National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER OPERATIONS AND PROFESSION OF ARMS

Major Lauren Banks

JCSP 46

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 46

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 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

CYBER OPERATIONS AND PROFESSION OF ARMS

By Major Lauren Banks

Word Count: 5,270

Nombre de mots : 5.270

CYBER OPERATIONS AND THE PROFESSION OF ARMS

"Despite our dependence on technology, wars will continue to be decided by people. So we must also create a cultural shift in which we value the innovators, experimenters and creative thinkers despite drawdowns and resource constraints. Our military structure must find ways to accommodate these skills within our cyber forces, including the ability to think in new and innovative ways."
- Lt. Gen. Edward C. Cardon, US Army

INTRODUCTION

Although the Canadian Armed Forces (CAF) has been historically configured to counter traditional military threats within the conventional air, land, and sea domains, the advent of hybrid threats from Canada's adversaries has necessitated the creation of forces capable of fighting in the non-traditional domains of information, space, and cyber. This is highlighted throughout the recently published CAF Pan-Domain Force Employment Concept (PFEC), which states that "Our adversaries are challenging us in the cyber, space, and information domains as well as in the land, maritime, and air domains. We must meet this challenge across all domains."[1] As strategic-level acknowledgement of this problem space has been increasing over the past decade, the demand for professional military cyber forces in the CAF led to the establishment of the Cyber Operator trade in 2017 to "conduct defensive cyber operations, and when required and where feasible, active cyber operations."[2] Despite several successful years for the trade, there remains significant skepticism and apprehension surrounding the CAF's ability to build and equip a uniformed force of cyber practitioners. In the absence of a conventional military requirement for uniformed members to perform tasks that can largely be done virtually, many feel that the CAF should either contract out the work, hire teams of highly paid civil servants within DND, or leave it to Other Government Departments (OGDs) to fill the gap. However, this rationale usually focuses on the aspects of military service as a hindrance to the recruitment and

[1] Canada. Department of National Defence. Pan-Domain Force Employment Concept. (Ottawa, ON: 2020), 4.
[2] Government of Canada. "Cyber Operator." https://forces.ca/en/career/cyber-operator/ (Accessed 5 May 2020)

retention of exceptional cyber professionals, instead of identifying ways in which existing military culture and traits could be leveraged to maximize the effectiveness of the CAF Cyber Force.

This paper will demonstrate that it is both feasible and necessary for the CAF to build and sustain a uniformed military CAF Cyber Force. This will be done by first examining the traits that are necessary for success within the broader cybersecurity profession and applying the principles of the CAF Profession of Arms in order to identify areas where the CAF could leverage existing military ethos to build the most effective CAF Cyber Force. It will then examine the challenges faced regarding recruitment and retention of members within the Cyber Operator trade through the lenses of Universality of Service and intrinsic vs. extrinsic motivation. Finally, several recommendations will be provided on the way forward for the CAF to fully leverage the benefit of military service to build the most effective and operationally-focused military Cyber Force. For the purposes of this paper, the 'CAF Cyber Force' refers to members of the Cyber Operator non-commissioned member (NCM) trade, as well as Officers who are employed within Defensive Cyber Operations or Offensive Cyber Operations roles.

SOCIAL ASPECTS OF THE CYBER WORKFORCE

When considering the relevant factors of employing a uniformed CAF Cyber Force, it is critical to consider the social dimension of the cyber profession in addition to the technical requirements that are more often the focus. In their article, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," Dawson and Thompson present the argument that failing to consider the social aspects of human behaviour within the cyber domain neglects a critical component in the development of a cybersecurity

workforce.[3] Further to this, they write:

> While there is a general appreciation of the social layer in broader cyber operations (e.g. the role of social networking in recent political unrest) and in intelligence analysis, there is less emphasis placed on understanding the role of social traits of the individual cybersecurity professional and their work performance.[4]

This is particularly relevant for the CAF, as it suggests that selection and recruitment should not focus entirely on technical skills or aptitude, but also on the military-specific ethos that could indicate success for future Cyber Operators. Further to this, the most effective approach to identifying and recruiting members who are best suited for service in the CAF Cyber Force would be to align the social traits of an effective cybersecurity professional with those of an effective service member. This section will demonstrate that several traits deemed necessary for success in the cyber operations field are aligned with existing traits within the CAF.

Dawson and Thompson identify the following six traits that they hypothesize to be necessary in order for a person to be successful in the cyber workforce; systematic thinkers, team players, technical and social skills, civic duty, continued learning, and the ability to communicate technical information to an audience that might not have a technical background.[5] By examining several of these traits further, it is possible to see links and parallels to military service and the Profession of Arms, therefore demonstrating the opportunity for the CAF's existing foundational culture to lend itself to an elite cyber workforce. Further to this, while aspects of military service may be considered as a deterrent to those seeking to pursue a career in the cyber field, they may in fact be a way to attract and retain the people that the CAF seeks to employ.

