National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

POLICY SHORTCOMING:
GROWING THE CAF CYBER OPERATOR OCCUPATION

Maj Mike Soley

JCSP 43 DL

Exercise *Solo Flight*

Disclaimer

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

PCEMI 43 AD

Exercice *Solo Flight*

Avertissement

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

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

POLICY SHORTCOMING: GROWING THE CAF CYBER OPERATOR OCCUPATION

Maj Mike Soley

Word Count: 3183

Compte de mots: 3183

POLICY SHORTCOMING:
GROWING THE CAF CYBER OPERATOR OCCUPATION

The Canadian Armed Forces (CAF) formally established the CYBER OPERATOR OCCUPATION on 31 January 2017, in order to grow its defensive and offensive cyber capabilities.[1] This paper aims to examine whether existing CAF and Government of Canada policy will adequately support the force generation of the specialized skills required to build Cyber Operator capacity.

To begin, this essay will demonstrate that existing CAF force generation policies to recruit specialized capabilities may be inadequate to meet the demand for the Cyber Operator Occupation. This paper will outline the global cyber threat facing Canada, and additional challenges for the CAF that shape the problem space for the force generation of Cyber Operators.

This paper will next outline CAF force generation capacity by exploring identified shortcomings in institutional recruitment, compensation, and retention policies. The intent is to identify policy gaps that further confound force generation efforts.

Given the global nature of the cyber threat, this paper will then examine the United Kingdom (UK) and United States (US) to determine how their respective militaries have approached this issue. Industry analysis and best practices will be considered to identify policies the CAF could adopt.

To conclude, this paper will outline policy areas to be addressed and updates that the CAF should consider to force generate Cyber Operators more effectively. This essay argues that

[1] Canada. Department of National Defence. *Military Employment Structure Implementation Plan (MES IP) For the CYBER OPERATOR Occupation*. Ottawa: Military Personnel Command, September, 2017, 3.

existing policy is inadequate to meet the demand for the Cyber Operator Occupation, but that best practices exist within allied military and industry policies that could be used to mitigate these policy shortcomings.

The Cyber Threat

The increasing prevalence of cyber warfare has complicated the traditional battle space, and this trend is set to continue. In assessing the future operating environment, the UK Ministry of Defence projects that adversaries will continue to "develop malicious cyber effects that strike at strategic, operational and tactical levels – not just against traditional military and critical infrastructure targets."[2]

To further complicate this general threat, the origins of a cyber attack can be indeterminate. Ridout describes the threat as "complicated by the multiplicity of state and non-state actors that can have an impact, combined with the difficulty of attributing malicious cyber activities to specific people and groups."[3] The cyber threat requires a whole of government response, including strong military action.

The CAF will encounter threats through its participation in the NATO deterrence mission against Russia. A significant enabler of Russian hybrid warfare strategy has been achieving dominance in the cyber domain. The country has demonstrated a high degree of skill, with cyber warfare capabilities becoming "one of the most important characteristics of Russian hybrid

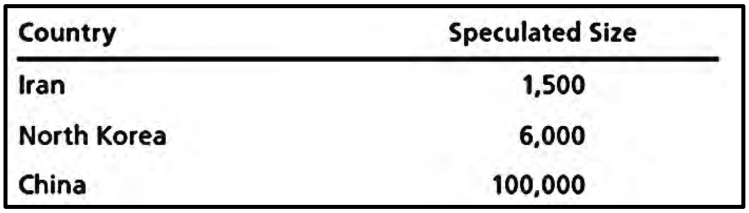
[2] United Kingdom. *Strategic Trends Programme: Future Operating Environment 2035*. 1st ed. Swindon: Ministry of Defence, November, 2014, 20.

[3] Ridout, Tim. "Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience." *The Fletcher Forum of World Affairs* 40, Building a Comprehensive Strategy of Cyber Defense no. 2 (Summer, 2016), 76.

tactics."[4] The UK assesses that Russian skill in this domain has progressed to the point that "they appear to be overmatching the West… with electronic warfare and cyber coming to prominence."[5]

Operations abroad are not the only concern for Canada, and the CAF must be prepared for malicious attacks from a range of actors. Projected strength of other adversary states' cyber elements are depicted in Table 1.

Table 1 - Potential Cyber Threat from Adversary States



Country	Speculated Size
Iran	1,500
North Korea	6,000
China	100,000

Adapted from: Table 2.4 Porche, Isaac R., I.,II, Caolionn O'Connell, Davis, John S.,II, Bradley Wilson, Chad C. Serena, Tracy G. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, and Michael Vasseur. Cyber Power Potential of the Army's Reserve Component: RAND Corporation, 2017, 19.

