National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Major Aly Alibhai

CAF Cyber Capability is M.I.A.

JCSP 47

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 47

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 47 – PCEMI 47
2020 – 2022

Exercise Solo Flight – Exercice Solo Flight

Major Aly Alibhai

CAF Cyber Capability is M.I.A.

Table of Contents

List of Figures

CAF CYBER CAPABILITY IS M.I.A.

Introduction

Information Technology (IT) and the cyber realm have changed the world. From the way we communicate, to the way we conduct business, IT has driven the world forward from the industrial age into the networked era. As these technologies continue to evolve, so do the number of malicious cyber events sponsored by state and non-state actors to achieve their strategic aims.

The McAfee Labs 2021 Global Threat Report highlighted that the volume of threats averaged 688 per minute world wide, in the first quarter of 2021.[1] The technology and public administration sectors observed a 56% and 39% increase respectively.[2] The report also indicated that Canada observed an increase in overall malicious cyber activity during the same time period.[3]

Recognizing the threat, the Canadian Armed Forces (CAF) has committed to developing an active cyber capability. The 2017 defence policy, Strong Secure Engaged (SSE) has mandated that the CAF assume a more assertive posture by hardening defences, and by conducting active cyber operations against potential adversaries.[4] SSE also defined several focal areas which include, improvements to cryptographic capabilities, information operations capabilities, and cyber capabilities to include: cyber security and situational awareness projects, cyber threat identification and response, the development of military-specific information operations, and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations.[5]

This paper will argue that the current efforts to develop said cyber capability require significant improvement as they are insufficient to mitigate the current and emerging threats. In order to prove this assertion, this paper will examine the growing complexity of cyber threats, the current structure of the CAF capability, the recruitment, training, and development of cyber operators, and the impacts of our procurement system on delivering the necessary technologies in a timely manner. Each section will also

---

1 ***McAfee Labs, Threat Report***. McAfee Labs. Jun 2021. Pg. 11

2 Ibid, 11.

3 Ibid, 12.

4 ***Strong Secure Engaged, Canadian Defence Policy***. Government of Canada, Department of National Defence. 2017. Pg. 16

5 Ibid, 72.

provide either key planning considerations or recommendations for senior leadership to consider in the development of this essential capability.

The Growing Cyber Threat

Malicious cyber actors are often opportunistic, targeting the low-hanging fruit of networks with visible vulnerabilities and valuable assets.[6] The environment for cybersecurity has changed over the last decade, with cyber crime and espionage costing the global economy billions of dollars every year.[7] Because government agencies have data or other assets that malicious cyber actors want; they will often go to great lengths to get it.[8] Due to the sensitivity of the information governments hold and the persistence of many of those who are targeting it, government organizations don't have the luxury of operating subpar cybersecurity without putting citizens' data and potential essential services at unacceptable levels of risk.[9] Malicious actors are also aware that government security teams are increasingly asked to "do more with less" and that many agencies may face shrinking budgets and resources.[10] Federal, provincial, and local government agencies are also connected to a wide array of contractors and third-party partners that can be targeted to steal user credentials and gain access to government networks.[11] The area of greatest risk involves attacks or cyber actions whose effect is the equivalent of the use of force.[12] There have been only a handful of such actions, such as the Iranian cyber attack on Aramco.[13] Russia's use of cyber as an instrument of state power is impressive and worrying.[14] Other significant incidents, such as North Korea's hacks against Sony, the Chinese hack of the U.S.

---

6 ***Top Government Cybersecurity Threats 2022***. Richberg. Fortinet. 23 Dec 2021. Accessed 21 May 2022. Top Government Cybersecurity Threats for 2022 | CISO Collective (fortinet.com)

7 ***From Awareness to Action A Cybersecurity Agenda for the 45th President, A Report of the CSIS Cyber Policy Task Force***. Whitehouse et Al. Center for Strategic and International Studies. Jan 2017. Pg. 3

8 ***Top Government Cybersecurity Threats 2022***. Richberg. Fortinet. 23 Dec 2021. Accessed 21 May 2022. Top Government Cybersecurity Threats for 2022 | CISO Collective (fortinet.com)

9 Ibid.

10 Ibid.

11 Ibid.

12 ***From Awareness to Action A Cybersecurity Agenda for the 45th President, A Report of the CSIS Cyber Policy Task Force***. Whitehouse et Al. Center for Strategic and International Studies. Jan 2017. Pg. 3.