---

[3] Jessica Dawson and Robert Thomson, The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance." *Frontiers in Psychology,* Volume 9 Article 744 (June 2018): 3.
[4] *Ibid.*, 2.
[5] *Ibid.*, 8-9.

Teamwork

The ability of an individual to operate within a team is critical to success in any current cyber work environment, as research has identified that cybersecurity teams are better able to solve complex tasks than individual analysts.[6] Further to this, "a current challenge with cyber security teams is that they tend to operate as a cluster of individuals in a group rather than exhibiting the cohesion and trust that involves a shared sense of identity."[7] While this may be a challenge within the private sector, the value of teamwork is an intrinsic part of the military ethos and, therefore, fully engrained into CAF members at the outset of their military training. As a fundamental belief and expectation of military service, there is an understanding among CAF members and, therefore, among Cyber Operators that "teamwork builds cohesion, while individual talent and the skills of team members enhance versatility and flexibility in the execution of tasks."[8] This foundational culture of teamwork bred into each CAF member will undoubtedly enhance his or her effectiveness when employed within a cyber role.

Civic Duty

Within the cyber profession, it is particularly important for all personnel to abide by a moral code and sense of duty towards their organization. As they often have access to all information on a network and have advanced administrator authorities to view, manage, and protect that information, their obligation to adhere to a strict moral code is essential in effectively security the networks and information within their purview. Additionally, it is very common for the cybersecurity specialists within an organization to possess advanced technical knowledge that is beyond the comprehension of senior leaders. When combined with the importance of

[6] Dawson and Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance." *Frontiers…*, 4.
[7] *Ibid.*, 8.
[8] Department of National Defence. *Duty With Honour: The Profession of Arms in Canada*. (Ottawa, ON: Canadian Defence Academy - Canadian Forces Leadership Institute, 2009), 29.

networks and systems to an organization's operations, this results in the need for a high level of trust placed in these cyber professionals. Dawson and Thompson further describe this as follows:

> Given the sensitivity of data that the cyber workforce will have access to, as well as the lack of knowledge of their superiors and their coworkers, the future cyber workforce is going to have to engender trust. Commitment to the organizational values as well as a national sense of pride and identity may go a long way in mitigating.[9]

This sense of duty is intrinsically woven into the Profession of Arms and is a common attribute across all military professionals in the CAF. In taking the oath of service, CAF members accept unlimited liability, which engrains a deep acknowledgement of service before self and unwavering commitment to mission accomplishment.[10] Although the nature of cyber operations does not always necessitate the member to physically deploy into harm's way, all uniformed members have an engrained sense of duty to Canada, their chain of command, and the mission. This same sense of loyalty and duty, when applied to the Cyber Operations field, would result in an exceptionally effective force.

Although there exists some overlap between the necessary traits for successful cyber professionals and CAF military service, there are numerous challenges facing the recruitment and retention of members within the CAF Cyber Force that must be addressed in order for these traits to be leveraged. If the CAF is to be successful in recruiting, training, employing, and retaining the most suitable individuals, then it is necessary to examine these challenges and determine ways to mitigate them, which will be further explored in the following section.

CHALLENGES FACING THE CAF CYBER FORCE

Over the past several years, there has been a growing shortage in cybersecurity skills with

[9] Dawson and Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance." *Frontiers…*, 9.
[10] Department of National Defence. *Duty With Honour: The Profession of Arms in Canada*, 27.

nearly three quarters of organizations globally affected by the shortage.[11] Consequently, there is concern that the CAF will face significant barriers when competing for a limited pool of qualified people, specifically surrounding the constraints tied to Universality of Service requirements and the rate of pay for CAF servicemembers compared with jobs within the private sector. However, further analysis suggests that Universality of Service requirements could actually benefit the CAF in attracting the right talent, as the unique cross-section of individuals who wish to identify as members of the Profession of Arms and have aptitude to succeed in cyber operations would excel within the Cyber Operator trade. This section will further examine how the commonly cited issues of recruiting and retention can be addressed with the correct approach to building a culture of professional military Cyber Operators that optimizes their intrinsic motivations and provides sufficient room to manoeuvre, operate autonomously, and pursue continuous professional development.