Note: Assessment of foreign military cyber forces made by original author using open source data.

The next most prevalent risk factor in generating CAF cyber capability is an identified shortage of cyber professionals. Research conducted by Libicki, Senty and Pollak note this shortage is especially acute for US Federal Government agencies. They note that "[g]overnment agencies face a more difficult challenge, since their pay scales are constrained," and that even for large institutions such as the CAF, with the capacity to recruit and train internally, there is still a shortage of skilled upper tier cyber expertise. [6]

[4] Oğuz, Şafak. "The New NATO: Prepared for Russian Hybrid Warfare?" *Insight Turkey* 18, no. 4 (Fall 2016): 165-80. Accessed November 26, 2017, 171.

[5] United Kingdom. *Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities*. Swindon: Ministry of Defence, February, 2018, 47.

[6] Libicki, Martin C., David Senty, and Julia Pollak. *Hackers Wanted: an examination of the cybersecurity labor market*. Rand Corporation, 2014, 72.

The extant threat of cyber attack underpins the requirement to force generate Cyber Operators for the CAF; however, competition from industry and other government departments has complicated the task.

CAF Force Generation Policy

In his mandate letter, the Minister of National Defence is charged to “protect Canadians and our critical infrastructure from cyber threats.”[7] Implicit within that statement is the task to generate a cyber capability for the CAF, further refined in the government’s most recent defence policy: *Strong, Secure, Engaged* (SSE). This section argues that existing CAF policy is insufficient for generating cyber capability.

A recent audit by the Office of the Auditor General (OAG) found institutional recruitment and retention policies for the CAF lacking. The OAG determined that current recruitment policy struggles to meet CAF requirements, noting it unlikely “that [the Regular Force] will be able to recruit, train, or retain sufficient personnel to meet its target of 68,000 members by the 2018–19 fiscal year.”[8] A subsequent report, focused solely on the Army Reserve, reached similar conclusions, noting that the “recruiting system was not able to recruit the number of soldiers needed by the Army Reserve, and that Army Reserve units had difficulty retaining their trained soldiers.”[9]

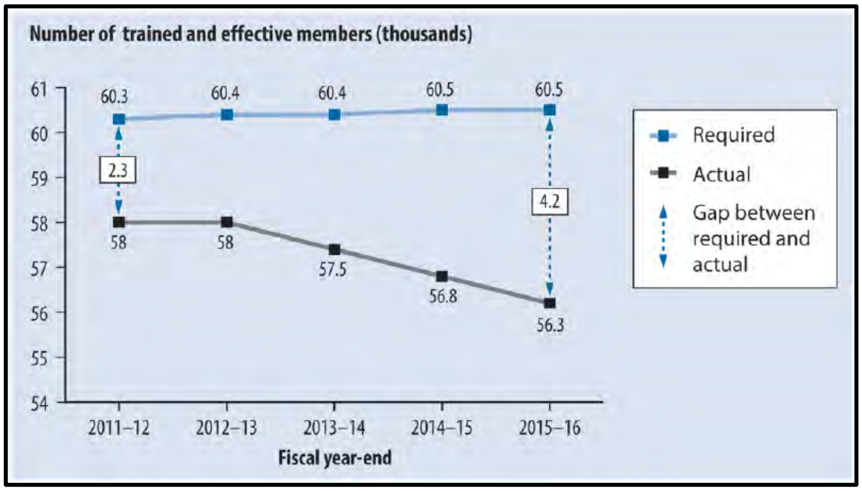
[7] Government of Canada. *Minister of National Defence Mandate Letter*. Ottawa: Office of the Prime Minister, 2015. Accessed March 10, 2018, 4. https://pm.gc.ca/eng/minister-national-defence-mandate-letter.

[8] Canada. Office of the Auditor General of Canada. *Report 5—Canadian Armed Forces Recruitment and Retention—National Defence*. 2016 Fall Reports of the Auditor General of Canada. Ottawa, ON: Government of Canada, 2016, 2.

[9] Canada. Office of the Auditor General of Canada. *Report 5— Canadian Army Reserve-National Defence*. 2016 Fall Reports of the Auditor General of Canada. Ottawa, ON: Government of Canada, 2016, 10.

The report determined that existing force generation policies to recruit and retain soldiers have led to a growing delta between recruitment capacity and the overall size of the force (Table 2); the shortage of trained personnel across the CAF is growing.