13 Ibid, 6.

14 Ibid, 6.

Office of Personnel Management[15], ransomware and malware attacks against the Department of National Defence and Global Affairs Canada[16], reflect a growing willingness of both state and non-state actors to use cyber tools for strategic gains.[17]

State cyber actors who target government networks are typically well organized and sophisticated.[18] Advanced persistent threat activity can now come from states, from proxy actors working on their behalf, or from criminal groups or syndicates.[19] All of these threat actors look to exploit fragmented network perimeters, siloed networking and security protocols, and aging legacy digital infrastructures.[20]

The list of methods employed by nefarious actors continues to grow in type and sophistication. The McAfee 2021 Global Threat Report summarized the attack vectors observed and detected on their systems in 2020 and the first half of 2021.

---

15 Ibid, 6.

16 ***Global Affairs Canada suffers 'cyber attack' amid Russia-Ukraine tensions***. Stephens. Global News. 24 Jan 2022. Accessed 21 May 2022. Global Affairs Canada suffers 'cyber attack' amid Russia-Ukraine tensions: sources - National | Globalnews.ca

17 ***From Awareness to Action A Cybersecurity Agenda for the 45th President, A Report of the CSIS Cyber Policy Task Force***. Whitehouse et Al. Center for Strategic and International Studies. Jan 2017. Pg. 3.

18 ***Top Government Cybersecurity Threats 2022***. Richberg. Fortinet. 23 Dec 2021. Accessed 21 May 2022. Top Government Cybersecurity Threats for 2022 | CISO Collective (fortinet.com)

19 ***Top Government Cybersecurity Threats 2022***. Richberg. Fortinet. 23 Dec 2021. Accessed 21 May 2022. Top Government Cybersecurity Threats for 2022 | CISO Collective (fortinet.com)