Current State of the Cyber Operator Trade

In order to analyze issues regarding recruitment and retention for the CAF Cyber Force, it is first necessary to examine the existing data that has been collected since the establishment of the trade. As of the date of this paper, 88 men and women have successfully been selected and transferred to the Cyber Operator occupation since its establishment in 2017.[12] This included two rounds of selection, the first drawing from a pool of existing uniformed members who had experience within the Canadian Forces Network Operations Centre (CFNOC) and the second drawing from the entire pool of serving CAF members who had reached Occupational

[11] "Cybersecurity Skills Shortage Worsening for Third Year in A Row, Sounding the Alarm for Business Leaders: Third Annual Global Study from ESG and ISSA Finds Cybersecurity Skills Shortage Impacts 74 Percent of Organizations; Explores Causes and Consequences of Cybersecurity Job Stress." (*NASDAQ OMX's News Release Distribution Channel*: 9 May 2019) https://search-proquest-com.cfc.idm.oclc.org/docview/2222013446?accountid=9867.

[12] Correspondence with Chief Warrant Officer Alex Arndt, 9 Apr 2020.

Functional Point (OFP) within their respective trades. Of those 88 personnel, there have only been a total of seven releases from the Regular Force, with three of those released members opting to pursue civilian employment within other departments of the Canadian government.[13] Of note, five of the personnel cited family stability as the reason for their retirement from military service, and a sixth member expressed that his reason for leaving was to return to more technical work, instead of the leadership and management tasks of the senior non-commissioned rank that he retired from.[14] This suggests that although there may be factors to military service that might improve retention if addressed, such as geographic stability or allowing for technical career progression, it is important to note that higher pay and relaxed physical fitness or dress standards were not key factors in these members' decisions.

It must also be acknowledged, however, that the available statistics have limited long-term value due to the relatively recent standup of the trade and a variety of unique conditions surrounding the first several rounds of hires. As more members are recruited directly into the trade or choose to apply for Voluntary Occupation Transfer, the long-term effects on retention will be more fully realized. In order to inform decision-makers in determining long-term success of the trade, and of the CAF Cyber Force as a whole, it is beneficial instead to explore the concepts of Universality of Service and intrinsic motivation to more accurately predict the perceived recruitment and retention issues within the Cyber Operator trade.

Universality of Service

Due to the limited pool of people to draw from, one strategy to increase intake to the Cyber Operator trade is to consider reducing certain standards that might be a deterrent from people choosing to join the CAF instead of seeking employment in the private sector. However,

---

[13] *Ibid*.
[14] *Ibid*.

despite the fact that Cyber Operators are recruited for their mental and cognitive skills and not for their physical abilities, the rationale to reduce the standards could have a detrimental impact on the success of the Cyber Operator trade in the long term. Not only has physical fitness been linked to higher cognitive ability when performing cyber-related tasks,[15] but any effort to reduce or amend the Universality of Service requirements could hamper the identity of Cyber Operators as members of the Profession of Arms and, therefore, benefits from military ethos could be diluted.

Within the US, numerous experts have posited that the US military should consider holding cyber soldiers to different standards than traditional troops, such as those of dress or physical fitness, in order to attract, train, and retain the best and brightest cyber personnel.[16] However, differences in the size, scope of work, and identities between the US and Canadian militaries must be carefully considered if the CAF intends to apply this same approach. Although there is certainly value in considering waivers for exceptional circumstances, such as during periods of increased conflict or by leveraging the medical Temporary Category (TCAT) program to retain individuals on a case-by-case basis, the consequences of implementing broad policies across the trade must also consider the negative implications that such a decision might have.

One such aspect would be the residual effects on the Cyber Operators' identity within the construct of the military ethos. As demonstrated in the previous section, the qualities of teamwork and civic duty that are engrained in CAF members would serve to improve the performance of Cyber Operators in the conduct of their duties, but these benefits could be

---

[15] Kirsi Helkala, Benjamin Knox, Øyvind Jøsok, Silje Knox, and Mass Lund, "Factors to Affect Improvement in Cyber Officer Performance." *Information and Computer Security* 24, no. 2 (2016): 160.
[16] Crispin Burke, "The Pentagon Should Adjust Standards For Cyber Soldiers - As It Has Always Done." *War on the Rocks* (24 January 2018), https://warontherocks.com/2018/01/pentagon-adjust-standards-cyber-soldiers-always-done/ (Accessed 6 May 2020)

hampered if Cyber Operators are not held to the same standards as all other trades and occupations within the CAF. Duty With Honour highlights 'identity' as one of the key attributes within the CAF Profession of Arms and lists 'physical fitness' as a key concept "that serve(s) to develop the military members' professional self-portrait."[17] Those who are drawn to apply to the Cyber Operator trade are likely seeking to join the CAF as a part of their identity, so removing Universality of Service requirements that are common to all other uniformed trades runs the risk that the Cyber Operator trade will not fully adopt the identity of military service.

