National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER CAPABILITY DEVELOPMENT: CONSIDERATIONS FOR OPTIMIZING ORGANIZATIONAL FORM IN THE DND/CAF

LCdr R.A.D. Chouinard-Prévost

JCSP 43

Exercise *Solo Flight*

Disclaimer

PCEMI 43

Exercice *Solo Flight*

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 – PCEMI 43
2016 – 2017

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBER CAPABILITY DEVELOPMENT: CONSIDERATIONS FOR OPTIMIZING ORGANIZATIONAL FORM IN THE DND/CAF

LCdr R.A.D. Chouinard-Prévost

Word Count: 5494

Compte de mots: 5494

CYBER CAPABILITY DEVELOPMENT: CONSIDERATIONS FOR OPTIMIZING ORGANIZATIONAL FORM IN THE DND/CAF

INTRODUCTION

In the digital age, the 'fire-proof house' may no longer be. That is what Victor Platt contended when he stated the globalized cyberspace arena was eroding the conventional wisdom associated with Canada's advantageous geographic situation.[1] This undeniable vulnerability has gained increased scrutiny in the last decade, and has resulted in Canada's 2010 Cyber Security Strategy.[2] Its first pillar—secure the Government's cyber systems[3]—has endured to this day and was restated by Minister of National Defence Harjit Sajjan in his speech to the Security Innovation Network's Information Technology Security Entrepreneurs Forum on 20 April 2016.[4] These systems include those employed by the Department of National Defence and the Canadian Armed Forces (DND/CAF). The responsibility to develop the capability to secure and protect them was relatively recently assigned to the Directorate of Cyber Force Development (D Cyber FD), which reports to the Director General Cyber (DG Cyber).

In late 2013, a study commissioned by D Cyber FD sought to determine the appropriate occupational options available to fulfill the roles related to cyber operations,[5] now a distinct warfighting domain.[6] In March 2016, as a result of this study, the Chief of

---

[1] Victor Platt, "Still the Fire-Proof House? An Analysis of Canada's Cyber Security Strategy," *International Journal* 67, no. 1 (March 2012): 155.

[2] Department of Public Safety, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Department of Public Safety, 2010).

[3] *Ibid*., 7.

[4] Harjit Sajjan, Keynote Address, Security Innovation Network's Information Technology Security Entrepreneurs Forum, Silicon Valley, California, United States, 20 April 2016.

[5] D.C. Hawco, *Job Study – Problem Definition Paper Cyber Specialist and Cyber Staff (Officer and NCM)* (Director General Cyber: file 5000-1 (D Cyber FD), 23 October 2013), 5.

[6] M.A.G. Norman, *VCDS Initiating Directive - Transfer of Leadership Responsibilities for VCDS Related Capability Development Responsibilities to ADM(IM), the Canadian Army and CFINTCOM* (Vice Chief of Defence Staff: file 1920-1 (CFD), 12 December 2016), 2.

Defence Staff (CDS) endorsed the creation of a cyber operator occupation, which was the result of the first spiral of DND/CAF's cyber military employment study.[7] The second spiral is intended to consider service-specific cyber requirements.[8] To help support part of the work of the second spiral, a request for research questions was made by the author: D Cyber FD presented two. While both are fundamentally different questions, they are together representative of the larger problem and their answers are interdependent—at least in part. Therefore, they are both presented here for consideration:

- Should the CAF develop the military cyber operator occupation to support both 'national' network and 'service-specific' network defence capabilities?[9]
- Should each of the services have its own cyber operators or should this kind of specialist work be performed by a joint organization on their behalf?[10]

Because of space restriction, the first research question will not be answered and will therefore be the subject of this paper's critical assumption, that from a technical perspective, cyber defenders are required to secure and protect service-specific networks, and most importantly, the industrial control systems, command and control systems, and weapon systems employed by each of the services. Given some of the researched evidence,[11] it should be considered a reasonable assumption.

---

[7] J.H. Vance, *Record of Discussion – Armed Forces Council (AFC) #160322* (Chief of Defence Staff: file 1150-4 (D NGHQ Sec), 22 March 2016), 4.

[8] Email received by author on 24 March 2017.

[9] Email received by author on 10 January 2017. This question was paraphrased.

[10] Email received by author on 10 January 2017.

[11] J. Johnson, "What Can RCAF Do Against Cyber Threats?" (Joint Command and Staff Programme, Canadian Forces College, 2017), 2; J.M. Lanouette, "Naval Cyber Warfare: Are Cyber Operators Needed on Warships to Defend Against Platform Cyber Attacks?" (Joint Command and Staff Programme, Canadian Forces College, 2016), 7; Ministry of Defence, *Strategic Trends Programme: Global Strategic Trends - Out to 2045* (London: Ministry of Defence, 2014), 168; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 85; Zoe Hawkins and Liam Nevill, *Digital Land Power: The Australian Army's Cyber Future* (Barton, Australia: The Australian Strategic Policy Institute Limited, December 2016) 5; Richard Bensing, "An Assessment of Vulnerabilities for Ship-Based Control Systems" (master's thesis, Naval Postgraduate School, 2009), 32; Lee Young-Ju, "Establishment of a

The second research question, to be considered this paper's research question, will be answered, *however neither fully nor directly*—this will be explained in the following section. Implied in the previous statements is the shear complexity of the problem to address. Indeed, beyond the interplay of the technical, economical, and geographical attributes of the problem, there are complex organizational, cultural and social dynamics to consider, especially within such a large organization as the DND/CAF. Because a holistic analysis of the questions cannot be accomplished in this short essay, this paper will focus very narrowly on organizational dynamics, and more specifically on considerations related to organizational structure.

Specifically, it will be demonstrated that the conflation of governance, unique DND/CAF attributes, resilience, as well as standardization and information symmetry favours a unitary (U-Form) organizational structure as the preferred *initial* organizational model for the DND/CAF cyber capability, which in turn favours the implementation of a joint organization responsible for generating the cyber operators who will perform work on behalf of the services.[12]

To prove this thesis, five sections will be used. The first section will focus on improving our understanding of the problem as well as presenting a reference framework centered on the organizational model for multidivisional (M-Form) and U-Form structures. The second section will build upon the first by using the reference framework, theory and other evidence to analyze governance as well as standardization and

---

Feasible Cyber Organization Structure to Enhance the Capabilities of Cyberspace Operations in the ROK's Defense Forces," *The Korean Journal of Defense Analysis* 28, no. 2 (June 2016): 227; William D. Bryant, "Mission Assurance through Integrated Cyber Defense." *Air and Space Power Journal* 30, no. 4 (Winter 2016): 6.