20 Ibid.

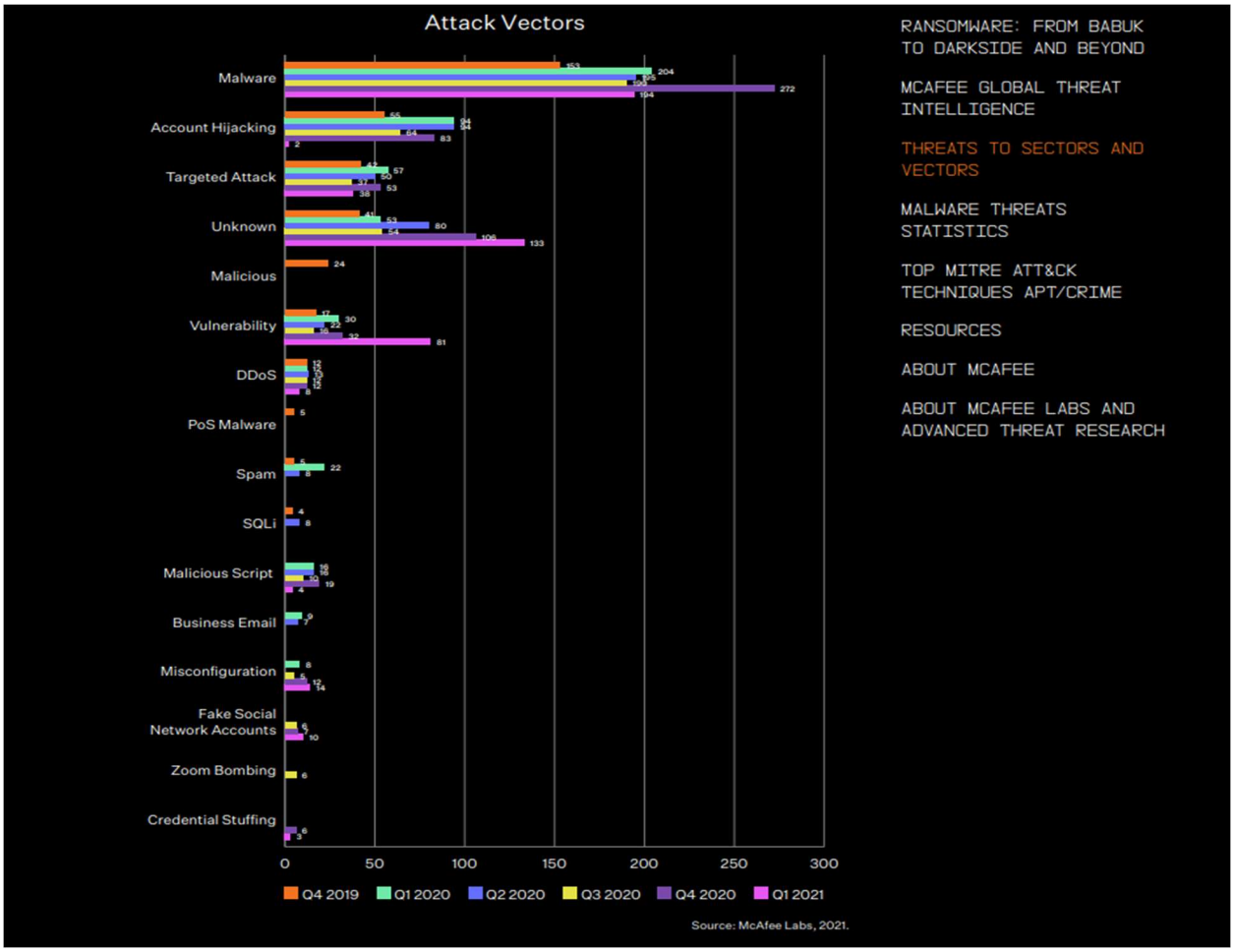

Fig 1.0 – Attack Vectors Observed by McAfee Systems

Source: McAfee Labs Threat Report Pg. 13

The graph highlights the need for organizations to possess diverse and robust capabilities. Moving forward, governments will need to pay special attention to three critical threat areas.[21] First is the digital attack surface. As agencies continue to expand their network infrastructure to accommodate work-from-anywhere, remote learning, and new cloud services, the remote environment provides ample opportunity for malicious actors to find vulnerabilities.[22] Instead of targeting only the traditional core networks of an organization, threat actors are exploiting emerging edge and "anywhere" environments

---

21 ***Top Government Cybersecurity Threats 2022***. Richberg. Fortinet. 23 Dec 2021. Accessed 21 May 2022. Top Government Cybersecurity Threats for 2022 | CISO Collective (fortinet.com)

22 Ibid.

across the extended network, including assets that may be deployed in multiple clouds with differing security policies and capabilities.[23]

Second there will be greater need to secure operational technologies (OT).[24] The convergence of IT and OT networks has enabled some attacks to compromise IT networks through OT devices and systems, and even through Internet-of-Things (IoT) devices deployed in remote users' home networks.[25]

And third, Artificial Intelligence (AI) will be a tool of choice.[26] The rise in deep fake technology will be of growing concern where AI is used to mimic human activities, and can be used to enhance social engineering attacks.[27] In the case of a phishing attack, malicious actors are not only looking to steal a user's identity and address book, but also the contents of their email inbox and outbox.[28] It is now possible to use such data to automatically generate phishing content that mirrors the writing style and syntax of a sender and tailors the content of each phishing email to topics they have already discussed.[29]

What this means for the CAF is that comprehensive capabilities to support military networks and operations, will require new and continuously upgraded technologies including but not limited to, machine learning and advanced analytics, next generation network architecture (hardware, software), advanced encryption and cryptographic methods, and robust security protocols. It will also require the recruitment, employment, and development of highly specialized and experienced personnel both military and civilian, in computer engineering, computer science, information systems and technology, and software engineering to form the foundation of any capability.[30] The subsequent sections of this paper will focus on the current developing CAF cyber capability.

---

23 Ibid.

24 Ibid.

25 Ibid.

26 Ibid.

27 Ibid.

28 Ibid.

29 Ibid.

30 ***The Cyber Security Discipline***. Canadian Center for Cyber Security, Government of Canada. 23 Jul 2020. Accessed 21 May 2022. The Cyber Security Discipline - Canadian Centre for Cyber Security