Table 2 - Growing Shortage of Trained CAF Personnel



Source: Canada. Office of the Auditor General of Canada. *Report 5—Canadian Armed Forces Recruitment and Retention—National Defence*. 2016 Fall Reports of the Auditor General of Canada. Ottawa, ON: Government of Canada, 2016, 5.

Specific policy gaps have been recognized by the OAG and acknowledged by the CAF. Failure to update or address policies that affect recruitment, workforce management and compensation, and retention will adversely affect growth objectives for the Cyber Operator Occupation.

Recruitment

The first gap is an effective recruitment strategy beyond general CAF efforts, which have been determined by the OAG to be deficient. If the CAF is challenged to effectively recruit and subsequently retain soldiers to meet its requirements, how will applying these same policies affect the pursuit of Cyber Operators? Research into the availability of trained cyber personnel noted that the "projected shortage is exacerbated by a rapidly growing demand for cybersecurity personnel in the private sector."[10] How will the CAF competitively recruit experienced individuals for full- or part-time reserve service?

Workforce Management and Compensation

Has the CAF planned to manage highly trained expertise from industry, or will it solely rely on training internal personnel with all applicants joining at the entry level? Will there be flexibility to transition between military and civilian service, as outlined in SSE, to "create a more agile model that supports the transition between full- and part-time service that meets the needs of the member and the institution?"[11]

CAF Cyber Command acknowledges the issue, stating that "[s]tructure does not address [the] challenge of ensuring that the right people receive the right training and are then operationally-employed in the cyber domain."[12]

A further policy gap relates to a reserve or part-time component. Analysis is ongoing, yet a definitive role for a Reserve Cyber Component is not yet complete. CAF Cyber Command has stated that "analytical work is currently underway to identify which cyber operations-related tasks can be performed by Reservists and how Reserve personnel with existing technical training can best support the CAF Cyber mission set."[13] A definitive plan must be put in motion.

[10] Porche, Isaac R., I.,II, Caolionn O'Connell, Davis, John S.,II, Bradley Wilson, Chad C. Serena, Tracy G. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, and Michael Vasseur. Cyber Power Potential of the Army's Reserve Component: RAND Corporation, 2017, xiii.

[11] Canada. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy.* Ottawa: Department of National Defence, 2017, 16.

[12] Canada. Department of National Defence. *CAF Cyber Capability – Reserve Component: Ideation & Planning Session*. Ottawa: CAF Cyber Command, December, 2017, slide 5.

[13] Canada. Department of National Defence. *CAF Cyber Capability …*, slide 12.

Retention

The OAG report further found that "certain practices in the recruitment process prevented qualified candidates from being enrolled," and articulated that the process "has a large impact on how long they will stay in the Canadian Armed Forces."[14] This speaks to the current organizational culture, with Cyber Command afforded a unique opportunity to influence a new military trade.

A final retention consideration would be Universality of Service. Will all Cyber Operators be required to deploy on operations, or is there an alternative employment model? The CAF Cyber Command acknowledges there are constraints within existing policy: "[c]urrent Universality of Service … may not suit some options under consideration."[15]

The CAF, and specifically Cyber Command, has acknowledged the identified shortcomings contained within the OAG report, stating that "more creative and tailored attraction, advertising, and marketing strategies are required to meet its recruiting targets for a number of occupations."[16] The CAF recognizes there are operational and strategic consequences in not addressing this issue, including: risk to CAF members, risk to sensitive information, significant financial cost, loss of access to allied information, or political embarrassment to the Government of Canada.[17] More importantly, not addressing the issue hands an advantage to the adversary.

While the CAF has taken the first steps in formalizing a cyber capability and is identifying the policy updates required to support capable force generation, many of Canada's

[14] Canada. Office of the Auditor General of Canada. *Report 5—Canadian Armed Forces Recruitment and Retention…,* 11.

[15] Canada. Department of National Defence. *CAF Cyber Capability …*, slide 14.

[16] Canada. Office of the Auditor General of Canada. *Report 5—Canadian Armed Forces Recruitment and Retention…,* 13.

[17] Canada. Department of National Defence. A-PD-055-002/PP-002 CYBER OP MOS ID..., 9.

allies have already taken similar steps; are there lessons that can be leveraged from allied militaries and the private sector?

Allied Perspective

Canada's allies are ahead of the CAF in addressing issues affecting cyber operator generation. This section will examine the perspectives of both the UK and US militaries and industry, as both nations reached similar conclusions on how to generate their respective cyber capabilities.