[12] For the purpose of this paper, services include the Canadian Special Forces Command, the Royal Canadian Navy, the Canadian Army, and the Royal Canadian Air Force.

information symmetry in the context of cyber capability, the overall aim of which will be to provide a part-assessment of the preferable organizational structure. With a substantially reduced theoretical focus, the third and fourth sections will aim to achieve the same as the second section by considering unique DND/CAF attributes and resilience, respectively. The last section, titled final analysis and conclusion, will aim to provide a final assessment on the optimal organizational form, detail a number of limitations applicable to the analysis, and recommend future work.

PROBLEM DEFINITION AND REFERENCE FRAMEWORK

This paper's research question—*should each of the services have its own cyber operators or should this kind of specialist work be performed by a joint organization on their behalf?*—suffers from two fundamental flaws. First, it presupposes a clear and unambiguous understanding of the vision for and the extent of the DND/CAF cyber capability. If such an understanding was prevalent, the first research question in the introduction—the one which led to the paper's critical assumption—would most probably be answered, at least partially. The second flaw is it may mislead to a premature analysis of possible occupational solutions, such as creating a new military occupation, expanding the role of an existing one, adding a sub-occupation to the newly created cyber operator trade, or creating a speciality within some existing occupation. While part of the answer should certainly include occupational considerations, the cyber capability's organizational dynamics, as macro-level considerations, must be understood to better inform an eventual occupational analysis—especially with an organization as large as the DND/CAF—and therefore should be addressed first in the process of answering the

research question. As Columbia University political science Professor Alexander Cooley stated, "variation in the organization of firms accounts for important differences in firm behavior as well as the behavior of individual actors within them."[13] Because of these important differences and because "economic firms and political hierarchies [will,] . . . when organized, administered, or delegated according to similar logics, . . . face common problems and challenges,"[14] this essay's problem space will focus on the organizational dynamics of organizational forms as they relate to the DND/CAF cyber capability.

Specifically, the organizational dynamics will be explored in the context of the following question: what organizational form would best position the DND/CAF to deliver the required cyber effects? The forms to be explored will be the multidivisional structure, or M-Form, and the unitary structure, or U-Form. As they relate to the research question, an M-Form structure would likely favour service-specific cyber operators while a U-Form structure would likely favour a joint organization performing the cyber operator work on behalf of the services. Unfortunately, the new question also presupposes a clear understanding of the intended DND/CAF cyber capability. To resolve this flaw, we will substitute the critical assumption for the clear understanding—stated more comprehensively in the introduction, the critical assumption was that, from a technical perspective, cyber defenders are required to secure and protect service-specific networks and systems.

Limiting this study to the use of the above model does not imply that other organizational approaches are not suitable. In fact, analyzing the DND/CAF organizational and social dynamics with other models would ultimately help answer the

---

[13] Alexander Cooley, *Logics of Hierarchy: The Organization of Empires, States, and Military Occupations* (Ithaca, New York: Cornell University, 2005), 3.
[14] *Ibid.*, 7.

research question more holistically— for example, such models could be based on relative power distribution, identity-based processes, rationalism, or constructivism. However, for reasons of space restriction, this study will limit its focus to the M-Form and U-Form approach.

It is worthy to outline why the third organizational structure, the holding structure, was discarded. The holding structure, also known as H-Form, is defined as "collections of many different unrelated U-form organizations," as opposed to the M-form's "many different related U-form organizations."[15] In other words, the H-Form organization has its divisions in completely unrelated business.[16] Because of the joint character of many CAF operations, there are significant synergies between the force generators in generating joint capabilities, and between the component commanders within the force employers in delivering operational effect. For that reason, the H-Form is unlikely to be applicable to the DND/CAF.

In Figure 1 and 2 below, the Conceptual M-Form Cyber Structure and the Conceptual U-Form Cyber Structure are illustrated. There are three important aspects which need qualification. First, these are conceptual organizational charts: they are not meant to accurately reflect reality. For instance, they do not account for the Vice Chief of Defence Staff (VCDS) directive related to the role of the Chief of Staff Information Management as the Cyber Force Commander.[17] The intent is to illustrate the differences between what could be one version of a conceptual M-Form organization centered on the DND/CAF cyber capability and one version of the same capability as a conceptual U-

---

[15] Matthew J. Holian, "Understanding the M-Form Hypothesis," *Journal of Industrial Organization Education* 5, no. 1, Article 4 (2010): 2.

[16] William G. Ouchi, "The M-Form Society: Lessons from Business Management," *Human Resource Management (pre-1986)* 23, no. 2 (Summer 1984): 194.

[17] Norman, *VCDS Initiating Directive . . .*, B-1/9.

Form organization. Second, note that there are additional force generators within DND/CAF, however, the arguments of this paper are centered on the services, hence the limited view on the Canadian Special Operations Command (CANSOFCOM), the Royal Canadian Navy (RCN), the Canadian Army (CA), and the Royal Canadian Air Force (RCAF). Third, the presented conceptual structures are predicated on the responsibility for cyber force generation,[18] or the responsibility to generate the latent cyber operational effect. For example, in Figure 1, the RCN is responsible to generate the naval cyber capability, and the CA is responsible to generate the army cyber capability. In Figure 2, the responsibility to generate joint and service-specific cyber capability rests with the Cyber Force Commander.[19] Therefore, these conceptual structures specifically do not address the DND/CAF force employment[20] model accomplished by the Canadian Joint Operations Command, the North American Aerospace Defense Command, and CANSOFCOM—note that CANSOFCOM also has a Force Generation mandate, hence its inclusion in the conceptual structures.

---

[18] In accordance with B-GJ-005-000/FP-001 *Canadian Forces Joint Publication 01 - Canadian Military Doctrine*, force generation is the process of organizing, training, and equipping forces for employment. Force generation integrates four major components: force structure, equipment, readiness, and sustainability.

[19] In accordance with the 1920-1(CFD) *VCDS Initiating Directive for the Transfer of Leadership Responsibilities for VCDS related Capability Development Responsibilities to ADM(IM), the Canadian Army and CFINTCOM*, the VCDS directed that force generation will be the responsibility of the Cyber Force Commander.

[20] In accordance with B-GJ-005-000/FP-001 *Canadian Forces Joint Publication 01 - Canadian Military Doctrine*, force employment is defined, at the strategic level, as the application of allocated military means to achieve specified objectives or effects through activities such as operations, defence diplomacy, and unilateral, bilateral, or multilateral defence activities.