If the goal is to build a professional military force, then it must be expected that those who are motivated to join the Cyber Operator trade will rise to the same standards as their brothers and sisters in arms. It is also critical to preserve the integrity of the CAF identity within the Cyber Force in order to ensure that the people who identify as both military and cyber professionals are attracted and retained. Dawson and Thompson write:

> Individuals are attracted to organizations that they believe reflect their values or are likely to match their interests. Additionally, if individuals find an organization does not correspond with their values, they are significantly more likely to attrit and find a better fit.[18]

By compromising the identity of the CAF within the Cyber Operator trade, the drawbacks may outweigh the benefits and the CAF will undoubtedly face further issues with retention of talent.

Intrinsic vs. Extrinsic Motivators

One of the most significant concerns regarding retention of Cyber Operators is pay. Given that the military pay scale is capped by rank, there is a concern that even with Specialist Pay incentives, the salary that the CAF can offer skilled Cyber Operators might be significantly

[17] Department of National Defence. *Duty With Honour: The Profession of Arms in Canada*, 20.
[18] D Dawson and Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance." *Frontiers…*, 6.

lower than what they could make within the private sector. However, there is evidence to suggest that not only does the CAF provide a competitive salary compared to the average civilian employer, but that the best and brightest talent within the Cyber Operations field may not be as motivated by a higher salary as many leaders assume.

It is commonly believed that jobs within the cybersecurity private sector are extremely lucrative, with many positions offering six figures or more. Although there do exist certain high-paying jobs, these positions usually require advanced skillsets and are not the norm. In fact, the average cyber security analyst salary in Canada is approximately $65K, with typical range of salaries falling between $45K and $88K.[19] Comparatively, the basic pay of a Cyber Operator at the Corporal rank level is $67K, as the trade is within the Specialist 1 pay category.[20] When factoring in the additional incentives of pension, opportunities for advancement, and benefits related to training and temporary duty travel, the salary offered by the CAF is quite competitive when compared to similar positions elsewhere in the industry.

In order to conduct a more holistic analysis, however, it is also critical to examine the various motivational factors that might contribute to the retention of the CAF Cyber Force. In his book *Drive*, Daniel H. Pink describes this concept by examining the social psychology behind the use of extrinsic rewards and how they apply to logarithmic and heuristic work. According to Pink, a logarithmic task is "one in which you follow a set of established instructions down a single path to conclusion,"[21] whereas a heuristic task is one in which "you have to experiment with possibilities and devise a novel solution."[22] Although it is generally believed that the

---

[19] "Average Cyber Security Analyst Salary in Canada." https://www.payscale.com/research/CA/Job=Cyber_Security_Analyst/Salary. (Accessed 6 May 2020)
[20] Government of Canada, "Pay Rates for Non-Commissioned Members." https://www.canada.ca/en/department-national-defence/services/benefits-military/pay-pension-benefits/pay/non-commissioned.html. (Accessed 6 May 2020)
[21] Daniel H. Pink, *Drive* (New York: Penguin Press, 2009), 23.
[22] *Ibid*.

presence of additional extrinsic rewards, such as higher pay, will always lead to higher job satisfaction and productivity, researchers have found that "external rewards and punishments… can work nicely with algorithmic tasks. But they can be devastating for heuristic ones."[23] In other words, people who work in fields that require creativity and problem-solving are most effective when they are not rewarded by extrinsic factors, but rather are driven to succeed by intrinsic motivation. From a CAF perspective, this can provide some useful insight into the type of recruit that would thrive within the CAF Cyber Operator profession, and the degree to which these individuals would be motivated by extrinsic factors, such as a higher paycheque.

The application of Pink's theory to the Cyber Operator profession, however, is contingent on whether cyber operations would be considered logarithmic or heuristic in nature. There may be an inclination to view cybersecurity work as logarithmic due to the required in-depth technical knowledge of the cyber domain, coupled with the military's use of repeatable processes such as Tactics, Techniques and Procedures (TTPs) and Standard Operating Procedures (SOPs). However, further analysis of the cybersecurity environment would reveal the opposite to be true. As Dawson and Thompson write:

> This complexity of human interactions across layers creates the uniqueness of the cyber domain, and it is understanding these human interactions that create underlying vulnerabilities on the network. In addition, cyber offensive techniques are often contingent upon exploiting known human behaviours. Therefore, cybersecurity professionals must understand not only the technical aspects of their field but also possess an in-depth knowledge of human interactions.[24]

To apply these principles in a military context, Cyber Operators are engaged in warfare through the cyber domain and, therefore, they not only must understand the human interactions that occur within the systems but also the added layer of adversary engagement, friendly use of

---

[23] *Ibid*, 24

[24] Dawson and Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance." *Frontiers…*, 2.