The UK notes that "[a]ppropriately targeted recruitment, education, training and retention of personnel for cyber operations will be key."[18] The US Army shares a similar viewpoint, noting it must "focus and strive to produce world-class cyberspace professionals by investing substantial energies into innovative recruiting, talent management and retention endeavors."[19] These are all policy areas identified in the OAG's report as inadequate.

Recruitment

A critical element of force generation is attracting the right personnel. A reoccurring theme in the current literature is that restrictive public sector human resource policies are inhibiting growth. Fortson notes that in addition to addressing policy, a wholesale cultural change is required: "the organizational culture transformation needed requires a strategy and

[18] United Kingdom. *Strategic Trends Programme…*, 33.

[19] United States. United States Army War College. *Putting the Pieces Together: Army Cyber Warrior Talent Management.* By Calondra L. Fortson, Colonel. Washington, D.C.: U.S. Army War College, 2017, Abstract.

operational approach committed to a renewal in thought, eliminating or minimizing parochial politics and a paralyzing bureaucracy."[20]

One unique factor of military service is government-sanctioned cyber warfare. An article on building the US Cyber Corps noted that service with the military "can offer incentives that aren't just financial… there's also the fun factor of doing something you can't do in civilian life." It further quotes the four-star Vice Chief of Staff, Gen. Daniel Allyn as saying: "The good news is, for our cyber professionals, they can do things in defense of our nation that [sic] would get arrested for in the outside world … That is very attractive."[21] This aspect bears consideration to reinforce recruitment efforts. There are several programs to help promote this and allow potential applicants to "try out" the job before committing to military service. One example is the university internship programs currently being run by the US Navy.[22]

An additional best practice is aptitude screening. Fortson notes a requirement to determine which aptitudes and competencies to screen for: "If the Army knows what cognitive and aptitude measures to screen for, leaders can better codify the Army's requirements for both civilian and military professionals."[23] Current Canadian Forces aptitude testing may be insufficient.

[20] *Ibid.,* 2.

[21] Freedberg, Sydney. Jr. "US Army Races To Build New Cyber Corps." Breaking Defense. Accessed March 10, 2018. https://breakingdefense.com/2016/11/us-army-races-to-build-new-cyber-corps/

[22] Matthews, William. "Military Battles to Man its Developing Cyber Force." GovTechWorks. December 01, 2015. Accessed March 10, 2018, 5. https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/#gs.ukQkiDM**.**

[23] United States. United States Army War College. *Putting the Pieces Together: Army Cyber…,* 23.

Workforce Management and Compensation

Ferrano notes that existing career management models are inhibiting the growth effort of cyber professionals, but a reserve force component is a powerful tool in generating cyber capability.[24] In an examination of cyber forces, Hannan also notes the "US and UK models of specialist reservists have influenced all manner of reserve forces across NATO … offering a potentially unique fast track to create cyber-defence forces."[25] Hannan further notes that, by recruiting direct from industry, reserve forces would have an immediate payoff in reduced training times and increased readiness: "Employing specialists who bring years or potentially decades of civilian experience to a military role (and giving them commensurate rank) pays huge dividends."[26] The CAF has an opportunity to benefit from the skills and experiences of the civilian sector not only for employment, but also for development of full-time Cyber Operators. Fortson endorses this approach, stating that "reserve component cyber experts are a tremendous resource because these soldiers already have the acquired skills [or abilities] by way of private sector employment."[27] A final benefit to reserve employment is skill retention: "Non-military employment allows them to more easily maintain currency in their cyber skills."[28]

For compensation policy, Fortson notes that the US Army has offered additional compensation incentives such as "special duty assignment pay, assignment incentive pay, and bonuses for Soldiers serving in operational assignments."[29]

[24] Ferrano, N. P. (2017). Cyber force generation. *Marine Corps Gazette*, 101(2), 52.

[25] Hannan, Noel K. "Using Reserves In Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches." *RUSI Journal* 160, no. 5 (Oct, 2015), 47.

[26] *Ibid.*

[27] United States. United States Army War College. *Putting the Pieces Together: Army Cyber…,* 4.

[28] Porche, Isaac R., I.,II, Caolionn O'Connell, Davis, John S.,II, Bradley Wilson, Chad C. Serena, Tracy G. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, and Michael Vasseur. Cyber …, xii-xiii.

[29] United States. United States Army War College. *Putting the Pieces Together: Army Cyber…,* 14.