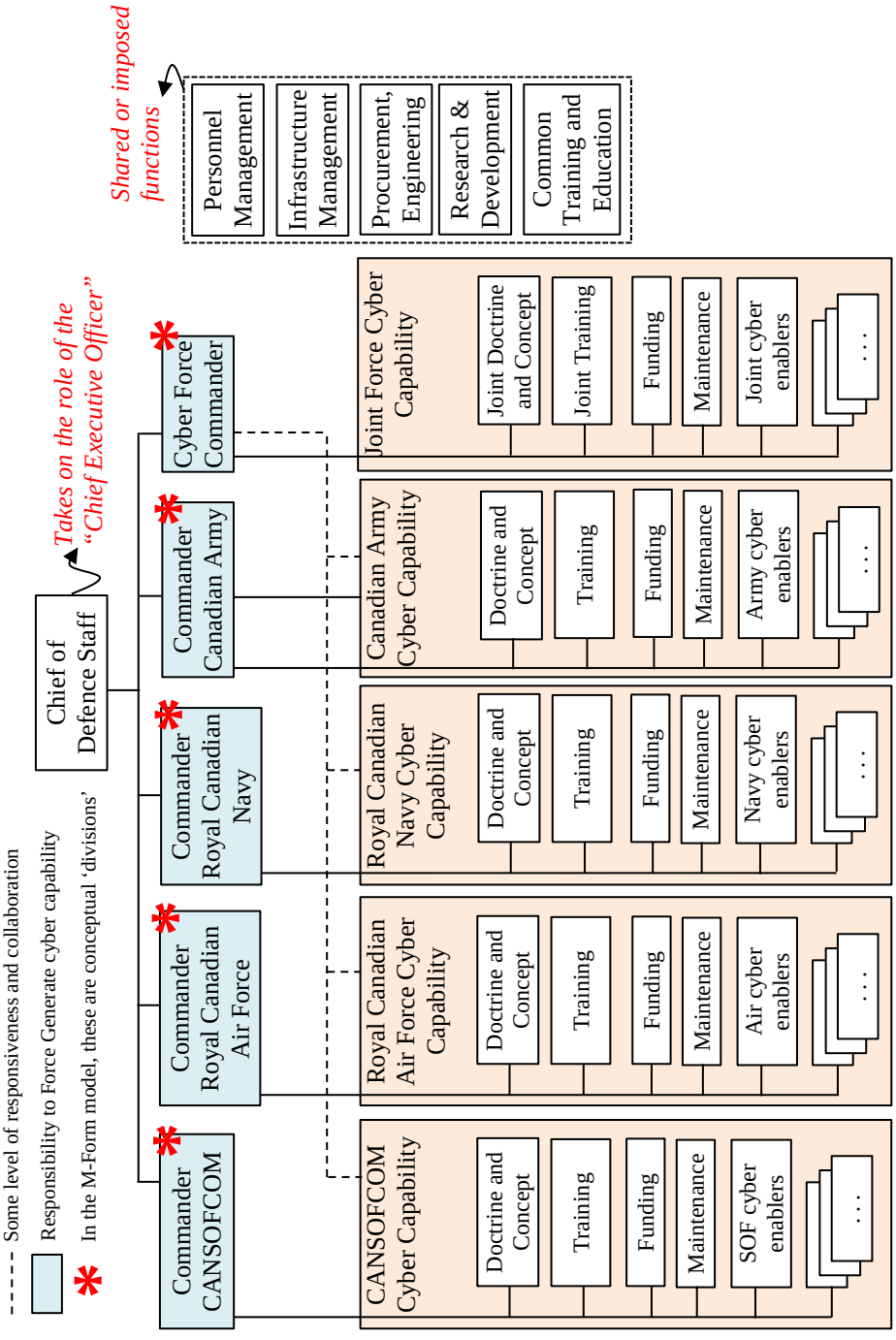

Figure 1 – Conceptual M-Form Cyber Structure

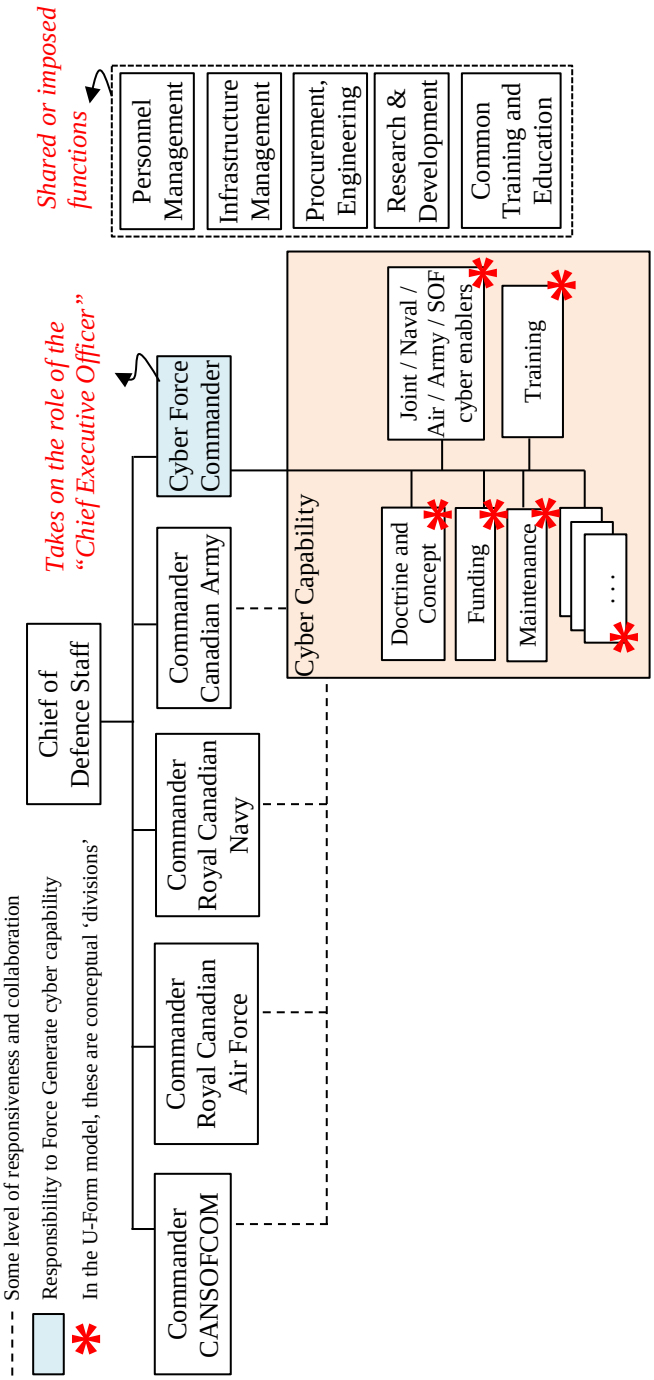

Figure 2 – Conceptual U-Form Cyber Structure

Mainly to add realism to the analysis, the above illustrated structures have been adapted from the purest representations of the U-Form and M-Form structures. While it would be interesting to isolate the problem from currently existing structures, it would

blind the reader from some of the factors relevant to the organizational dynamics in the DND/CAF and would be detrimental to the more practical goal this paper aims to achieve. The incongruences are explained below.