Structure and Organization

The current structure of the CAF cyber capability is limited and disorganized. SSE mandates the CAF to assume a more assertive posture by hardening defences and by conducting active operations.[31] It mandates improvements to cryptographic capabilities, information operations capabilities, cyber security and situational awareness projects, cyber threat identification and response, military-specific information operations, and offensive cyber capabilities able to target, exploit, influence, and attack in support of military operations.[32] The current mandate does not explicitly include capabilities to degrade, disrupt, manipulate, interdict, or interfere with an adversary's capabilities, networks, or infrastructure.[33] It also does not include capabilities or activities to gain access to, install, maintain, copy, distribute, search, modify, delete or intercept anything on or through the global information infrastructure.[34] These later capabilities/activities are critical components of an offensive and active cyber capability, and would form the foundation of an aggressive posture, deterrence, and strike ability. While defensive operations are considered to have the advantage in cyberspace, an organization must have a balance of defensive and offensive capabilities, and the skills and expertise needed to carry out both are nearly identical.[35] Without these specific capabilities/activities, the CAF would introduce critical vulnerabilities into its overall capability, affecting interoperability with NATO, other international partners, and other government departments (OGDs) like the Communication Security Establishment (CSE) and Canadian Security and Intelligence Service (CSIS). Therefore, it is essential the CAF adopt accepted definitions/standards of defensive, active, and offensive cyber operations, and build a complete capability that keeps pace with the emerging threats and its allies/partners.

The CAF has allocated a total of 99 positions to develop its cyber capability, 85 current positions, and 14 new cyber operator non-commissioned members (NCMs).[36] The cyber operator positions belong

---

31 ***Strong Secure Engaged, Canadian Defence Policy***. Government of Canada, Department of National Defence. 2017. Pg. 72

32 Ibid, 110.

33 ***A Deep Dive into Canada's Overhaul of Its Foreign Intelligence and Cybersecurity Laws***. Parsons and Gold. Just Security. 2 Jun 2020. Accessed 21 May 2022. A Deep Dive into Canada's Overhaul of Its Foreign Intelligence and Cybersecurity Laws (justsecurity.org)

34 Ibid.

35 ***Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance***. Yale Journal of International Affairs. 10 Jun 2020. Accessed 03 Apr 2022. Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance — Yale Journal of International Affairs

36 ***Joint Capabilities***. Government of Canada. 1 Mar 2021. Accessed 21 May 2022. Joint Capabilities - Canada.ca

to Associate Deputy Minister Information Management (ADM (IM)) which is a corporate organization and has no command authority.[37] This is an incredibly small number of personnel when you consider the overall size of the CAF, the number of operations, missions, tasks, and networks, these personnel would be required to support and monitor. It also is not nearly enough personnel to create a diverse, competent, and redundant capability, to tackle the numerous and diverse problems/threats that exist in the cyber realm. Potential remedies include, engaging trained, specialized civilian personnel to augment the current/planned positions, creating liaison positions for members of OGDs like CSIS, the CSE, or the Royal Canadian Mounted Police (RCMP) Cyber Division, to collaborate and advise on the development of our capability, and/or to create a specialized cyber regiment, similar to the British Army, to force generate, develop, manage, and employ personnel in of support operations.[38]

Another major issue with the structure is that the CAF has not created or defined readiness levels for its overall capability, or components of its capability.[39] There are disagreements as to whether cyber readiness standards need to be defined before personnel qualifications are established or vice versa, and the entire process has been characterized as "ad hoc".[40] Without defined readiness levels it would be impossible to determine, relevant technologies, services, solutions, recruitment standards, and required training for operators to build components, and the overall capability. The desired end-state and readiness levels should have been the first elements established. These standards and readiness levels already exist within industry and with OGDs. For example, for a network to be considered secure, there are minimum standards of security, both hardware and software, that must be achieved.[41] To be considered a certified cyber security analyst, there are required courses, certifications and credentials an individual must

---

[37] ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

[38] ***Army Launches First-Ever Dedicated Cyber Regiment***. Newton. Forces Net. 4 Jun 2020. Accessed 21 May 2022. Army Launches First-Ever Dedicated Cyber Regiment (forces.net)

[39] ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

[40] ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

[41] ***Compliance FAQs: Federal Information Processing Standards (FIPS)***. National Institute of Standards and Technology, US Department of Commerce. 10 Jul 2018. Accessed 21 May 2022. Compliance FAQs: Federal Information Processing Standards (FIPS) | NIST

possess.[42] It would be easy for the CAF to adopt and employ these well-established readiness levels/standards without re-inventing the wheel.

While the current structure of the CAF capability is disorganized and limited, there are solutions available, by adopting accepted definitions of capabilities, augmenting the current number of positions with civilian/OGD expertise, and adopting industry standard readiness levels, the CAF could develop a more complete capability. The next section will focus on recruitment, training and development of cyber operators.