Retention

A reserve force component positively affects retention. Mathews notes that that the use of reserve forces has helped mitigate issues retaining qualified cyber-operators, as "[a] lot of them hold positions in civilian companies that are critical to understanding our [cyber] domain." As they are already in the cyber field, "their skills and training are current, and because they already have civilian jobs, they don't represent the same kind of retention challenge as active duty troops."[30]

The US Navy has made conclusions similar to *SSE* for developing new service models. The Secretary of the US Navy advocates for more flexibility with respect to cyber personnel career management, even considering "on- and off-ramps for people" to transition between full-time service and periods employed within industry.[31] Fortson suggests that sabbaticals might be an option for cyber personnel, affording "the cybersecurity workforce the opportunity to collaborate and grow professionally within the private sector."[32]

Industry Perspective

Industry research complements military findings, although policies may be governed by different constraints than those influencing public service, giving greater latitude in recruitment and compensation policy. This section will briefly examine those practices most relevant to the CAF.

[30] Matthews, William. "Military Battles to Man its Developing Cyber Force…, 6. https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/#gs.ukQkiDM

[31] Hicks, Kathleen H., and Henry A. Kissenger. *"Discussion with the Secretaries of the U.S. Military Departments"*. Report. Center for Strategic and International Studies. Washington, DC: CSIS Headquarters, March 12, 2018, 16.

[32] United States. United States Army War College. *Putting the Pieces Together: Army Cyber…,* 28-29.

Recruitment

As cyber presence increases on operations, the CAF will require individuals with the right aptitude and propensity to learn. Regardless of whether employees are trained internally or come from industry, rapidly evolving technologies necessitate the right competencies. Industry research reflects this, outlining that "cybersecurity companies have instituted cyber aptitude or skills testing as part of the application process to evaluate a candidate's expertise."[33] With respect to best fit, research highlighted "the importance of a candidate's organizational fit and cultural behaviors, alongside technical skill requirements, as part of their selection criteria."[34] Organizational fit will be challenging to implement for the CAF, as qualitative indicators are subjective, and difficult to standardize institutionally.

Workforce Management and Compensation

If salaries are not competitive, the CAF risks losing trained Cyber Operators, representing both an opportunity and financial cost. One potential solution is offered by Libicki, Senty and Pollack who recommend that "[c]ivil service and related rules that unnecessarily prevent federal agencies from hiring talented cybersecurity professionals should be waived."[35] This factor could be addressed with specialist allowances, signing bonuses and retention bonuses for personnel to make compensation competitive with industry, similar to other specialist trades in the CAF such as Special Forces operators.

[33] Schmidt, Lara, Caolionn O Connell, Hirokazu Miyake, Akhil R. Shah, Joshua W. Baron, Geof Nieboer, Rose Jourdan, David Senty, Zev Winkelman, and Louise Taggart. *Cyber Practices: What Can the US Air Force Learn from the Commercial Sector?*. RAND Project Air Force Santa Monica CA, 2015., XV.

[34] *Ibid.,* 47.

[35] Libicki, Martin C., David Senty, and Julia Pollak. *Hackers Wanted…,* 74.

While competitive salaries were seen as important, exorbitant salaries were not a powerful retention tool. Research found that "median salaries for corporate IT and InfoSec professionals are similar to the pay and benefits for military personnel, when accounting for additional allowances and tax advantages."[36] Provided that salaries are competitive, there are other complementary retention practices.

Retention

Hiring and training cyber professionals does little good if the skill set cannot be retained, as identified within the CAF by the OAG report. Corporate practices for retaining cyber personnel involve "providing job satisfaction through good working environments, belief in the mission, opportunities for training, exposure to and engagement with professional organizations."[37]

Best practices to address the recruitment, management, and retention of cyber professionals can be summarized as follows:

- Promote the unique aspects of military service, and update policy to screen potential applicants for aptitude and organizational fit.
- Address workforce management and compensation by establishing a reserve element, and offer a competitive salary and allowances.
- Address retention by ensuring the working environment is rewarding through opportunities for engaging work, professional training and engagement across industry, as well as adopting flexible employment models to best suit the careers of cyber professionals.

[36] Schmidt, Lara, Caolionn O Connell, Hirokazu Miyake, Akhil R. Shah, Joshua W. Baron, Geof Nieboer, Rose Jourdan, David Senty, Zev Winkelman, and Louise Taggart. *Cyber* ..., XV.

[37] *Ibid*.

Policy Updates

Having identified the policy shortcomings governing the CAF contrasted with the perspectives of allied militaries and industry, this section recommends policy updates to improve the force generation of cyber operators. Table 3 outlines policy themes taken from this paper and relevant CAF and Government of Canada policies that support them. These policies are further grouped against *SSE* to reinforce their significance within Canada's current defence policy.