In the Conceptual M-Form Cyber Structure, there are two elements of incongruence with the purest representation of the M-Form structure.[21] The first incongruence is a result of making the assumption that the Conceptual M-Form Cyber Structure suffers from one of the two types of conflation identified by Oliver Williamson—the well-known economist who praised the M-Form structure for favouring "goal pursuit and least-cost behavior more. . . than the . . . U-Form organizational alternative"[22]—as making the organization suboptimal. This conflation was characterized by sociologist Robert Freeland as 'participative decentralization' and defined as the state of the divisions within the multidivisional structure becoming "involved in long-term planning and performance evaluation through gaining representation on the committee or committees responsible for overseeing governance."[23] Arguing the merit and validity of this incongruence as a generalization of the organizational dynamics of the DND/CAF would be a very interesting topic, however, for the purpose of this paper, it will have to remain an assumption—an assumption which is deemed valid to the extent that the DND/CAF can be considered a large bureaucracy where inputs in the long term strategy is generally sought from across the organization. Notwithstanding the incongruence, Freeland presents a convincing argument that 'participative decentralization' is a desirable attribute "in a highly diversified firm

---

[21] A good example of the M-Form can be seen in: Cooley, *Logics of Hierarchy* . . ., 6.

[22] Oliver E. Williamson, *Markets and Hierarchies* (New York: Free Press, 1975), 150, quoted in Ouchi, "The M-Form Society . . ., 193.

[23] Robert F. Freeland, "The Myth of the M-Form? Governance, Consent, and Organizational Change," *American Journal of Sociology* 102, no. 2 (September 1996): 484.

operating in a number of distinct markets"[24] for reasons of identification, evaluation and implementation of long-range strategies.[25] For this reason, as it applies to the Conceptual M-Form Cyber Structure, this first incongruence is considered an acceptable deviation to the pure M-Form organization. The second incongruence from the pure M-Form organization is a result of the functions which are either shared across or imposed upon the rest of the organization within the Conceptual M-Form Cyber Structure. These are illustrative of the organizational relationships with the DND/CAF. Examples include research and development, infrastructure management, and procurement. These functions go beyond the roles intended for the 'central office' of the pure M-Form organization, which are supposed to be limited to strategic planning, performance measurement, and capability investment.[26] Notwithstanding, these shared or imposed functions could in fact—at least in part—be the organizational manifestation of the synergies needed between the divisions of the multidivisional organization.[27] For this reason and the fact those entities are more representative of the DND/CAF reality, the second incongruence is considered an acceptable deviation to the pure M-Form organization.

In the above illustrated Conceptual U-Form Cyber Structure, there is one element of incongruence with the purest representation of the U-Form structure:[28] the shared or imposed functions should in fact be fully allocated to the Cyber Force Commander. However, as previously stated, for reasons of realism the presented conceptual U-Form structure and its incongruence to the pure representation will need to be retained.

---

[24] *Ibid*., 517.
[25] *Ibid*., 518.
[26] *Ibid*., 484; Cooley, *Logics of Hierarchy* . . ., 22.
[27] Holian, "Understanding the M-Form Hypothesis . . ., 3; Ouchi, "The M-Form Society . . ., 196-197.
[28] A good example of the U-Form can be seen in: Ouchi, "The M-Form Society . . ., 193.

GOVERNANCE, STANDARDIZATION AND INFORMATION SYMMETRY

This section will explore two central organizational ideas, and their applicability within the context of cyber in the DND/CAF. These central ideas are governance, and standardization and information symmetry.

Governance "refers . . . to the creation of a setting in which others can manage effectively."[29] The organizational form is all important to the type of governance which will prevail across the organization.[30] Governance in the DND/CAF manifests itself, amongst others, through mechanisms of decision-making, processes of prioritization, assignments of authorities, responsibilities, and accountabilities, processes of risk management, and standardizations of certain functions and methods.

One of the more obvious manifestations of governance in an organization is accountability and its allocation amongst its divisions. For a service-specific construct, it was recognized that failing to clearly demarcate accountabilities will result in frictions between the services and other agencies.[31] Two potential causes for these frictions are the M-Form's principal-agency problem characterized by Cooley[32] and the lack of awareness of synergies[33]—in the case of the synergies, it is perhaps also the agreement on what synergies should be leveraged. The Conceptual M-Form Cyber Structure therefore presents an inherent risk of inefficacy should a poorly defined set of authorities, responsibilities, and accountabilities be implemented, and therefore allow for M-Type opportunism[34] to surface in the form of own-agenda pursuit. However, and somewhat

---

[29] Ouchi, "The M-Form Society . . ., 197.
[30] *Ibid.*, 197-202.
[31] Hawkins and Nevill, *Digital Land Power* . . ., 59.
[32] Cooley, *Logics of Hierarchy* . . ., 14.
[33] Holian, "Understanding the M-Form Hypothesis . . ., 6.
[34] Cooley, *Logics of Hierarchy* . . ., 14.

counterintuitively, the M-Form structure generally incurs less governance costs, which stem from the decentralization of decision-making.[35] Although a risk exists that principal-agency problems and poorly crafted accountabilities create frictions within the Conceptual M-Form Cyber Structure, it seems counterbalanced by the risk related to centralization of decision-making in the Cyber Force Commander within the Conceptual U-Form Cyber Structure, which increases the overall governance burden. Furthermore, it is important to consider that while effective prioritization of cyber requirements between each of the services and the Cyber Force Commander could suffer due to the principal-agency problem, the previously mentioned 'participative decentralization' incongruence which characterizes DND/CAF would improve the alignment between the divisions.

Another perspective relates to the types of governance and their affinities with each of the organizational forms. In his arguments surrounding the various types of governance, William Ouchi contended that no type of governance was sufficient on its own and that the M-Form was the preferred organizational structure as it had all three types[36]—that is market, bureaucracy, and clan, with clan governance being the way to achieve long term equity between the divisions, and the other two being based on competition and rules, respectively.[37] As Ouchi stated:

> No one mode of governance can ever be complete. Because perfect competition never exists, markets can never govern completely. Because rules are inflexible and human beings fallible, bureaucracy can never govern completely. Because people are self-interested and individual tastes divergent, clans can never govern completely.[38]

---

[35] *Ibid*.
[36] Ouchi, "The M-Form Society . . ., 200-201.
[37] *Ibid.*, 198-199.
[38] *Ibid.*, 202.

Based on Ouchi's observations, a Conceptual M-Form Cyber Structure would encourage the services to implement a cyber capability which is best adapted to the operational environment within which they each conduct their mission, would prescribe a vision and overall mission for all to achieve, and would allow for cyber capabilities within some services to take priority over others with the understanding that priority will eventually shift back to those who made the temporary sacrifice. In contradistinction, the Conceptual U-Form Cyber Structure would have more difficulty adapting the cyber capabilities to the service-specific operational environments, would be more inflexible to outside pressure due to a greater reliance on one-size fits all approaches,[39] and various entities under the Cyber Force Commander would attempt to gain increasingly greater influence at the expense of others—potentially impacting cyber capabilities intended for specific services.

