners* [emphasis added], the CAF will initiate the development of the cyber force required to conduct operations in the cyber domain, as it does in the land, sea, air and space domains, in order to best support all CFDs mission areas," Department of National Defence, *Chief of Defence Staff Guidance to the Canadian Armed Forces* (Ottawa, ON: Chief of the Defence Staff, 2013) 13, https://www.cfmws.com/en/AboutUs/MFS/NewsandUpdates/Documents/CDS_Guidance_to_the_CAF_EN_REV4.pdf.

[45] Major P.J. Kendall on the cyber security strategy's action plan, quoted in Jordan Press, "Canada's military squeezed out of cyber-defence, emails warn," *Postmedia News,* 12 March 2014, last modified 12 March 2014, http://o.canada.com/news/national/canadas-military-squeezed-out-of-cyber-defence-emails-warn.

[46] See: Public Safety Canada, "Action Plan 2010-2015 . . .," 4.

as possible."[47] As Christensen has shown, pursuing a sustaining strategy, while trying to reinvent oneself in a disruptive environment, does not work.[48]

The Criticality of Executive Influence

The last ID/IS theory aspect considered is the biographic makeup of key Cyber Force executive leadership. Understanding this sensitive terrain allows us to infer institutional bridging capacity between the tensions of sustaining and disruptive trajectories, and, if an independent disruptive operating engine for the CF, per the ID/IS model (Table 1 and Figure 4), can be established.

The dedicated personal leadership of ADM(IM) and DGC is a bright spot in CF preparedness to grow and sustain the Cyber Force. Rarely do individuals rise to this level of executive trust without having demonstrated competence and commitment to Canadian ideals in their own right. Yet, circumstantial evidence suggests that those who recently occupied these critical roles have ascended largely within the predictively institutional confines of routine bureaucratic progression. While professional dedication is a necessary condition to steward institutional-level disruptive growth, it is not a sufficient condition in and of itself.

---

[47] Brigadier-General Greg Loos, quoted in Parliament of Canada, "Minutes of Proceedings and Evidence . . .,", 2/16. Interestingly, this view is somewhat contradicted in the continuation of DGC's testimony when it is indicated that the new Cyber Force will "require new processes and procedures, new training at all levels and a different way of thinking." *Ibid*.

[48] Consolidation within an existent collaboration (where multiple OGDs make no adaptation to existing operating models) will not work when it comes to establishing new and disruptive, or disruptive-capable, ventures. Using a market example, F.W. Woolworth department stores attempted to get into the newly-disruptive discount retailing market space by opening its 'Woolco' brand in the late 1960s/early 1970s. Rather than treating Woolco as a separate entity with a separate cost structure and business model, Woolworth tried to economise operations by having the two organisations share background infrastructure and systems. As such, the disruptive entity fell under the institutional influence of the established incumbent and was unable to grow or compete independently on its own merits, and was eventually closed down. Christensen, "The Innovator's Dilemma . . .," 128-133.

The incumbent ADM(IM)'s strong CV includes military (Reservist) and civilian business consultant perspectives, which probably provide valuable insights into the institutional- and civilian soldier-warrior mindsets.[49] While the senior leadership, expert team, and training capacity of Figure 4's *Disruptive Growth Engine* are seemingly present, the incumbent's professional background seems limited by an absence of truly disruptive or dynamic entrepreneurial experience that would indicate amenable understanding of disruptive management as the IS model demands. While the ADM's civilian IT business perspective no doubt gives him a lexicon upon which to build, such was gained largely as a consultant providing arguably sustaining-type business services, and not disruptive changes *per se*.[50]

Both recent DGCs have similar career ascendency profiles reflective of sustaining institutional trajectories, but not necessarily indicative of past failures or experiences that would provide the necessary insights a disruptive venture needs.[51] This is not wholly a handicap, as in terms of RPV and strategic adaptability, this setup has the benefit of giving them the high visibility and pan-departmental coordinative tools that are required to bridge gaps between sustaining and disruptive aspects of the new Cyber Force (see Table 1).

---

[49] Department of National Defence, "Leonard (Len) J. Bastien – Biography," last modified 27 July 2014, http://www.forces.gc.ca/en/about-org-structure/assistant-deputy-minister-information-mgmt-bio.page.

[50] For example, compare the services at Innosight Consulting at http://www.innosight.com, and the ADM(IM)'s prior consultancy at CGI at http://www.cgi.com/en. The incumbent's experience in rationalising service provision to grow departmental capacity demonstrates progress along the sustaining vector of an established business model (see Figure 1), but little to demonstrate intimate understanding of constructing a dynamic hub of innovation that an innovation vector requires.