Table 3 – Recommended Policy Updates

Policy Areas to Address	Applicable Policies	Relevance to Defence Policy
Update Recruitment Policy • To compete with industry and recruit specialized talent into senior positions. • Aptitude screening and assessment of organizational fit. • Internship programs to "try out" Cyber Operator occupation.	• Defence Administrative Orders and Directives (DAOD) 5002-0 Military Personnel Requirements and Production, 5002-1 Enrolment, 5031-1 Canadian Forces Military Equivalencies Program, 5070-0 Military Employment Structure.	• SSE Initiative 1 – Effective recruiting. • SSE Initiative 2 – Promote unique aspects of cyber service. • SSE Initiative 88 – Develop cyber capabilities. • SSE Initiative 65 – Improve cyber capabilities.
Update Compensation and Allowances • Signing bonuses, competitive salaries, allowances, and retention bonuses.	• Compensation and Benefits Instruction. (CBI) Chapter 204 - Pay • CBI Chapter 205 – Allowances.	• SSE Initiative 79 – Align remuneration and benefits. • SSE Initiative 89 – Attract cyber talent.
Develop an Adaptable Service Model • Support transition between military and civilian employment. • Universality of Service considerations.	• DAOD 5031-0 Learning and Professional Development, DAOD 5032-0 Universality of Service. • Canadian Forces Administrative Orders (CFAO) 49-4,5 Career Policy.	• SSE Initiative 5 – Retention Strategy. • SSE Initiative 6 – Flexible career path. • SSE Initiative 78 – Adaptable service model.
Build a Reserve Force Competent • Benefit from cyber skills of civilian sector; compliments adaptable service models to retain personnel.	• Queen's Regulations and Orders (QR&Os Volume 1 Chapter 9 – Reserve Service. • DAOD 5031-1 Canadian Forces Military	• SSE Initiative 74 – Increase reserve force. • SSE Initiative 75 – Full-time capability with part-time service. • SSE Initiative 80 – Retain

	Equivalencies Programme.	cyber skills. • SSE Initiative 90 – Integrate reserve forces.

Sources: Canada. Department of National Defence. *Canadian Forces Administrative Orders.* Ottawa: Corporate Secretary. Last accessed 20 May 2018. http://corpsec.mil.ca/admfincs/subjects/cfao/intro_e.asp; Canada. Department of National Defence. *Compensation and Benefits Instructions*. Ottawa: Last accessed 20 May 2018. http://www.forces.gc.ca/en/caf-community-benefits/cbi-benefits.page;
Canada. Department of National Defence. *Defence Administrative Orders and Directives.* Ottawa: Department of National Defence. 2017. Last accessed 20 May 2018. http://intranet.mil.ca/en/defence-admin-orders-directives/index.page; Canada. Department of National Defence. *Queens' Regulations and Orders.* Ottawa: 2017. Last accessed 20 May 2018. http://www.forces.gc.ca/en/about-policies-standards-queens-regulations-orders/index.page; Canada. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy.* Ottawa: Department of National Defence, 2017; Canada. Department of National Defence. *Well-Supported, Diverse, Resilient People Chief Reserves Council*. Ottawa: Military Personnel Command, May, 2018.

Although not an exhaustive list, updating these policies will grant flexibility to CAF Cyber Command to benefit the force generation of Cyber Operators. Failure to do so will diminish efforts to grow a critical capability for the CAF and Government of Canada.

Summary

This paper has demonstrated that existing CAF and Government force generation policies used to recruit specialized capabilities for the CAF are not adequate to meet the Cyber Operator Occupation demand; new and updated policies are required.

This paper first defined the threat. As the battlefield becomes more complex, and institutional systems become increasingly digitized, so will our reliance on networked systems, increasing our vulnerabilities. This is made additionally difficult by the scarcity of highly trained professionals.

Next, institutional policy gaps were covered. A telling report from the OAG outlined deficiencies within the CAF's current recruitment and retention policies such that there is a growing capability gap across the institution. While the CAF has acknowledged these shortcomings, how can Cyber Command be successful when these same deficient policies are applied to the force generation of Cyber Operators, an emerging specialty requiring highly skilled and in-demand personnel? Considerable effort has gone into researching how to recruit and retain Cyber Operators, with best practices fielded from allied militaries and across industry.

Finally, this paper made several recommendations on which policy areas could be addressed and updates for the force generation of the Cyber Operator trade, specifically to address recruitment, workforce management, and retention policies. Leveraging best practices from allied militaries and industry, and applying policies already in place in the CAF, may enable CAF Cyber Command to generate for the Cyber Operator MOS.