While it can be argued that the nascence of the cyber capability within DND/CAF could result in increased potential for principal-agency problems as well as authority, responsibility and accountability definition problems, the above observations seem to favour the Conceptual M-Form Cyber Structure over the Conceptual U-Form Cyber Structure. However, another critical area of consideration in determining the best-fit organizational structure is its affinity to standardization and information symmetry. Given the military context, standardization is to be construed to encompass doctrines, tactics, techniques and procedures. Information symmetry is concerned with information flow, which is impacted by the "organizational architecture of the various divisions."[40] Plainly stated, at the core level in a U-Form structure, there is strong coordination and

[39] Holian, "Understanding the M-Form Hypothesis . . ., 6.
[40] Cooley, *Logics of Hierarchy* . . ., 46.

flow of information between each of the divisions. In an M-Form structure, there is weak coordination and flow of information between each of the divisions.[41]

An interesting point of departure for standardization and information symmetry is the work of Pierre Barbadoux. In referring the works of Herbert Simon and Adam Smith, Barbadoux explained the principle of decomposition as the "tightness of coupling between components," and "the degree to which the organization architecture enable (or prohibit) the mixing and matching of components."[42] One of the aspects of the principle of decomposition he described was the requirement for specifying interfaces and information patterns between the other organizational components.[43] While his article focussed on organizational change and the organization's ability to cope, his concepts of standardization of functional structure and formalization of information flow as key components to organizational design[44] bring to the forefront the importance of standardization and information symmetry. Indeed, Cooley addresses both topics in favour of the U-Form. Specifically, the U-Form exhibits "comparatively . . . [lesser] informational asymmetries between the periphery and core" than the M-Form counterpart, and "is more likely . . . to successfully promote institutional transformation and change in the periphery."[45]

While the above standardization and information symmetry considerations seem to tip the balance in favour of the Conceptual U-Form Cyber Structure, the importance of subscribing to service-specific doctrines cannot be discarded. Indeed, documents such as

---

[41] *Ibid*., 46-47.

[42] Pierre Barbadoux, "A Design-Oriented Approach to Organizational Change: Insights from a Military Case Study," *Journal of Organizational Change Management* 24, no. 5 (2011): 628.

[43] *Ibid.*

[44] *Ibid*., 636.

[45] Cooley, *Logics of Hierarchy* . . ., 14.

the United States (US) Air Force Information Dominance strategy,[46] contentions that cyberspace needs to have service-specific cultural or doctrinal approaches,[47] and the fact that doctrine takes a "substantial time to mature,"[48] calls into question the efficacy of a U-Form model for the cyber capability within DND/CAF. At issue is the relative significance of service-specific doctrine, experience and knowledge over what would be available from a centralized model. Also at issue is the ability for services to implement a cyber capability which is best adapted to the operational environment within which missions are conducted.

These concerns were also raised relatively recently within DND/CAF. In January 2016 at a meeting chaired by DG Cyber, the Commanding Officer of the Canadian Forces Network Operations Centre (CFNOC) outlined "concerns regarding unique platforms within the environments," that "defence . . . [may] not be best accomplished via a centrally localized model," and finally that all backgrounds are important to defend against cyber threats.[49] At the same meeting, the Canadian Army representative stated the need for the cyber operator to understand the Canadian Army doctrines and standard operating procedures.[50]

Yet another interesting counterpoint has recently been presented by Frank Cilluffo and Joseph Clark, respectively Associate Vice President and policy analyst at George Washington University. While they did not contend to have the service-specific cyber

---

[46] United States Air Force, *Information Dominance Vision* (Washington, D.C.: United States Air Force, 2016).

[47] Hawkins and Nevill, *Digital Land Power* . . ., 8; Young-Ju, "Establishment of a Feasible Cyber Organization Structure . . ., 237.

[48] Hawkins and Nevill, *Digital Land Power* . . ., 8.

[49] F. Allen, *Record of Discussion – Cyber Operator Sponsor Advisory Group (SAG) 3 Meeting Held at NDHQ Ottawa on 20 January 2016* (Director General Cyber and Director Personnel Generation Requirements: file 5555-CYBER-1 (DPGR 2-7), 29 February 2016), 3.

[50] *Ibid*.

commands dissolved—the US has cyber commands within each of its four military services, as well as a cyber command in the US Coast Guard and a US Cyber Command joined with the National Security Agency (NSA)—they did argue for greater power and influence for the US Cyber Command by having it removed from the US Strategic Command and placed one level up on par with the Special Operations Command.[51] This move, they argued, would help "mature the cyber components themselves as well as the tactics, techniques, and procedures for their use," and "deconflict efforts across the whole of the US government."[52] Such a command would be "charged with finding out how US forces could employ cyber to better execute the principles of war."[53] The principal arguments for the move are centered on the sub-optimal level of integration of cyber capabilities[54] and the need for the maturation of the capabilities for all components. These arguments are pro-centralization arguments and therefore favor the Conceptual U-Form Cyber Structure. As these arguments were intended for the most powerful and diversified military in the world, they bring an interesting perspective to the assertion that the M-Form structure is the preferred organizational model for large diversified organizations.

The DND/CAF has only recently structured itself with an organization responsible to oversee the development of cyber capability. In accordance with the lead for the development of joint cyber doctrine, as of April 2017, an approved DND/CAF joint doctrine had not been published, although a draft had been socialized with multiple

[51] Frank J. Cilluffo and Joseph R. Clark, "Repurposing Cyber Command," *Parameters* 43, no. 4 (Winter 2014): 111-113.
[52] *Ibid.*, 113.
[53] *Ibid.*, 114.
[54] *Ibid.*, 117.

other organizations.[55] Noting there are no service-specific cyber doctrines, tactics, techniques or procedures within the CAF—the CFNOC, whose operators receive cyber specialist training inclusive of some of those elements, serves as a joint organization—there is therefore no widely available standardization within DND/CAF for the conduct of cyber operations. In the not so distant future, the standardization will therefore be a major focus as the cyber capability within DND/CAF gains momentum. Concurrently to the all-important maturation of doctrines, tactics, techniques and procedures, the information related to cyber capability must be disseminated, and more importantly, understood and acted on as intended. The realm of capability development within the context of a warfare domain which knows no geographical boundaries, no mature legal framework, and a multitude of national and international stakeholders, is extremely complex. Given the complexity and the nascence of the capability, the requirement for information symmetry is therefore significantly magnified. Consequently, despite the need to subscribe to service-specific doctrines and the related advantages of the M-Form structure, the requirement for standardization and information symmetry at this early stage of the capability development process favours the Conceptual U-Form Cyber Structure—at least until initial standardization has occurred and the importance of information symmetry has decreased.

The final section will address the dichotomy between the analysis results of governance, and standardization and information symmetry.