systems, and overall mission. It is fairly simple to see this concept in the context of cyber warfare when considering one of Sun Tzu's fundamental theories on war:

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.[25]

When the role of the CAF Cyber Force is viewed not simply as a technical function, but as a form of military operations to which operational art must be applied, it is evident that the tasks required for it to be effective are the artistic, empathetic, and non-routine tasks that define heuristic work.[26]

This is fundamentally important for the CAF Cyber Force, as it provides a starting point to assess the underlying motivating factors that would, if maximized, not only recruit the brightest talent, but drive them to work to their maximum potential. Pink proposes that this intrinsic motivation can be fostered through autonomy, ample opportunity to pursue mastery, and believing in their work as it relates to a larger purpose.[27] Having examined the application of the Profession of Arms to the cybersecurity workforce, and with a deeper understanding of the intrinsic motivation that will drive the most effective military cyber operations professionals, the following section will pose several recommendations on how the CAF can leverage these concepts to continue to build the most effective CAF Cyber Force.

RECOMMENDATIONS FOR THE CAF CYBER FORCE

Despite the arguments supporting the employment of military cyber forces within Canada, the reality of CAF resource constraints has necessitated significant skepticism as to the role of the Canadian military in future cyber operations. As the cyber domain is unrestricted by

---

[25] Sun Tzu, *The Art of War*. Translated by Samuel B. Griffith. (Oxford University Press, 1963)
[26] Pink, *Drive*, 26.
[27] *Ibid*. 58

geography and effects can be achieved remotely, the role of the military within the Whole-of-Government approach when facing Canada's adversaries remains in question. Further to this, the Government of Canadian (GoC) has demonstrated the intention to reconsider long-standing norms and provide new authorities to OGDs that would enable a more integrated approach across all departments. For example, the authority to conduct Active Cyber Operations (ACO) was added to the mandate of the Canadian Security Establishment (CSE) upon royal assent of Bill C-59, which authorized CSE to:

> …carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization on terrorist group as they relate to international affairs, defence or security.[28]

This could lead many to believe that if another GoC agency is able to conduct ACO, then building such a capability within the CAF, despite being a conceptually good idea, could be considered redundant or a misuse of resources. However, this line of thinking fails to acknowledge ACO as an arm of joint military operations and, consequently, discounts the military skills and aptitudes needed to effectively integrate the employment of ACO effects.

Further to this, failing to develop an integrated military force that is capable of engaging in cyber warfare will cripple the CAF as a fully enabled, modern, and capable military force within the international military community. When describing the potential dangers of only investing in defensive cyber capabilities, Brigadier Marcus Thompson, Australian Army, summarized that "it is not good enough for a professional military force to be capable of only 'taking a punch'"[29] and "professional military forces cannot always choose the terrain in which

---

[28] Bill C-59, *An Act Respecting National Security Matters*, 1st sess., 42nd Parliament, 2019, clause 76 (assented to 21 June 2019), para 19. https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent#ID0EQTCK (Accessed 3 May 2020)

[29] Marcus Thompson, "The ADF and Cyber Warfare." *Australian Defence Force Journal* (No. 200, 2016) https://www.defence.gov.au/ADC/ADFJ/Documents/issue_200/Thompson_Nov_2016.pdf, 46.

they fight. Nevertheless, they must understand, and be prepared to fight, in any terrain occupied by an adversary."[30] Similarly, the requirement for uniformed forces within the US military has been acknowledged due to the requirement for integration of cyber capabilities into full-spectrum operations, authority to operate within the context of a military conflict, and deployability of cyber forces.[31]

Although Canada will require an approach that takes into account the unique authorities, relationships, and resource constraints of the GoC, the need for a uniformed force of Cyber Operators will undoubtedly prevail. As previously demonstrated in this paper, it will not only be possible to build an advanced CAF Cyber Force that is capable of meeting the demands of the future threat environment, but it will be well poised to do so by leveraging the strengths of the military to attract and retain the best cyber talent. In order to accomplish this, the following sections provide recommendations on establishing a strong cyber warfighting culture within the CAF, as well as strategies to foster the intrinsic motivation that will drive the CAF Cyber Force to excel.

Cyber Military Culture

In order to effectively build the professional military cyber force required, the CAF must aim to establish a strong military culture within the CAF Cyber Force that portrays the image of a Cyber Operator not as a standard cybersecurity professional in uniform, but as a distinct and elite military professional. Fostering this strong military identity among the CAF Cyber Force will be critical in maintaining the pride and distinction that comes with serving in uniform, as the lack of this distinction will undoubtedly cause the Cyber Operators to see themselves as

---

[30] *Ibid.*, 27.
[31] Christopher Paul, Isaac R. Porche III, Elliot Axelband, *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces* (Santa Monica: RAND Corporation, 2014), 27.

indistinguishable from their civilian counterparts in the public or private sector. If the intrinsic motivation that comes with military identity is removed, it could be replaced by other motivating factors offered elsewhere outside the CAF.

