Reviewed by ADM(RS) in accordance with the *Access to Information Act*. Information UNCLASSIFIED.

Evaluation of the Cyber Forces

DG Evaluation
Performance Measurement and Evaluation Committee
April 2021 1258-3-031 - ADM(RS)

Canada

TABLE OF CONTENTS

INTRO

Pages 3–13

- Acronyms
- Report Guide
- Executive Summary
- Evaluation Scope
- Program Profile
- Evaluation Context

01

PROGRAM IMPLEMENTATION & MANAGEMENT

Pages 14–20

- Findings 1-6
- Recommendations 1, 2 and 3

02

RESEARCH & DEVELOPMENT

Pages 21–23

- Findings 7 and 8

03

PERSONNEL GENERATION

Pages 24–28

- Findings 9-12
- Case Study
- Recommendation 4

04

CONCLUSION & ANNEXES

Pages 29–35

- Conclusions
- Management Action Plan
- GBA+ Annex
- Methodology
- Limitations

05

ACRONYMS

ADM	Assistant Deputy Minister
ADM(IE)	Assistant Deputy Minister (Infrastructure and Environment)
ADM(IM)	Assistant Deputy Minister (Information Management)
ADM(Mat)	Assistant Deputy Minister (Materiel)
ADM(RS)	Assistant Deputy Minister (Review Service)
ADM(S&T)	Assistant Deputy Minister (Science & Technology)
ARA	Accountability, Responsibility and Authority
C4I	Command, Control, Communications, Computers and Intelligence
CA	Canadian Army
CADSI	Canadian Association of Defence and Security Industries
CAF	Canadian Armed Forces
CANSOFCOM	Canadian Special Operations Force Command
C Cyber	Chief of the Cyberspace Staff
CDS	Chief of the Defence Staff
CFC	Cyber Force Commander
CFD	Chief of Force Development
CFINTCOM	Canadian Forces Intelligence Command
CFIOG	Canadian Forces Information Operations Group
CFNOC	Canadian Forces Network Operations Center
CFSCE	Canadian Forces School of Communications and Electronics
CJOC	Canadian Joint Operations Command
CMA	Cyber Mission Assurance
CMAP	Cyber Mission Assurance Program
CMP/MPGTG	Chief of Military Personnel/Military Personnel Generation Training Group
COS(IM)	Chief of Staff (Information Management)
CSE	Communication Security Establishment
DAOD	Defence Administrative Orders and Directives
D Cyber Ops FD	Director Cyber Operations Force Development
DG Cyber	Director General Cyberspace
DGICFD	Director General Information Capabilities Force Development
DGIMO	Director General Information Management Operations
DND	Department of National Defence
DRF	Departmental Results Framework
FA	Functional Authority
FP&R	Force Posture & Readiness
FY	Fiscal Year
GBA+	Gender-Based Analysis Plus
GC	Government of Canada
HR	Human Resources
IM	Information Management
IM Gp	Information Management Group
ISED	Innovation, Science and Economic Development
IT	Information Technology
JFCCC	Joint Force Cyber Component Commander
L1	Level 1
NATO	North Atlantic Treaty Organization
NORAD	North American Air Defence Command
OGD	Other Government Department
OPI	Office of Primary Interest
Ops	Operations
PT	Platform Technology
RCAF	Royal Canadian Air Force
RCN	Royal Canadian Navy
RMC	Royal Military College
SSC	Shared Services Canada
SSE	Canada's defence policy: *Strong, Secure, Engaged*
TBS	Treasury Board Secretariat
USA	United States of America
VCDS	Vice Chief of the Defence Staff

REPORT GUIDE

As a pilot for this report format within DGE, here are some guidelines for navigating the document.

This document is best viewed on a device such as a laptop, desktop or tablet, as opposed to printing.

There are links embedded which connect to other sections of the report, external documents or public sites for further investigation. **While this report contains active hyperlinks, these links will not be updated after the report's publication.**

Within the narrative, some words may be in colour. This highlights the most pertinent points for the reader, enabling him/her to more quickly read a page. In addition, colours are associated with report section themes, (e.g., program implementation or research & development).

This document, if printed, should be done so in colour to maintain the integrity and intent of the graphical components.

This icon indicates a recommendation made by ADM(RS), for which the Management Action Plans can be found in Annex A.

EXECUTIVE SUMMARY

This report presents the results of the evaluation of the Cyber Forces, conducted during Fiscal Year (FY) 2019/20 by Assistant Deputy Minster (Review Services) (ADM(RS)) in compliance with the 2016 Treasury Board *Policy on Results*. The evaluation examines the performance of the Cyber Forces over a three-year period, FY 2017/18 to 2019/20 and was conducted in accordance with the Department of National Defence (DND) and the Canadian Armed Forces (CAF).