[51] See: Department of National Defence, "Commander JTFN – Brigadier-General Loos, G.D., OMM, CD," last modified 21 June 2013, http://www.cfna.forces.ca/info/com-eng.asp; and The Nauticapedia, "Biographical Data – Hawco Darren," last updated 26 May 2014, http://www.nauticapedia.ca/dbase/Query/Biolist3.php?name=Hawco,%20Darren&id=15930&Page=1&input=hawco.

In a note of cautious optimism, DGC's ability to build a disruptive engine is enhanced by awareness of these gaps, and understanding that drawing on the right technical backgrounds from within the sustaining base of the existent military force is necessary before a different, and disruptively dynamic, cyber force development model can be built and sustained.[52] However, in sum, while professional competency is evident within DGC, the skills required to generate a truly disruptive agency are less so, and therefore subject to concern.

Conclusion

This paper used the Christensen-Raynor *Innovator's Dilemma and Innovator's Solution* models to broadly assess if the CF's current Cyber Force organisational strategy and structure could succeed in this inherently disruptive environment or not. It concludes that the existing CF framework and vision follow a sustaining trajectory along a traditional force development paradigm, with little evidence of deliberate effort to create a disruptively attuned mindset. This outcome does not doom the Cyber Force from ever operating within or adhering to disruptive principles; however, such is likely to emerge from evolutionary strategy and growth (see Figure 3), supported by a deep public purse to impose the necessary resources and structures for success, rather than from disruptive vision itself.

---

[52] The right mix of cyber forces in the future will involve "Regular, Reserve, civilian and perhaps contractor or managed services support . . .. We have classifications and trades today that draw from some of the right technical backgrounds to offer a starting point to develop higher order cyber functions, skills and knowledge. . .. You have to accept that the model for cyber force development is not like air, land or sea where you are going to build a big platform and keep it for 40 years. Your platform is changing on a daily basis. It speaks to a force development team that understands change and is queued to respond to those changes." Brigadier-General Greg Loos, quoted in Chris Thatcher, "Operationalizing the cyber domain," *Vanguard* (June/July 2013): 14, last accessed 17 May 2015, http://vanguardcanada.uberflip.com/i/139409-june-july-2013/5.

Building a disruptively competitive organisation requires deliberate forethought, planning, and appropriate cost structures to motivate the desired behaviours. It demands a different Human Resource approach to attract and retain a team wired to think and assess challenges of the cyber setting in a unique way: this complex, volatile, and *strategic* environment requires operators who are comfortable leading from the basis of functional expertise, not rank, so argument for command and control models akin to those used within existent Special Operations Force models is strong.[53]

As can be seen, leading an organisation to operate and thrive within the disruptive environment of "neurocortical warfare"[54] has less to do with technology than it does with human dynamics and organisational design and structure: recruit the team you need, but place it within a structure that will nurture what is needed from that team. Insofar as the evidence gathered on current CF Cyber Force strategy revealed, this necessary degree of disruptive structuring is not as evident as ID/IS theory demands.

Although it lies beyond the scope of this paper to address, asking if the American cyber model offers insights to what could be applied in Canada certainly merits consideration. In it, US Cyber Command falls under the *military* remit of a single four-star general under US Strategic Command (USSTRATCOM), with a singular chain of command running from the President, to the Secretary of Defense, and USSTRATCOM

---

[53] Szabunio, "Developing a Cyberagenda . . .;" and Leblanc, "Human Resources Issues . . .," 6,13.

[54] "Neocortical warfare is warfare that strives to *control* or *shape* the behavior of enemy organisms, but without destroying the organisms. It does this by *influencing*, even to the point of regulating, the consciousness, perceptions and will of the adversary's leadership: the enemy's neocortical system. In simple ways, neocortical warfare attempts to penetrate adversaries' recurring and simultaneous cycles of [Boyd's] observation, orientation, decision and action." Emphasis in original. Richard Szafranski, "Neocortical Warfare? The Acme of Skill," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla, and David Ronfeldt, 395-416 (Santa Monica: RAND Corporation, 1997), 404, last accessed 18 May 2015, http://www.au.af.mil/au/awc/awcgate/milreview/neocortical.pdf.

into US Cyber Command.[55] Key to its mandate is the broad spectrum liaison and partnership links, not only with traditional JIMP/OGD agencies, but also with private industry: if Cyber Command's writ to defend the United States is to succeed, it must coordinate its actions "across the government, with allies, and with *partners in the commercial sector*."[56]

In the interim, the absence of a clear strategy for the Canadian Cyber Force is *not* a strategy. Much work to develop, generate and grow a disruptively capable fighting force remains to be done.