It will undoubtedly be challenging as the CAF continues to invest in growing a robust and professional uniformed Cyber Force, but there is much to be leveraged from the efforts made by allies in the recent decades. For example, in February 2015 the US Army officially recognized the Cyber Branch and Career Management Field as its first new combat arms branch in nearly 30 years.[32] Within the Australian Defence Force (ADF), which is much closer in size and mandate to the CAF, the Information Warfare Division was established in 2017 "to make sure the ADF has the right people, skills, equipment and resources to combat the growing threat of information warfare to our war fighting capability and Australia's national interests."[33] Although there has been much progress within the CAF with the establishment of the Canadian Cyber Force, the Joint Force Cyber Component Command (JFCCC), and the Cyber Operator trade itself, this progress must continue in order to further establish the CAF Cyber Force as a recognized Force Employer and joint enabler across the broader CAF. Efforts to create a separate Cyber Officer occupation within the CAF, as both the US and Australian militaries have done, and the continued career management to place experienced Cyber Operations personnel in key positions within JFCCC and the Canadian Joint Operations Command (CJOC) will be critical in the success of this effort. Further research is recommended in both of these areas, as they are beyond the scope of this paper.

As previously mentioned, members of the CAF Cyber Force will need to closely integrate

[32] Edward C. Cardon, "Cyber Capabilities Key to Future Dominance." (*Army* 66, no. 2: 2016), 25.
[33] Australian Government. Department of Defence, "Information Warfare Division." https://www.defence.gov.au/jcg/iwd.asp (Accessed 3 May 2020)

with their counterparts elsewhere in government and industry as part of a Whole-of-Nation (WoN) effort. In establishing an advanced military cyber culture, the CAF Cyber Operators will undoubtedly bring a unique and valuable asset to this effort, and will demonstrate the same dedication and professionalism that the rest of the CAF is known for. In assessing how to effectively integrate into this WoN effort, the CAF must examine efforts among allies such as the ADF Information Warfare Division (IWD). This organization works closely with industry, academia, business, corporations and other government agencies to develop capabilities to be employed within the ADF across a number of activities, including "stability and security operations through to full conflict and war."[34] Further to this, there has been substantial progress within the US to acknowledge and embrace the roll of the military as a contributor to the broader National strategy, summed up by Lt. Gen. Cardon:

> Because the cyber domain is a combination of public, private, governmental, commercial and military activity, the Army does not enjoy a monopoly on cyber capability, talent or innovation. To succeed in the cyber domain, our partnerships with the brightest minds and most innovative organizations must be cultivated and retained to ensure our ability to operate on the leading edge and succeed in this dynamic domain.[35]

The establishment of a solid military culture within the CAF Cyber Force will ensure its readiness and ability to contribute effectively to joint military operations alongside the Canadian Army, Royal Canadian Air Force, Royal Canadian Navy, and CAF Space Force. This approach will also ensure the CAF's ability to contribute the necessary military arm to a WoN approach within Canada that is capable of meeting the demands of the future threat environment. To return to the personnel perspective, this will also ensure that members of the CAF Cyber Force fully embrace the identity of military ethos as members of the Profession of Arms. Equally important

---

[34] Australian Government. Department of Defence. "Information Warfare Division." https://www.defence.gov.au/jcg/iwd.asp (Accessed 3 May 2020).
[35] Edward C. Cardon, "Cyber Capabilities Key to Future Dominance." (*Army* 66, no. 2: 2016), 25.

to this will be continued efforts to foster the intrinsic motivation within these members in order to enable them to perform to their maximum ability. Recommendations on how to accomplish this will be provided in the following section.

Foster Intrinsic Motivation

As previously demonstrated, it will be critical to provide members of the future CAF Cyber Force with autonomy, pursuit of mastery, and larger purpose in order to foster the intrinsic motivation necessary for the most effective accomplishment of their duties. Failing to do this could result in retention issues, as the more advanced members could instead decide to pursue employment outside the CAF. This could also decrease the operational effectiveness of the force as a whole, as the lack of intrinsic motivation could result in decreased ability to solve the extremely complex threats within the cyber domain. However, successfully fostering this intrinsic motivation could not only elevate the overall effectiveness of the CAF Cyber Force members, but also attract and retain the most elite members of the broader cybersecurity workforce. This section will draw from the principles covered in the previous sections and make recommendations specific to CAF service on how intrinsic motivation can be fostered.