[55] Nathalie Desarzens, discussion with author, 28 April 2017.

UNIQUE ATTRIBUTES

While the previous sections have provided a quasi-theoretical approach to helping determine the optimal DND/CAF cyber capability organizational structure, there are practical elements within the cyber domain and DND/CAF which have organizational design implications.

The first element is remoteness. Aside from the great distances in between Canada's military installations as well as between Canada and its areas of operations, the military operating environment obligates deployed units to be capable of operating in isolation. Within cyberspace, the notion of isolation or remoteness can occur in various ways such as when there is limited or non-existent bandwidth, when communication control measures are in place, or when access to enterprise command and control systems are severed.[56]

The second element is technical acumen. Cyber warriors require very high levels of technical knowledge and skills to operate effectively in cyberspace.[57] Indeed, "experience within the Five-Eyes . . . community indicates that it takes approximately six months to train an entry-level Cyber Specialist and a further two to three years in which to become effective before sub-specializing further in this environment."[58] Complicating the matter is the high susceptibility "to skill fade owing to the complexity and volatility

[56] Lanouette, "Naval Cyber Warfare . . ., 32.
[57] Chief of Force Development, *The Future Security Environment 2013-2040* (Ottawa: Department of National Defence, 2014), 73.
[58] Hawco, *Job Study – Problem Definition Paper* . . ., 2.

of the environment,"[59] volatility which often manifests itself in the rate of change in cyber technologies, thereby driving the need to constantly train.[60]

The third element is collective training. While the cyber warrior requires constant training, the deployed units operating in cyber-contested environments must train to deliver their intended operational effects in degraded environments. For example, the RCN's warships do this in part through a rigorous and regular training regimen guided by its operational training programs in the Sea Training Guide (Edition Bravo) and CFCD 102 Combat Readiness Requirements.

The last element is convergence. The DND/CAF has envisioned achieving "integration of weapons, sensors, data and information into collaborative services on a unified and secure network infrastructure."[61] This vision, together with the intent of converging networks to a singular configuration,[62] imply that compromised software, hardware or firmware within the future networked infrastructure—which will include some weapon systems and sensors—have the potential for strategic repercussions.

These four elements taken together serve as a forcing function to assess impact on the optimal organizational structure. Remoteness of operations enforces independence of action, but most importantly enforces accountability and responsibility for the effectiveness of these independent actions. The requirement for specialized and hard-to-maintain technical skills to support the operational effects within the battlespace as part of a wider combat team—who in turn must be collectively train to be resilient when

---

[59] *Ibid.*, 4.

[60] Defence Research & Development Canada – Centre for Operational Research and Analysis. *CF Cyber Operations in the Future Cyber Environment Concept* (Ottawa: Department of National Defence, 2009), 22.

[61] J.H. Vance, *CDS Directive – CAF Integrated Command and Control Information System* (Chief of Defence Staff: 3 December 2015), 5.

[62] Vice Chief of Defence Staff, *The CAF C4ISR Strategic Vision, Goals and Objectives* (Ottawa: Department of National Defence, 2016), 25.

challenged with degraded cyber capabilities—increases the need to generate the cyber warrior as an integral part of the unit and the service. While the notion of self-organizing team[63] as described by Canadian Forces College Professor Alan Okros may seem attractive for the cyber warrior team, it does not seem to lend itself well to the nature of the environment. Indeed, unlike a Helicopter Air Detachment, a Military Police Platoon or a Brigade Group, the cyber warrior's craft is deeply connected to the systems he or she protects. Together with the notion of convergence which will increase the interconnectedness of DND/CAF networks and thereby increase the risk exposure associated with deployed industrial control systems, weapon systems and sensors, the cyber warrior protecting these deployed and highly unique service-specific assets are likely to benefit from a service-centric approach that grooms cyber capabilities in the context of naval, air and land effects.

Consequently, the unique attributes of remoteness, technical acumen, collective training, and convergence require a degree of independence at the service level as well as a decentralized decision-making structure, both characteristics of the M-Form structure,[64] thereby favouring the Conceptual M-Form Cyber Structure.

[63] Alan Okros, "Becoming an Employer of Choice: Human Resources Challenges within DND and the CF," In *Public Management of Defence in Canada*, ed. Craig Stone (Toronto: Breakout Education Network, 2009), 157.

[64] Cooley, *Logics of Hierarchy . . .*, 22.

RESILIENCE

An important concept that has gained increased interest in recent times is resilience, the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."[65] This concept is all-important in the cyber warfare domain. Indeed, as was cleverly stated by Alexander Moens, Seychelle Cushing, and Alan W. Dowd, author of the Fraser Institute's *Cybersecurity Challenges for Canada and the United States*, "if deterrence is what kept the peace during the Cold War and the Nuclear Age, resilience may be the governing principle of the Digital Age."[66] The ability to recover and function under unfavourable conditions is of the utmost importance.[67]

The DND/CAF recognized the criticality of cyber capability resilience in its assessment of the future security environment[68] and has even prescribed resilience as a core capability requirement for its Command, Control and Information System (C2IS).[69] With deployed service-specific networks and systems, there are additional end-points, gateways, industrial control systems, and weapon systems to secure and protect. The National Institute of Standards and Technology's *Guide to Industrial Control Systems Security* is consistent with the message of resiliency by stating as one of its security objectives the continued maintenance of "functionality during adverse conditions."[70] As was previously stated in the unique attributes section, if the responsibility to generate the

---

[65] Bryant, "Mission Assurance . . ., 10; North Atlantic Treaty Organization, *Cybersecurity: A Generic Reference Curriculum* (Norfolk, Virginia: North Atlantic Treaty Organization, 2016), 64; Department of Homeland Security, *DHS Risk Lexicon* (Washington, DC: Department of Homeland Security, Risk Steering Committee, September 2010), 26.

[66] Moens, Cushing, and Wood, *Cybersecurity Challenges . . .*, 8.

[67] *Ibid.*, 9; William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (September 2015).

[68] Chief of Force Development, *The Future Security Environment . . .*, 132.

[69] Vance, *CDS Directive . . .*, 7.

[70] National Institute of Standards and Technology, *Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security* (Washington, D.C.: US Department of Commerce, 2015), 2

cyber capability resides out of the service, there is a danger that the organization may unwittingly accept risks to its resilience by reducing its ability to respond when compromised.

Notwithstanding, the increased focus on automation of cyber defence systems[71] casts doubts on the notion of resilience when forces are deployed. Automation is however predicated on the efficacy of firewalls and end-point protection systems, as well as signature and anomaly-based intrusion detection systems. Because these systems are designed and updated based on what can be expected or what is already known,[72] automation does not replace the notion of resilience fundamental to successful operations in cyber-contested environments abroad.