[55] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (Sep/Oct 2010): 'New Strategy' Section (PDF pg. 4-5/9), last accessed 17 May 2015, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

[56] *Ibid*., (emphasis added).

BIBLIOGRAPHY

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" In *Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND Corporation, 1997.

Bailetti, Tony, Dan Craigen, David Hudson, Renaud Levesque, Stuart McKeen, and D'Arcy Walsh. "Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity." *Technology Innovation Management Review* 3 no. 8 (August 2013): 5-14. http://timreview.ca/article/711.

Boutilier, Alex. "CSIS can't keep up with 'daily' state-sponsored cyber attacks." *Toronto Star*. Last modified 14 May 2015. http://www.thestar.com/news/canada/2015/05/14/csis-cant-keep-up-with-daily-state-sponsored-cyber-attacks.html.

Canada. Department of National Defence. *Chief of Defence Staff Guidance to the Canadian Armed Forces.* Ottawa, ON: Chief of the Defence Staff, 2013. https://www.cfmws.com/en/AboutUs/MFS/NewsandUpdates/Documents/CDS_Guidance_to_the_CAF_EN_REV4.pdf.

Canada. Department of National Defence. "Commander JTFN – Brigadier-General Loos, G.D., OMM, CD." Last modified 21 June 2013. http://www.cfna.forces.ca/info/com-eng.asp.

Canada. Department of National Defence. "Assistant Deputy Minister (Information Management)." Last modified 24 July 2014. http://www.forces.gc.ca/en/about-org-structure/assistant-deputy-minister-information-mgmt.page.

Canada. Department of National Defence. "Leonard (Len) J. Bastien – Biography." Last modified 27 July 2014. http://www.forces.gc.ca/en/about-org-structure/assistant-deputy-minister-information-mgmt-bio.page.

Canada. Department of National Defence. "Vice Chief of the Defence Staff." Last modified 18 November 2014. http://www.forces.gc.ca/en/about-org-structure/vice-chief-defence-staff.page.

Canada. Parliament of Canada. The Standing Senate Committee on National Security and Defence. *Minutes of Proceedings and Evidence*. 05 November 2012. Last accessed 16 May 2015. http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-e.HTM.

Canada. Public Safety Canada. *Action Plan 2010-2015 for Canada's Cyber Security Strategy*. Ottawa: Queen's Printer, 2013. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx.

Canada. Treasury Board of Canada Secretariat. "2014 Public Service Employee Survey Results by Question for Assistant Deputy Minister (Information Management)." Last modified 13 January 2015. http://www.tbs-sct.gc.ca/pses-saff/2014/results-resultats/bq-pq/03/370/org-eng.aspx.

Canada. Treasury Board of Canada Secretariat. "2014 Public Service Employee Survey Results by Question for Director General Information Management Operations - Canadian Forces Information Operations Group (Units & Detachments)." Last modified 13 January 2015. http://www.tbs-sct.gc.ca/pses-saff/2014/results-resultats/bq-pq/03/370/379/org-eng.aspx.

CGI. "CGI at a glance." Last accessed 16 May 2015. http://www.cgi.com/sites/default/files/brochures/cgi_broc02_letter_cgi_at_a_glance.pdf.

Christensen, Clayton M. *The Innovator's Dilemma*. New York: HarperBusiness, 2000.

Christensen, Clayton M., and Michael E. Raynor. *The Innovator's Solution*. Boston: Harvard Business Review Press, 2003.

Christensen, Clayton, and Michael Raynor. "The Innovator's Solution." *Executive Book Summaries* 25, no. 11 (November 2003): 2-8. Last accessed 16 April 2015. http://www.slideshare.net/rajeshsoundararajan/exec-summaries-the-innovators-solution.

Christensen, Clayton. "Clayton Christensen." Last accessed 13 May 2015. http://www.claytonchristensen.com.

De Guzman, Mari-Len. "Defence initiative gives Canadian Forces IT ammunition." *IT World Canada*, 17 October 2007. Last accessed 16 May 2015. http://www.itworldcanada.com/article/defence-initiative-gives-canadian-forces-it-ammunition/268.

Kotter, John P. "Leading Change: Why Transformation Efforts Fail." *Harvard Business Review* 73, no. 2 (March/April 1995): 59-67.

Leblanc, Sylvain. *Human Resources Issues Currently Affecting the Development of the CAF Cyber Force. Technical Report ECE-2013-01, Computer Science Laboratory.* Kingston: Royal Military College of Canada, 2013.