Program Description

The Cyber Forces comprises three Programs from the Defence Program Inventory: 1.5 Cyber Operations; 2.6 Ready Cyber Forces; and 4.6 Cyber, C4I Force Development. In short, the Cyber Forces are those military and civilian personnel that force generate, force employ and force develop Cyber Operations, Network Operations and Cyber Mission Assurance (CMA).

The responsibility for the Cyber Forces is under the authority of Assistant Deputy Minister (Information Management) (ADM(IM)), through which Director General Information Management Operations (DGIMO) is lead for Programs 1.5 and 2.6 and Director General Cyberspace (DG Cyber) is the lead for Program 4.6. As military organizations, DGIMO and DG Cyber report to Chief of Staff (Information Management) (COS (IM)), who is also the Cyber Force Commander (CFC) and the Chief of Cyberspace Staff respectively.

Scope

Due to the newness of the Cyber Forces, a formative evaluation was conducted, which focused on program design, delivery and early initial outcomes.

Results

Findings were aligned according to themes of program implementation & management, research & development, and personnel generation.

Program Implementation & Management

- Accountabilities, Responsibilities and Authorities (ARA) associated with cyber are still unclear in terms of direction and responsibilities; however, this is being worked on by DGIMO and DG Cyber, and they will be further clarified by new Defence Administrative Orders and Directives (DAOD).
- Program implementation is limited by a lack of resources in personnel, funding and security-cleared materiel to undertake cyber initiatives (e.g., the Cyber Mission Assurance Program (Canada's defence policy: *Strong, Secure, Engaged* (SSE) 87)).

Research & Development

- Cyber projects have little direct influence on operations because of slow procurement processes, necessary modifications to existing projects to incorporate cyber requirements and rapid technological change.
- There is significant engagement with stakeholders in DND/CAF and Other Government Departments (OGD).

Personnel Generation

- Attracting and retaining military and civilian personnel is a challenge.
- Security clearance process timelines impacting the Cyber Forces' ability to meet its requirements ||||||||||| ||||||||||||||||||||||||||||||||||||||||||||||
- Career development is improving as cyber personnel gain access to job opportunities to advance their career.

Overall Conclusions

As a new group, DG Cyber and DGIMO have produced and are currently working on various initiatives to set in place the foundational components needed for an effective Cyber Force in the future. However, unless appropriate attention is given to the cyber domain, the rate of implementation will continue to be constrained.

- The program design theory is robust.
- The Cyber Forces need DND/CAF-wide support and investment to ensure a holistic and effective implementation of CMA and other cyber initiatives.
- Cyber stakeholders require greater strategic guidance.
- Early program developments indicate signs of progress for training of the Cyber Forces.

EXECUTIVE SUMMARY – KEY FINDINGS AND RECOMMENDATIONS

KEY FINDING	RECOMMENDATION
PROGRAM IMPLEMENTATION & MANAGEMENT	
1. Unclear ARAs, the current organizational construct of ADM(IM), and the lack of a Cyber Champion [redacted] of the Cyber Forces for the CAF and the ability to inform senior management decision making.	1. To make Cyber Forces management more effective, ADM(IM) should review, update and promulgate cyber relevant ARAs across DND/CAF to ensure their awareness.
2. There is no cyber-specific internal governance body. The cyber domain utilizes the existing ADM(IM) governance bodies of the Department, supported by Working Groups which tend to be informational. Stakeholders are responsible for developing their own cyber strategies.	2. Review the current governance framework to determine whether the cyber domain requires a distinct structure.
3. Although there are a number of strategic documents for the planning of the Cyber Forces, awareness and use are not evident across DND/CAF.	See recommendation 1.
4. Implementation of SSE 87 will [redacted] across DND/CAF.	See recommendation 1.
5. The responsibility for defining cyber readiness has not been resolved. [redacted] with the exception of the Navy which has made some progress.	**Suggestion for Follow-up:** Examine the formalization, direction and compliance of cyber readiness.
6. [redacted]	3. Create an institutionalized, centralized, serviced cyber range with classification adaptability and remote access.