As Minister Sajjan stated, "we cannot protect what we cannot predict."[73] When automated systems fail to detect malicious code, anomalous behaviours, or return false positives or false negatives,[74] it is the cyber defender's responsibility to act.[75] Indeed, "the most critical component of cyberspace resiliency . . . most often lies outside cyberspace—with the human war fighter. People are what makes [*sic*] this work."[76] If the previous paragraphs seemed overly technical and disjointed from the paper's central topic, this previous sobering thought certainly brings the narrative back to the organizational dynamics surrounding resilience. As was argued by Cooley, the "M-Form legacies and institutions are more likely to endure after collapse of a hierarchy than U-

---

[71] Sajjan, Keynote Address . . .

[72] Ed Skoudis and Tom Liston, *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses, 2nd Edition* (New Jersey, Prentice Hall, 2006), 581-82

[73] Sajjan, Keynote Address . . .

[74] Chris Sanders and Jason Smith, *Applied Network Security Monitoring: Collection, Detection, and Analysis* (Waltham, MA: Elsevier Inc., 2014), 159.

[75] Lanouette, "Naval Cyber Warfare . . ., 52.

[76] Bryant, "Mission Assurance . . ., 12.

Form institutions."[77] Although Cooley's statement was made in the political context, organizations continuously fight to evolve and not dissolve. The organizational pressures come in all sizes: funding shortfalls, staffing freeze, incompatible social trends, aging demography, disruptive technologies, increased operational demands, increased media scrutiny, political turmoil, new legislative framework, environmental disasters, and legitimacy crisis are but a few examples. DND/CAF is not immune to those pressures, and certainly, its cyber capability—once matured—will be more resilient in the context of a Conceptual M-Form Cyber Structure. This organizational resiliency will translate into operational resiliency, which in cyberspace signifies operational effectiveness.

FINAL ANALYSIS AND CONCLUSION

The sum of these findings presents a dichotomy between governance, unique attributes, resilience, and standardization and information symmetry. Three—governance, unique attributes, and resilience—seem to favour the Conceptual M-Form Cyber Structure, while the other—standardization and information symmetry—seem to favour the opposite. To resolve the dichotomy, the element of temporality needs to be considered. Given the nascence of the cyber capability within DND/CAF and the resultant increased potential for principal-agency problems as well as authority, responsibility and accountability definition problems, the governance advantages conferred by a Conceptual M-Form Cyber Structure may quickly be counterbalanced by the Conceptual U-Form Cyber Structure's improved standardization and information symmetry. Similarly, the previously described unique attributes along with the concept of resilience both infer a cyber capability that is more mature than currently available in

[77] Cooley, *Logics of Hierarchy* . . ., 13.

DND/CAF. For those reasons, and as this paper initially contended as its thesis, the conflation of governance, unique DND/CAF attributes, resilience, as well as standardization and information symmetry favours the Conceptual U-Form Cyber Model as the preferred *initial* organizational model, which would favour a joint organization performing the cyber operator work on behalf of the services. However, given temporality has significantly affected the conflation's overall assessment, it is important to only consider it valid up until DND/CAF's cyber capability has sufficiently matured, at which point a new assessment would be required. Based on the presented arguments, it seems more likely that the then-preferable model will be the Conceptual M-Form Cyber Model, the organizational dynamics of which will favour a service-specific cyber operator and capability.

Although a small step forward in the resolution of a significantly more complex problem, the M-Form and U-Form organizational dynamics analyzed in the context of cyber capability development have helped understand many of the considerations related to a service-specific cyber capability and a joint cyber capability performing work behalf of the services. The above findings are relevant not only because they can be used to further the analysis of the DND/CAF cyber capability's organizational structure, but also, they give insight on elements which could impact social dynamics within the services and which could be used in future cyber-related occupational analyses. It remains that this paper has three significant flaws: first, it is predicated on the critical assumption that the service-specific networks and systems require cyber operators for their security and protection; second, it is limited in its theoretical rigour as it uses only one organizational model; and third and last, it does not address the notions of scale and scope—concepts

that have correlation to size—which are important factors in choosing the appropriate organizational form. The seminal works of Oliver Williamson and Alfred Chandler should be reviewed to gain an appreciation of these notions.[78] For instance, preliminary research on relatively small to medium-sized cyber military forces such as the United Kingdom, Australia, New Zealand, France, Spain, Hungary, Czech Republic, Lithuania, and Slovakia, all point to centrally coordinated organizations. In contradistinction, the United States have comparatively massive service-specific cyber commands as well as a separate US Cyber Command joined with the NSA, which together represent a decentralized organization. Readers should therefore carefully consider these limitations when using the information within.

Together with the recommendations to analyze the scale and scope of the organization, to validate the critical assumption, and to expand the study to the use of other organizational analysis models, there are a number of other areas which should be explored to ultimately answer the research question. First, DND/CAF should carefully consider whether a theoretical framework will be more conducive to developing the right cyber capability than an iterative process. The high priority, visibility and urgency conferred to the development and implementation of a robust cyber capability, as well as the requirement to achieve resilience sooner rather than later, may be incompatible with an approach fully supported by research. Second, there should be a study of the organizational and employment models of the intelligence and signal communities. Given the close relationship these share with the cyber domain, such a study could give

[78] Also in the bibliography, these works are: Oliver E. Williamson, *Markets and Hierarchies: Analysis and Antitrust Implications* (New York: Free Press, 1975); Alfred D. Chandler Jr., *Strategy and Structure: Chapters in the History of the American Industrial Enterprise* (Cambridge: MIT Press, 1969); Alfred D. Chandler Jr., *Scale and Scope: The Dynamics of Industrial Capitalism* (Cambridge: Harvard University Press, 1990).

additional insight. Third, as this paper centered its analysis on the force generation of cyber capability, efforts should be applied to study the organizational dynamics in the context of force employment.

BIBLIOGRAPHY

Allen, F. *Record of Discussion – Cyber Operator Sponsor Advisory Group (SAG) 3 Meeting Held at NDHQ Ottawa on 20 January 2016*. Director General Cyber and Director Personnel Generation Requirements: file 5555-CYBER-1 (DPGR 2-7), 29 February 2016.

Barbadoux, Pierre. "A Design-Oriented Approach to Organizational Change: Insights from a Military Case Study." *Journal of Organizational Change Management* 24, no. 5 (2011): 626–639.

Bensing, Richard. "An Assessment of Vulnerabilities for Ship-Based Control Systems," Master's Thesis, Naval Postgraduate School, 2009.

Brangetto, Pascal. *National Cyber Security Organisation: France.* Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Bryant, William D. "Mission Assurance through Integrated Cyber Defense." *Air and Space Power Journal* 30, no. 4 (Winter 2016): 5–17.

Burton, Joe. "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation." *Defence Studies* 15, no. 4 (2015): 297–318.

Butrimas, Vytautas. *National Cyber Security Organisation: Lithuania.* Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Canada. Chief of Force Development. *The Future Security Environment 2013-2040*. Ottawa: Department of National Defence, 2014.