Libicki, Martin C. *Who Runs What in the Global Information Grid: Ways to Share Local and Global Responsibility*. Santa Monica, CA: RAND Corporation, 2000.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009).

Lynn, William J. III. "Defending a New Domain." *Foreign Affairs* 89, no. 5 (Sep/Oct 2010): 97-108. Last accessed 17 May 2015. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

McGuffin, Lieutenant-Colonel W.C. "Soldiers of FORTRAN: Militarization of the 5th Dimension." Joint Command and Staff Programme Master of Defence Studies Research Paper. Toronto: Canadian Forces College, 2013.

Mitchell, Samuel T., II. "Identifying Disruptive Technologies Facing the United States in the Next 20 Years." Master of Military Art and Science Research Paper. Fort Leavenworth, KS: United States Army Command and General Staff College, 2009.

Okros, Alan, John Verdun, and Paul Chouinard. "Complex Adaptive Systems." In *The Meta-Organization*. Toronto, ON: Defence Research and Development Canada, 2011.

Pilieci, Vito. "Cyber security a non-stop headache for federal government, conference hears." *Ottawa Citizen*, 29 October 2014. Last modified 29 October 2014. http://ottawacitizen.com/business/local-business/cyber-security-a-non-stop-headache-for-federal-government-conference-hears.

Porter, Kate. "Cybersecurity non-profit finds home in Ottawa suburb." *CBC News*, 05 November 2013. Last updated 05 November 2013. http://www.cbc.ca/news/canada/ottawa/cybersecurity-non-profit-finds-home-in-ottawa-suburb-1.2415303.

Press, Jordan. "Canada's cyberspace top gun talks military strategy." *Postmedia News*, 06 August 2013. Last modified 06 August 2013. http://o.canada.com/technology/canadas-cyberspace-top-gun-talks-military-strategy.

Press, Jordan. "Canada's military squeezed out of cyber-defence, emails warn." *Postmedia News.* 12 March 2014. Last modified 12 March 2014. http://o.canada.com/news/national/canadas-military-squeezed-out-of-cyber-defence-emails-warn.

Pudas, Terry, J. "Disruptive challenges and accelerating Force transformation." *Joint Force Quarterly* 42 (3rd Quarter 2006): 43-50.

Raynor, Michael. "Growth and Innovation in Established Firms." Business 600 Course Lecture, Richard Ivey School of Business – University of Western Ontario, London, ON, January-February 2003.

Rid, Thomas. “Cyberwar Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (Feb 2012): 5-32.

Simons, Robert. *Performance Measurement & Control Systems for Implementing Strategy*. Upper Saddle River: Prentice Hall, 2000.

Szabunio, Lieutenant-Colonel Paul A. “Developing a Cyberagenda – Vision for Command and Control of Cyber Operations.” Joint Command and Staff Programme (Distance Learning) CF549DL – Advanced Topics in Campaign Design Forum Discussion, Canadian Forces College, April 2015.

Szabunio, Lieutenant-Colonel Paul A. “Military Responses to Malicious Cyber Activities.” Joint Command and Staff Programme (Distance Learning) CF549DL – Advanced Topics in Campaign Design Forum Discussion, Canadian Forces College, April 2015.

Szafranski, Richard. “Neocortical Warfare? The Acme of Skill.” In *In Athena's Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla, and David Ronfeldt, 395-416. Santa Monica: RAND Corporation, 1997. Last accessed 18 May 2015. http://www.au.af.mil/au/awc/awcgate/milreview/neocortical.pdf.

Thatcher, Chris. “Operationalizing the cyber domain.” *Vanguard* (June/July 2013): 12-14. Last accessed 17 May 2015. http://vanguardcanada.uberflip.com/i/139409-june-july-2013/5.

The Nauticapedia. “Biographical Data – Hawco Darren.” Last updated 26 May 2014, http://www.nauticapedia.ca/dbase/Query/Biolist3.php?name=Hawco,%20Darren&id=15930&Page=1&input=hawco.

Venus Cybersecurity Corporation. “Venus Cybersecurity Corporation is a new kind of company.” Last modified 11 March 2014. http://www.venuscyber.com/sites/all/documents/VENUS%20Membership%20and%20Structure.pdf.

Walkling, Lieutenant-Colonel Jason. “Considerations: Canadian Forces’ Efforts in the Electromagnetic Spectrum and Cyber Operating Environment.” Master of Defence Studies Research Paper. Toronto: Canadian Forces College, 2013.