In a dynamic, rapidly evolving threat environment, the CAF must generate institutional policies to be able to capably recruit and force generate the Cyber Operators it needs to fill a critical capability.

BIBLIOGRAPHY

Boo, Hyeong-wook. "An Assessment of North Korean Cyber Threats." *The Journal of East Asian Affairs* 31, no. 1 (Spring, 2017): 97-117.

Boutilier, Alex. "Canada developing arsenal of cyber-weapons." *Thestar.com*. March 16, 2017. Accessed March 10, 2018. https://www.thestar.com/news/canada/2017/03/16/canada-developing-arsenal-of-cyber-weapons.html.

Boutilier, Alex. "Canada's military seeks major cyber defence upgrade." *Thestar.com*, December 27, 2017. Accessed March 10, 2018. https://www.thestar.com/news/canada/2017/12/27/canadas-military-seeks-major-cyber-defence-upgrade.html.

Canada. Department of National Defence. A-PD-055-002/PP-002 CYBER OP MOS ID 00378, *The Canadian Armed Forces Military Employment Structure, Occupational Specifications, Non-Commissioned Member Occupations, Occupation Cyber Operator.* Part 2, Vol. 2. Ottawa: DGPR, September, 2017.

Canada. Department of National Defence. *CAF Cyber Capability – Reserve Component: Ideation & Planning Session*. Ottawa: CAF Cyber Command, December, 2017.

Canada. Department of National Defence. *Compensation and Benefits Instructions.* Last accessed 20 May 2018. http://www.forces.gc.ca/en/caf-community-benefits/cbi-benefits.page

Canada. Department of National Defence. *Canadian Forces Administrative Orders.* Ottawa: Corporate Secretary. Last accessed 20 May 2018. http://corpsec.mil.ca/admfincs/subjects/cfao/intro_e.asp

Canada. Department of National Defence. *Defence Administrative Orders and Directives.* Ottawa: Department of National Defence. 2017. Last accessed 20 May 2018. http://intranet.mil.ca/en/defence-admin-orders-directives/index.page;

Canada. Department of National Defence. *Military Employment Structure Implementation Plan (MES IP) For the CYBER OPERATOR Occupation*. Ottawa: Military Personnel Command, September, 2017.

Canada. Department of National Defence. *Queens' Regulations and Orders.* Ottawa: 2017. Last accessed 20 May 2018. http://www.forces.gc.ca/en/about-policies-standards-queens-regulations-orders/index.page

Canada. Department of National Defence. "*Reserve Compensations Benefits Allowance Comparative Matrix*." Ottawa: Director of Reserve Employer Support, 2018

Canada. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy.* Ottawa: Department of National Defence, 2017.

Canada. Department of National Defence. *Well-Supported, Diverse, Resilient People – Chief Reserves Council*. Ottawa: Military Personnel Command, May, 2018.

Canada. "Detailed Action Plan for OAG Report Recommendations." *Fall 2016 Report of the Auditor General of Canada (Tabled on 29 Nov 2016) Report 5: Canadian Armed Forces Recruitment and Retention*. Ottawa: Department of National Defence 2016.

Canada. House of Commons. *Report 5, "Canadian Armed Forces recruitment and retention - National Defence", of the Fall 2016 reports of the Auditor General of Canada: report of the Standing Committee on Public Accounts*. By Kevin Sorenson, 2016.

Canada. *Minister of National Defence Mandate Letter*. Ottawa: Office of the Prime Minister, 2015. Accessed March 10, 2018. https://pm.gc.ca/eng/minister-national-defence-mandate-letter.

Canada. Office of the Auditor General of Canada. *Report 5—Canadian Armed Forces Recruitment and Retention—National Defence*. 2016 Fall Reports of the Auditor General of Canada. Ottawa, ON: Government of Canada, 2016.

Canada. Office of the Auditor General of Canada. *Report 5—Canadian Army Reserve—National Defence*. 2016 Fall Reports of the Auditor General of Canada. Ottawa, ON: Government of Canada, 2016.

Canadian Press. "Ottawa Sets aside $1.6 Billion for outside Help with Military Challenges." Thestar.com. April 09, 2018. Accessed April 26, 2018. https://www.thestar.com/news/canada/2018/04/09/ottawa-sets-aside-16-billion-for-outside-help-with-military-challenges.html.

Cullen, Patrick J., Dr., and Erik Reichborn-Kjennerud. *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare A Multinational Capability Development Campaign project*. United Kingdom Ministry of Defence, September 2017.