Recruitment Training and Development of Cyber Operators

The current CAF initiatives to recruit, train and develop cyber operators are inadequate to create a comprehensive capability. Indications are that the CAF is not only behind in developing cyber capabilities but is potentially more than a decade behind its key allies.[43] Currently recruitment of cyber operators is limited to NCMs already enlisted in the CAF, and is dependent on career managers (who are not subject matter experts) to provide personnel with related skillsets on an "ad hoc" basis.[44] There is no direct entry plan for civilians who may already possess related education and experiences.[45] There is no officer trade.[46] While recruitment of trained, specialized, and experienced IT and cyber professionals is a significant challenge in today's marketplace, there are simple marketing strategies that could be employed to further attract civilians to enlist into the military. For example, the Australian Defence Force offers subsidized post secondary education in needed domains.[47] The CAF could introduce a specialized pay

---

42 ***How to Become a Cyber Security Analyst: Requirements & Job Description***. Berkley Extension, University of California at Berkely. Accessed 21 May 2022. How to Become a Cyber Security Analyst [Requirements & Job Description | Berkeley Boot Camps

43 ***Canada's Active Cyber Defence is Anything But Active***. Rudolph. Canadian Global Affairs Institute. July 2021. Accessed 21 May 2022. Canada's Active Cyber Defence is Anything But Active - Canadian Global Affairs Institute (cgai.ca)

44 ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

45 ***Cyber Operator***. Department of National Defence, Government of Canada. Accessed 21 May 2022. Cyber Operator | Canadian Armed Forces

46 ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

47 ***Enrolments open for new ADF Cyber Gap Program***. Milne. Defence Connect. 3 Apr 2020. Accessed 21 May 2022. Enrolments open for new ADF Cyber Gap Program - Defence Connect

scale similar to the special force's community, medical, dental, or legal trades, or it could simply offer signing bonuses.

The minimum requirement to enter the CAF cyber trade is a secondary high school graduation diploma, secondary 5 in Quebec, or equivalency including grade 12 applied math or grade 12/secondary 5 with computer studies, computer science or programming.[48] A quick comparison to OGDs for similar positions highlights a massive discrepancy. In a recent positing for an IT Security Analyst at CSIS, the minimum requirements include, an undergraduate degree in Computer Science, Computer, Electrical, Software, Network Engineering or Security and three years of experience, or technologist diploma equivalent professional designation and four years of experience, or a college diploma in a related field and six 6 years of experience.[49] Related experience includes three or more of the following, experience working with and securing IT infrastructure components and services (e.g. networks, storage, applications, directory services, databases, web services, cloud/virtualization services etc.), experience drafting and reviewing technical and/or standards/guidance documents, experience implementing security requirements in IT systems, experience advising, briefing or training employees at all levels, experience working with government policies on IT security, experience working with IT risk management processes, experience working with and/or supporting Security Information and Event Management systems, experience with forensic analysis of IT hardware and software, or experience with developing scripts on various systems.[50] CSIS also highlighted that having any industry certifications and/or training is a considerable asset. Certifications/courses desired include but not limited to EC-Council Certified Ethical Hacker, EC-Council Certified Security Analyst, Certified Information System Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Risk and Information Systems Control (CRISC), or Certified Information Security Manager (CISM).[51] To also compare, the Canadian Association of Defence Security Industries states in their report, The Cyber Collaboration Imperative 2020, that in the US, cyber staff have been in the domain for 20 years, and in Russia, 30 years.[52] Industry

---

48 ***Cyber Operator***. Department of National Defence, Government of Canada. Accessed 21 May 2022. Cyber Operator | Canadian Armed Forces

49 ***IT Security Analyst***. Canadian Security and Intelligence Service, Government of Canada. 17 May 2022. Accessed 21 May 2022. IT Security Analyst - Canada.ca

50 Ibid.

51 Ibid.

52 ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

experts also acknowledge that there is an expected level of cyber technical knowledge and understanding which takes years to develop in order to be functional in the domain.[53]

Once selected for the CAF cyber trade, members are sent to Willis College in Ottawa to complete a 60-week foundational cyber analyst course.[54] Members are taught knowledge and best practices for securing Windows and Linux workstations and servers, as well as software, network services, routers and switches, email and database infrastructure, and wireless devices.[55] They are also taught how to scan networks for vulnerabilities and produce reports and plans which will mitigate those vulnerabilities.[56] Upon graduation, members complete an additional 12 weeks at the Canadian Forces School of Communications and Electronics.[57] The discrepancies and gaps in competencies are obvious. One could easily argue that based on the minimum requirements, and limited foundational training provided, that current cyber operators are not adequately prepared to conduct successful defensive, active, or offensive cyber operations. Current cyber operators have indicated that the training provided is not agile enough to keep pace with the growing threats, operators experience significant skill fade as there is no continuation or specialization training, and there is no integration of industry standard courses or certifications.[58] The pace of advancement is such that a cyber professional can become substantially ineffective in as little as three months without supplemental education.[59] Skills, more than the capabilities themselves, are what