At first glance, autonomy may seem like a bad fit for a military environment, as the CAF typically employs a model of maximum accountability up the chain of command and a strict culture of following orders. However, the increasingly complex global environment and increased need for agility has resulted in senior leadership acknowledging the need to evolve. This is further defined in the PFEC:

> The increased importance of operating at the Speed of Operational Relevance and the imperative to synchronize activities and effects cross multiple domains will demand that authorities, responsibilities, and accountabilities (ARA) continue to be pushed as far forward as possible.[36]

[36] Canada. Department of National Defence. Pan-Domain Force Employment Concept. (Ottawa, ON: 2020), 26.

Although complete autonomy will not be possible, as cyber missions must be tied to the desired operational outcome and, therefore, certain constraints will need to be provided to assure overall mission success, the CAF Cyber Force must still provide leverage to the Cyber Operators at the pointy end to take action as necessary to accomplish the mission. They must be told what, but not how. From a social perspective, this is also supported by Dawson and Thompson that "within the cyber domain, clarity should identify best practices without being overly strict. Best practices should not become encoded rules or laws in order to prevent undue rigidity."[37] In providing clear guidance and direction through standard military mechanisms such as Orders and Rules of Engagement, as well as formalizing and socializing adequate ARAs that provide the necessary accountability without hindering freedom of action at the tactical level, the CAF's Cyber Operators will be enabled to take the necessary action to accomplish the mission effectively, and will remain motivated to continue to do so.

The need to pursue mastery, whether through practice or formalized training, is of particularly high importance to all members of the cyber profession. They must continuously dedicate effort towards training and education in order to keep up with rapidly evolving technologies and an increasingly dynamic threat environment, or risk becoming significantly less effective after as little as three months.[38] Although this is a trait common across all organizations that employ a cyber workforce and most companies recognize the importance of investing in the training of their personnel, the CAF particularly emphasizes Professional Development (PD) as a key factor to achieving the objective of maintaining the highest standards of professionalism within its ranks.[39] By leveraging the CAF's robust PD system through the continued

[37] Dawson and Thomson, "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance." *Frontiers…*, 8.
[38] *Ibid.*, 3
[39] Department of National Defence. *Duty With Honour: The Profession of Arms in Canada*, 57.

development of Cyber Operator courses, combined with an investment in continuous training offered by private industry, the CAF can ensure the continued learning of its personnel and support the pursuit of mastery that is required to keep them motivated.

Undoubtedly, the easiest intrinsic motivation factor that the CAF can offer is contributing to a higher purpose, as all serving CAF members are bound by fundamental Canadian military values and that "overall, (the) concept of duty motivates personnel both individually and collectively to strive for the highest standards of performance while providing them with purpose and direction throughout the course of their service."[40] Although CAF Cyber Operators will be bound to these values as members of the military profession, the further development of CAF cyber operations as a joint operational arm of the overall CAF mission will further foster the belief in a higher purpose.

CONCLUSION

This paper has demonstrated that not only does the CAF need to build an effective uniformed Cyber Force in order to remain relevant in future joint operations, but that the qualities engrained in military service members will be an asset to the uniformed military professionals within the CAF Cyber Force. This was done through an analysis of the necessary traits for success, several recruitment and retention considerations, and the intrinsic motivating factors that will contribute to the most elite cadre of Cyber Operators. If the CAF is successful in fostering a strong military cyber culture and providing the autonomy, opportunities for pursuit of mastery, and operationally-focused direction that promotes belief in the overall mission, then they will surely be successful.

The military ethos within the CAF Profession of Arms unifies the three professional

[40] *Ibid.*, 32.

attributes of identity, expertise, and responsibility.[41] As the CAF continues to evolve through the complex threat environment of the 21st century, it will be necessary to invest in the cadre of military professionals needed to meet the demands of the future operating environment. If the CAF is aiming to recruit the same people who would be drawn to employment outside of the military in search of a better pay check, then it is only a matter of time before those people leave. However, if the CAF aims to recruit cyber professionals that embody the same principles of unlimited liability, fighting spirit, discipline, teamwork, and physical fitness[42] that are intrinsic to the Profession of Arms, it will result in a highly effective force of talented Cyber Operators and reduce the likelihood of retention. The resulting CAF Cyber Force will be comprised of intrinsically motivated, operationally-focused military professionals who are trained and ready to face the hybrid threats facing the CAF in the future alongside their brother and sisters in arms in the other domains.

[41] Department of National Defence. *Duty With Honour: The Profession of Arms in Canada*, 8.
[42] *Ibid.*, 27-29.