"Cybersecurity and Cross-Sector Coordination: A Conversation with Keith Alexander." *The Fletcher Forum of World Affairs* 40, no. 2 (Summer, 2016): 57-62.

Dreyfuss, Joel. "The Cybersecurity Talent War You Don't Hear About." *CNBC Online*. May 13, 2015. Accessed March 10, 2018. https://www.cnbc.com/2015/05/12/the-cybersecurity-talent-war-you-dont-hear-about.html.

Farmer, Ben. "Fitness Tests Waived for MoDs New Reservist Cyber Warriors". *The Daily Telegraph*. https://www.telegraph.co.uk/news/uknews/defence/11360976/Fitness-tests-waived-for-MoDs-new-reservist-cyber-warriors.html.

Ferrano, N. P. (2017). Cyber force generation. *Marine Corps Gazette*, 101(2), 52-55.

Franz, T., Lt Col. (2011). The cyber warfare professional: Realizations for developing the next generation. *Air & Space Power Journal*, 25(2), 87-99.

Hannan, Noel K. "Using Reserves In Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches." *RUSI Journal* 160, no. 5 (Oct, 2015): 46.

Hicks, Kathleen H., and Henry A. Kissenger. *"Discussion with the Secretaries of the U.S. Military Departments"*. Report. Center for Strategic and International Studies. Washington, DC: CSIS Headquarters, March 12, 2018.

Li, Jennifer J. and Lindsay Daugherty. Training Cyber Warriors: What can be Learned from Defense Language Training?: RAND Corporation, 2015.

Libicki, Martin C., David Senty, and Julia Pollak. *Hackers Wanted: an examination of the cybersecurity labor market*. Rand Corporation, 2014.

Matthews, William. "Military Battles to Man its Developing Cyber Force." GovTechWorks. December 01, 2015. Accessed March 10, 2018. https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/#gs.ukQkiDM**.**

Oğuz, Şafak. "The New NATO: Prepared for Russian Hybrid Warfare?" *Insight Turkey* 18, no. 4 (Fall 2016): 165-80. Accessed November 26, 2017.

Porche, Isaac R., I.,II, Caolionn O'Connell, Davis, John S.,II, Bradley Wilson, Chad C. Serena, Tracy G. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, and Michael Vasseur. Cyber Power Potential of the Army's Reserve Component: RAND Corporation, 2017.

Ridout, Tim. "Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience." *The Fletcher Forum of World Affairs* 40, no. 2 (Summer, 2016): 63-83.

Schmidt, Lara, Caolionn O Connell, Hirokazu Miyake, Akhil R. Shah, Joshua W. Baron, Geof Nieboer, Rose Jourdan, David Senty, Zev Winkelman, and Louise Taggart. *Cyber Practices: What Can the US Air Force Learn from the Commercial Sector?*. RAND PROJECT AIR FORCE SANTA MONICA CA, 2015.

Schoka, Andrew . "Training Future Cyber Officers: An Analysis of the US Army ROTC?s Efforts to Produce Quality Junior Cyber Officers." *Small Wars Journal*, September 10, 2016. Accessed March 10, 2018. http://smallwarsjournal.com/jrnl/art/training-future-cyber-officers-an-analysis-of-the-us-army-rotc%E2%80%99s-efforts-to-produce-quality.

Shane, Leo . "Congress could give fitness waivers to more troops as it targets high-demand skills." *Army Times*, March 1, 2018. Accessed March 10, 2018. https://www.armytimes.com/news/pentagon-congress/2018/03/01/congress-could-give-fitness-waivers-to-more-troops-as-it-targets-high-demand-skills/.

Stavridis, J., & Weinstein, D. (2014). Time for a U.S. CYBER FORCE. United States Naval Institute. *Proceedings*, 140(1), 40-44.

Sydney J. Freedberg. Jr. "US Army Races To Build New Cyber Corps." Breaking Defense. Accessed March 10, 2018. https://breakingdefense.com/2016/11/us-army-races-to-build-new-cyber-corps/

United Kingdom. *Global strategic trends: out to 2045.* 5th ed. Swindon: Ministry of Defence, 2014.

United Kingdom. *Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities*. Swindon: Ministry of Defence, February, 2018.

United Kingdom. *Strategic Trends Programme: Future Operating Environment 2035*. 1st ed. Swindon: Ministry of Defence, November, 2014.

United States. United States Army War College. *Putting the Pieces Together: Army Cyber Warrior Talent Management.* By Calondra L. Fortson, Colonel. Washington, D.C: U.S. Army War College, 2017.