---

[53] ***The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance***. Dawson and Thompson. Frontiers in Psychology. 12 Jun 2018. Accessed 21 May 2022. Frontiers | The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance | Psychology (frontiersin.org)

[54] ***Congratulations to the First Cyber Operator Graduates from the CFSCE***. Department of National Defence, Government of Canada. 21 Sep 2021. Accessed 21 May 2022. Congratulations to the First Cyber Operator Graduates from the CFSCE - Canada.ca

[55] ***Become A Cyber Security Analyst***. Willis College. 2022. Accessed 21 May 2022. CyberSecurity Analyst Program - Willis College - Campuses In Ottawa, Winnipeg, Arnprior & Online

[56] Ibid.

[57] ***Congratulations to the First Cyber Operator Graduates from the CFSCE***. Department of National Defence, Government of Canada. 21 Sep 2021. Accessed 21 May 2022. Congratulations to the First Cyber Operator Graduates from the CFSCE - Canada.ca

[58] ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

[59] ***The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance***. Dawson and Thompson. Frontiers in Psychology. 12 Jun 2018. Accessed 21 May 2022. Frontiers | The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance | Psychology (frontiersin.org)

matter when discussing cyber.[60] Operators have also commented that the trade is poorly managed, in that there is no effective career management for the occupation, and the ad hoc employment structure does not address the challenge of ensuring that the right people receive the right training.[61]

In order to address the gaps in standards and training, the CAF should look to incorporate industry approved courses/certifications into the foundation qualifications. It should also look to develop a comprehensive continuation and specialization program. Other options include creating liaison positions for operators within leading edge IT/cyber organizations (CISCO networks, Microsoft, or Symantec) or with ODGs (CSIS, CSE, or the RCMP Cyber Division) to develop core skills, and gain valuable experience. Without urgent improvements, the operators, more than likely, will be overmatched by adversaries, and unable to contribute in a multinational, coalition, or domestic task force. The final section will focus on the limitations of the procurement system on delivering necessary technologies in a timely manner and its potential impact on the cyber capability.

Impacts of the Procurement System

It has been argued by many that the CAF has one of the worst procurement systems of any western military.[62] The system is riddled with bureaucracies, inefficiencies, and procedures that cause routine delays in delivering training, capabilities, technologies, and systems, that are desperately needed to support operations at all levels.[63] A military program/project manager may have as many as a half dozen oversight bodies and committees to report to, which adds unnecessary complexity to the process.[64] Most training/materiel purchased by the CAF are commercially available off-the-shelf (COTs) or military off-the-shelf (MOTs) systems.[65] On average the CAF system can take over a year to deliver a COTs/MOTs system, that could easily be purchased by a civilian or private industry within weeks.

---

60 ***Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance***. Yale Journal of International Affairs. 10 Jun 2020. Accessed 03 Apr 2022. Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance — Yale Journal of International Affairs

61 ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

62 ***Canada has the worst military procurement system in the Western World: Richard Shimooka in the Hill Times***. Shimooka. Macdonald Laurier Institute. 21 Jan 2019. Accessed 21 May 2022. Canada has the worst military procurement system in the Western World (macdonaldlaurier.ca)

63 Ibid.

64 Ibid.

65 Ibid.

Changes in IT and cyber technology occur rapidly, in weeks to months, and as technology changes, so do the level and complexity of threats. Most private industries and other organizations are constantly updating, improving, and patching their systems to ensure they have the latest and greatest technology/training backstopping their networks. Failure to do so, would leave their capabilities inefficient and vulnerable. Procurement in the CAF simply can not keep up with this pace.[66] Another critical limitation is the inability to conduct integral supply chain integrity checks on electronics, computers, networking equipment, and other digital equipment during the procurement process. These checks are important to ensure technologies being purchased are from reputable vendors, and do not contain inherent exploits or vulnerabilities. These requests are routinely completed by OGDs that are inundated with requests, which also results in significant delays in delivery of materiel.