—. Department of Public Safety. *Action Plan 2010-2015 for Canada's Cyber Security Strategy*. Ottawa: Department of Public Safety, 2013.

—. Department of Public Safety. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa: Department of Public Safety, 2010.

—. Department of Public Safety. *Cyber Incident Management Framework for Canada*. Ottawa: Department of Public Safety, 2013.

—. Defence Research & Development Canada – Centre for Operational Research and Analysis. *CF Cyber Operations in the Future Cyber Environment Concept*. Ottawa: Department of National Defence, 2009.

—. Treasury Board Secretariat. *Operational Security Standard: Management of Information Technology Security (MITS)*. Ottawa: Treasury Board Secretariat, 2004, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328, last accessed 2 May 2017.

—. Treasury Board Secretariat. *Policy on Government Security*. Ottawa: Treasury Board Secretariat, 2012, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578, last accessed 2 May 2017.

—. Treasury Board Secretariat. *Security Organization and Administration Standard*. Ottawa: Treasury Board Secretariat, 1995, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12333, last accessed 2 May 2017.

—. Vice Chief of Defence Staff. *The CAF C4ISR Strategic Vision, Goals and Objectives*. Ottawa: Department of National Defence, 2016.

Cendoya, Alexander. *National Cyber Security Organisation: Spain.* Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Chandler Jr., Alfred D. *Scale and Scope: The Dynamics of Industrial Capitalism*. Cambridge: Harvard University Press, 1990.

—. *Strategy and Structure: Chapters in the History of the American Industrial Enterprise*. Cambridge: MIT Press, 1969.

Cilluffo, Frank J. and Joseph R. Clark. "Repurposing Cyber Command." *Parameters* 43, no. 4 (Winter 2014): 111–118.

Conti, Gregory, and David Raymond. "Leadership of Cyber Warriors: Enduring Principles and New Directions." *Small Wars Journal* 7, no.7 (July 2011): 1–10.

Cooley, Alexander. *Logics of Hierarchy: The Organization of Empires, States, and Military Occupations*. Ithaca, New York: Cornell University, 2005.

Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace.* Calgary: Canadian Defence & Foreign Affairs Institute, 2012.

Freeland, Robert F. "The Myth of the M-Form? Governance, Consent, and Organizational Change." *American Journal of Sociology* 102, no. 2 (September 1996): 483–526.

Geers, Kenneth. "The Cyber Threat to National Critical Infrastructures: Beyond Theory." *Information Security Journal: A Global Perspective* 18 (2009): 1–7.

Glorioso, Ludovica. *National Cyber Security Organisation: Italy*. Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Hawco, D.C. *Job Study – Problem Definition Paper Cyber Specialist and Cyber Staff (Officer and NCM)*. Director General Cyber: file 5000-1 (D Cyber FD), 23 October 2013.

Hawkins, Zoe, and Liam Nevill. *Digital Land Power: The Australian Army's Cyber Future*. Barton, Australia: The Australian Strategic Policy Institute Limited, December 2016.

Holian, Matthew J. "Understanding the M-Form Hypothesis." *Journal of Industrial Organization Education* 5, no. 1, Article 4 (2010): 1–10.

Hriciková, Lea and Kadri Kaska. *National Cyber Security Organisation: Slovakia.* Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Johnson, J. "What Can RCAF Do Against Cyber Threats?" Joint Command and Staff Programme, Canadian Forces College, 2017.

Kovács, László, and Gergely Szentgáli. *National Cyber Security Organisation: Hungary*. Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Lanouette, J.M. "Naval Cyber Warfare: Are Cyber Operators Needed on Warships to Defend Against Platform Cyber Attacks?" Joint Command and Staff Programme, Canadian Forces College, 2016.

—. "Naval Cyber Warfare Capability Requirements." Joint Command and Staff Programme, Canadian Forces College, 2016.

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

Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89, no. 5 (September 2015): 97–108.

Minárik, Tomáš. *National Cyber Security Organisation: Czech Republic.* Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Moens, Alexander, Seychelle Cushing, and Alan W. Wood. *Cybersecurity Challenges for Canada and the United States*. Vancouver, BC: Fraser Institute, 2015.

Norman, M.A.G. *VCDS Initiating Directive - Transfer of Leadership Responsibilities for VCDS Related Capability Development Responsibilities to ADM(IM), the Canadian Army and CFINTCOM*. Vice Chief of Defence Staff: file 1920-1 (CFD), 12 December 2016.

Okros, Alan. “Becoming an Employer of Choice: Human Resources Challenges within DND and the CF.” In *Public Management of Defence in Canada*, edited by Craig Stone, 141–193. Toronto: Breakout Education Network, 2009.

Osula, Anna-Maria. *National Cyber Security Organisation: United Kingdom.* Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Ouchi, William G. “The M-Form Society: Lessons from Business Management.” *Human Resource Management (pre-1986)* 23, no. 2 (Summer 1984): 191–213.

Pernik, Piret, Jesse Wojtkowiak, and Alexander Verschoor-Kirss. *National Cyber Security Organisation: United States.* Tallin, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Platt, Victor. “Still the Fire-Proof House? An Analysis of Canada’s Cyber Security Strategy.” *International Journal* 67, no. 1 (March 2012): 155–167.

Sajjan, Harjit. Keynote Address, Security Innovation Network’s Information Technology Security Entrepreneurs Forum, Silicon Valley, California, United States, 20 April 2016.

Skoudis, Ed, and Tom Liston. *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses, 2nd Edition*. New Jersey, Prentice Hall, 2006.

Sanders, Chris, and Jason Smith. *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Waltham, MA: Elsevier Inc., 2014.

United Kingdom. Ministry of Defence. *Strategic Trends Programme: Global Strategic Trends - Out to 2045*. London: Ministry of Defence, 2014.

United States. National Institute of Standards and Technology. *Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security*. Washington, D.C.: US Department of Commerce, 2015.

—. United States Air Force. *Information Dominance Vision*. Washington, D.C.: United States Air Force, 2016.

Vance, J.H. *CDS Directive – CAF Integrated Command and Control Information System*. Chief of Defence Staff: 3 December 2015.

—. *Record of Discussion – Armed Forces Council (AFC) #160322*. Chief of Defence Staff: file 1150-4 (D NGHQ Sec), 22 March 2016.

Welsh, William. “Cyber Warriors: The Next Generation.” Last accessed 7 May 2017, https://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx.

Williamson, Oliver E. *Markets and Hierarchies: Analysis and Antitrust Implications*. New York: Free Press, 1975.

Young-Ju, Lee. “Establishment of a Feasible Cyber Organization Structure to Enhance the Capabilities of Cyberspace Operations in the ROK’s Defense Forces.” *The Korean Journal of Defense Analysis* 28, no. 2 (June 2016): 223–248.