BIBLIOGRAPHY

Australian Government. Department of Defence. “Information Warfare Division.” https://www.defence.gov.au/jcg/iwd.asp (Accessed 3 May 2020)

“Average Cyber Security Analyst Salary in Canada.” https://www.payscale.com/research/CA/Job=Cyber_Security_Analyst/Salary. (Accessed 6 May 2020).

Canada. Department of National Defence. Canadian Armed Forces Joint Doctrine Note: Cyber Operations. Ottawa, ON: D Cyber FD, 2017-02.

Canada. Department of National Defence. Duty With Honour: The Profession of Arms in Canada. Ottawa, ON: Canadian Defence Academy - Canadian Forces Leadership Institute, 2009.

Canada. Department of National Defence. Pan-Domain Force Employment Concept. Ottawa, ON: 2020.

Bill C-59, *An Act Respecting National Security Matters*, 1st sess., 42nd Parliament, 2019, clause 76 (assented to 21 June 2019). https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent#ID0EQTCK (Accessed 3 May 2020)

Burke, Crispin. “The Pentagon Should Adjust Standards For Cyber Soldiers - As It Has Always Done.” *War on the Rocks*. 24 January 2018. https://warontherocks.com/2018/01/pentagon-adjust-standards-cyber-soldiers-always-done/ (Accessed 6 May 2020)

Cardon, Edward C. "Cyber Capabilities Key to Future Dominance." *Army* 66, no. 2 (2016): 22-25.

Clausewitz, Carl V. *On War*. Edited and Translated by Michael Howard and Peter Paret. Princeton, New Jersey: Princeton University Press, 1976.

Clarke, Richard A and Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* New York: Penguin Press, 2019.

Correspondence with Chief Warrant Officer Alex Arndt, 9 Apr 2020.

"Cybersecurity Skills Shortage Worsening for Third Year in A Row, Sounding the Alarm for Business Leaders: Third Annual Global Study from ESG and ISSA Finds Cybersecurity Skills Shortage Impacts 74 Percent of Organizations; Explores Causes and Consequences of Cybersecurity Job Stress." *NASDAQ OMX's News Release Distribution Channel*, May 09, 2019. https://search-proquest-com.cfc.idm.oclc.org/docview/2222013446?accountid=9867. (Accessed 5 May 2020)

Dawson, Jessica and Robert Thomson. “The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Frontiers in Psychology 9 (2018): 744.

Hayes, Lt Col Jonathan, USMC. “A New Way to View Active Cyber Defense: Patrol Base Operations Offer and Model for Understanding and Framing Active Cyber Defense.” *Proceedings.* Annapolis: US Naval Institute. Vol 145/2/1392 (February 2019): 28-29.

Helkala, Kirsi, Benjamin Knox, Øyvind Jøsok, Silje Knox, and Mass Lund. "Factors to Affect Improvement in Cyber Officer Performance." *Information and Computer Security* 24, no. 2 (2016): 152-163.

Government of Canada. “Pay Rates for Non-Commissioned Members.” https://www.canada.ca/en/department-national-defence/services/benefits-military/pay-pension-benefits/pay/non-commissioned.html. (Accessed 6 May 2020)

Lewis, James A. “Cyberspace and Armed Forces: The Rationale for Offensive Cyber Capabilities.” *Strategic Insights.* Australia: Australian Strategic Policy Institute International Cyber Policy Centre. Published May 2016.

McQuaid, Patricia A and Stephanie Cervantes. “How to Achieve a Seasoned Cybersecurity Workforce.” *Software Quality Professional.* Milwaukee: American Society for Quality. Vol 21/4 (September 2019): 4-10.

National Initiative for Cybersecurity Careers and Studies. “NICE Cybersecurity Workforce Framework.” https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework (Accessed 2 May 2020).

Paul, Christopher, Isaac R. Porche III, Elliot Axelband. *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.* Santa Monica: RAND Corporation, 2014.

Pink, Daniel H. *Drive*. New York: Riverhead Books, 2009.

Robart, Brent. “Leadership Requirements in Emerging Domains of Operations.” Toronto: Canadian Forces College, 2019.

Thompson, Marcus. “The ADF and Cyber Warfare.” *Australian Defence Force Journal*. No. 200, 2016: 43-48. https://www.defence.gov.au/ADC/ADFJ/Documents/issue_200/Thompson_Nov_2016.pdf (accessed 2 May 2020).

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. Oxford University Press, 1963.

United States Cyber Command. “U.S. Cyber Command History.” cybercom.mil. https://www.cybercom.mil/About/History/ (accessed 2 May 2020).

United States Department of Defense. *Beyond the Build: Delivering Outcomes through Cyberspace*. Fort George G. Meade, Maryland: US Cyber Command, 3 Jun 2015.

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly*. National Defense University Press. Vol 73 (2nd Quarter 2014): 12-19.