There is no silver bullet to resolve the majority of these problems. However, there are a few steps/measures that could be implemented to work within the current system. First, the CAF should work with vetted industry leaders to develop "provision of service" contacts to deliver capabilities, services, and training that are a combination of existing and emerging technologies, with robust options for future upgrades and innovations.[67] Second, the CAF should redesign relevant standing offers and supply arrangements, and develop new contracting vehicles capable of responding to urgent operational requirements within a maximum 30-day time period. Third, it should develop a dedicated procurement cell to support the cyber capability/operators, staffing it with seasoned procurement officers, and specialized technical writers/systems engineers to negotiate the numerous administrative steps in the process. These steps could aid in reducing some of the delays while helping the cyber capability/operators maintain moderate pace with innovation.

Conclusion

The new cyber capability is an essential capability needed to support the CAF. The number and complexity of threats is growing, and it is a domain/weapon of choice for both state and non-state actors alike. The current efforts of the CAF are unfortunately insufficient to meet the growing threat, and to develop a comprehensive capability. There are significant issues with the current structure, recruitment, training, and overall development that will leave the institution vulnerable until they are rectified.

---

[66] ***Evaluation of the Cyber Forces***. Government of Canada. Apr 2021. Accessed 21 May 2022. Evaluation of the Cyber Forces - Canada.ca

[67] ***Bytes to Bullets, Industry's Role in Preparing Canada for the Future of Cyber Defence***. Canadian Association of Defence and Security Industries. 2019. Pg. 23.

Significant issues with the CAF procurement system will also limit/hinder its ability to procure the latest and greatest technologies/solutions in a timely manner.

There are solutions that can and should implemented to improve the overall capability development. By utilizing established industry definitions and readiness levels, by expanding recruitment options attracting qualified civilians, by including industry standard and approved courses in foundation training, liaising with industry experts and OGDs, and by supporting the capability/operators with a dedicated procurement team, theses measures may help push the current capability to the next level. The conflict in the cyber realm is only just beginning, and the CAF must utilize every resource available to develop a competent, comprehensive, and effective capability before it is too late.

Bibliography

Berkely Extension. ***How to Become a Cyber Security Analyst: Requirements & Job Description***. University of California at Berkely. Accessed 21 May 2022. How to Become a Cyber Security Analyst [Requirements & Job Description | Berkeley Boot Camps

Canadian Armed Forces. ***Cyber Operator***. 2022. Accessed 03 Apr 2022. Cyber Operator | Canadian Armed Forces

Canadian Association of Defence and Securities Industry. ***From Bullets to Bytes, Industry's Role in Preparing Canada for the Future of Cyber Defence***. 2019.

Canadian Center for Cyber Security. ***The Cyber Security Discipline***. Government of Canada. 23 Jul 2020. Accessed 21 May 2022. The Cyber Security Discipline - Canadian Centre for Cyber Security

Canadian Security and Intelligence Service. ***IT Security Analyst***. Government of Canada. 17 May 2022. Accessed 21 May 2022. IT Security Analyst - Canada.ca

Coursera. ***10 Popular Cybersecurity Certifications [2022 Updated].*** 15 Mar 2022. Accessed 03 Apr 2022. 10 Popular Cybersecurity Certifications [2022 Updated] | Coursera

Dawson and Thompson***. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance***. Frontiers in Psychology. 12 Jun 2018. Accessed 21 May 2022. Frontiers | The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance | Psychology (frontiersin.org)

Evans et Al. ***From Awareness to Action A Cybersecurity Agenda for the 45th President***. Center for Strategic Studies and International Studies. Mar 2017. Accessed 03 Apr 2022. From Awareness to Action: A Cybersecurity Agenda for the 45th President (csis-website-prod.s3.amazonaws.com)

Government of Canada. ***Canada Defence Policy, Strong Secure Engaged***. 2017.

Government of Canada. ***Congratulations to the First Cyber Operator Graduates from the CFSCE***. 21 Sep 2021. Accessed 03 Apr 2022. Congratulations to the First Cyber Operator Graduates from the CFSCE - Canada.ca

Government of Canada. ***Evaluation of Cyber Forces***. Apr 2021. Accessed 03 Apr 2022. Evaluation of the Cyber Forces - Canada.ca

Government of Canada. ***Joint Capabilities, Canadian Armed Forces***. 01 Mar 2021. Accessed 03 April 2022. Joint Capabilities - Canada.ca

Hill, J. ***The 4 levels of cybersecurity readiness***. ATT Business. 05 Oct 2017. Accessed 03 Apr 2022. The 4 Levels of Cybersecurity Readiness | AT&T Business (att.com)

Kehler et Al. ***Rules of engagement for cyberspace operations: a view from the USA***. Journal of Cybersecurity, Volume 3, Issue 1. Mar 201. Accessed 03 Apr 2022. Rules of engagement for cyberspace operations: a view from the USA | Journal of Cybersecurity | Oxford Academic (oup.com)

Liddel, A. ***A guide for understanding cybersecurity certifications***. Cybersecurity Guide. 24 Mar 2022. Accessed 03 Apr 2022. Guide to the Best Cybersecurity Certifications for 2022 (cybersecurityguide.org)

Marshall, B. ***Offensive Cyber in the Canadian Armed Forces: Opportunities from Bill C-51***. Government of Canada. 17 Feb 2022. Accessed 03 Apr 2022. Offensive Cyber in the Canadian Armed Forces: Opportunities from Bill C-51 - Canada.ca

McAfee. ***Macfee Labs Threat Report***. Jun 2021. Accessed 03 Apr. McAfee Labs Threats Report, June 2021

Milne. S. ***Enrolments open for new ADF Cyber Gap Program***. Defence Connect. 3 Apr 2020. Accessed 21 May 2022. Enrolments open for new ADF Cyber Gap Program - Defence Connect

National Institute of Standards and Technology ***Compliance FAQs: Federal Information Processing Standards (FIPS)***. US Department of Commerce. 10 Jul 2018. Accessed 21 May 2022. Compliance FAQs: Federal Information Processing Standards (FIPS) | NIST

Newton, S. ***Army Launches First-Ever Dedicated Cyber Regiment***. Forces Net. 4 Jun 2020. Accessed 03 Apr 2022. Army Launches First-Ever Dedicated Cyber Regiment (forces.net)

Nguyen, R. ***Navigating Jus Ad Bellum in the Age of Cyber Warfare***. University of California, Berkely, School of Law, California Law Review. 2013. Accessed 03 Apr 2022. Navigating Jus Ad Bellum in the Age of Cyber Warfare (californialawreview.org)

Parsons and Gold***. A Deep Dive into Canada's Overhaul of Its Foreign Intelligence and Cybersecurity Laws***. Just Security. 2 Jun 2020. Accessed 21 May 2022. A Deep Dive into Canada's Overhaul of Its Foreign Intelligence and Cybersecurity Laws (justsecurity.org)

Richberg, J***. Top Government Cybersecurity Threats 2022***. Richberg. Fortinet. 23 Dec 2021. Accessed 21 May 2022. Top Government Cybersecurity Threats for 2022 | CISO Collective (fortinet.com)

Rudolph, A. ***Canada's Active Cyber Defence is Anything But Active***. Canadian Global Affairs Institute. 21 Jul 2021. Accessed 3 Apr 2022. Canada's Active Cyber Defence is Anything But Active - Canadian Global Affairs Institute (cgai.ca)

Schimook, R. ***Canada has the worst military procurement system in the Western World***: ***Richard Shimooka in the Hill Times***. MacDonald Laurier Institute. 21 Jan 2019. Accessed 03 Apr 2022. Canada has the worst military procurement system in the Western World (macdonaldlaurier.ca)

Schmitt, M. ***Tallinn Manual on The International Law Applicable to Cyber. NATO Cooperative Cyber Defence Center of Excellence***. Cambridge University 2013. Accessed 03 Apr 2022. Manual (csef.ru)

Schwartz, D. ***What is Your Level of Cybersecurity Readiness?*** Cybersixgill. 01 Mar 2022. Accessed 03 Apr 2022. What is Your Level of Cybersecurity Readiness? | Cybersixgill

Siebring, J. ***Operationalization of cyber defence: the next steps***. Canadian Forces College. 2021. Accessed 03 Apr 2022. Operationalization of Cyber Defence: The Next Steps (forces.gc.ca)

Smythe, C. ***Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance***. Yale Journal of International Affairs. 10 Jun 2020. Accessed 03 Apr 2022. Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance — Yale Journal of International Affairs

Willis College. ***Cybersecurity Analyst***. 2022. Accessed 03 Apr 2022. CyberSecurity Analyst Program - Willis College - Campuses In Ottawa, Winnipeg, Arnprior & Online