EXECUTIVE SUMMARY – KEY FINDINGS AND RECOMMENDATIONS

KEY FINDING	RECOMMENDATION
RESEARCH & DEVELOPMENT	
7. [redacted]	
8. The program design has incorporated relevant knowledge from DND/CAF, OGDs and allied stakeholders; however, engagement with private industry and academia has been a challenge.	
PERSONNEL GENERATION	
9. Cyber positions are being allocated across DND/CAF [redacted]	
10. Career development opportunities for cyber personnel have been limited, although signs of positive progress are evident.	**Suggestion for Follow-up:** Examine the career progression opportunities of Cyber Operators.
	Suggestion for Follow-up: Examine the results of the Cyber Leadership study conducted by Director Cyber Operations Force Development (D Cyber Ops FD), slated to begin in March 2020, which will examine this issue [redacted]
11. Security clearances processes and timelines [redacted]	
12. As cyber training continues to be developed and formalized, the [redacted]	4. Assess the feasibility of standardizing third-party training with training validations.

EVALUATION SCOPE

Coverage and Responsibilities

The evaluation examined the following three Programs: 1.5 Cyber Operations; 2.6 Ready Cyber Forces; and 4.6 Cyber and C4I Force Development. The time period examined by the evaluation covers FY 2017/18 to FY 2019/20.

The Key Findings were aligned into three themes:

1. Program Implementation & Management
2. Research & Development
3. Personnel Generation

Photo credit: Canadian Forces Combat Camera, DND, IS2014-7532-10

A **formative evaluation** places a greater emphasis on the assessment of the design and delivery of a new program to ensure that the program is being developed and delivered in a manner that will enable it to be successful as it matures.

Due to the newness of the Cyber Forces, the evaluation was conducted as a **formative evaluation**. As a result, the evaluation examined the design and delivery of the programs as well as focused on initial immediate outcomes as opposed to intermediate or ultimate outcomes. It was too early to effectively and accurately assess the program's intermediate and ultimate outcomes. Immediate outcomes assessed included:

- Fully capable, interoperable and relevant cyber projects are available in support of CAF operators
- Units are adequately trained and staffed with personnel able to perform effectively and efficiently as dictated by the Force Posture and Readiness Plan
- Materiel is available in the required quantity, type and condition to achieve the required readiness level
- Required governance and force structures are in place to achieve readiness levels

Out of Scope

Scoping discussions with program managers indicated that the conduct of cyber operations was not mature enough to be evaluated. For this reason, they were excluded from the scope of the evaluation. Additionally, security classification limitations have resulted in Command, Control, Communications, Computers and Intelligence (C4I) content specific to force development also being excluded from the scope.

PROGRAM PROFILE

Cyberspace is critical for the conduct of modern military operations and is recognized as a domain of operations.

The onset of the Information Age has led to an evolution in the conduct of operations for DND/CAF. Although land, sea and air remain the prevailing environments of operations, increasingly, there has been a need to engage in and operationalize cyberspace. In light of the complex and rapidly evolving nature of the cyber domain, DND/CAF recognizes the need for robust cyber capabilities to ensure mission success, as recognized in SSE.

The "Cyber Forces" refer to three Programs from the Defence Program Inventory:

1.5 Cyber Operations

2.6 Ready Cyber Forces

4.6 Cyber, C4I Force Development

The Cyber Forces are those military and civilian personnel that force generate, force employ and force develop Cyber Operations, Network Operations and Cyber Mission Assurance.

The Cyber Forces fall under the responsibility of Assistant Deputy Minister (Information Management) (ADM(IM)) through Director General Information Management Operations (DGIMO), which is the lead for Programs 1.5 and 2.6, as well as Director General Cyberspace (DG Cyber), which is the lead for Program 4.6. As military organizations, DGIMO and DG Cyber report to Chief of Staff (IM) (COS(IM)), who is also the CFC and the Chief of the Cyberspace Staff, respectively. Additionally, as NDHQ entities, they report to ADM(IM) for administration.

DGIMO provides the operational foundation of the Information Management Group (IM Gp). In this role, DGIMO conducts and supports CAF operations while also providing Information Management/ Information Technology (IM/IT) support for certain departmental activities. Additionally, DGIMO is responsible for computer network and cyber defence.

DG Cyber conceives and designs CAF cyber capabilities as well as C4I capabilities to then build and implement, as well as integrate them with extant forces to conduct a full spectrum of cyber operations.

PROGRAM PROFILE

Cyber Operations

Program Objectives

Employ cyber forces to detect, deter, defend and defeat threats, adversaries or attacks against DND/CAF through the global cyber environment to achieve Canadian military objectives.

Program Activities

- Conduct defensive operations
- Conduct active operations
- Support operations

Ready Cyber Forces

Program Objectives

Prepare and sustain combat effective cyber forces that are able to respond to a spectrum of tasks, as may be directed by the Government, within the required response time.

Program Activities

- Collective training
- Individual cyber training
- Sustaining cyber materiel readiness
- Managing readiness

Cyber Force Development

Program Objectives

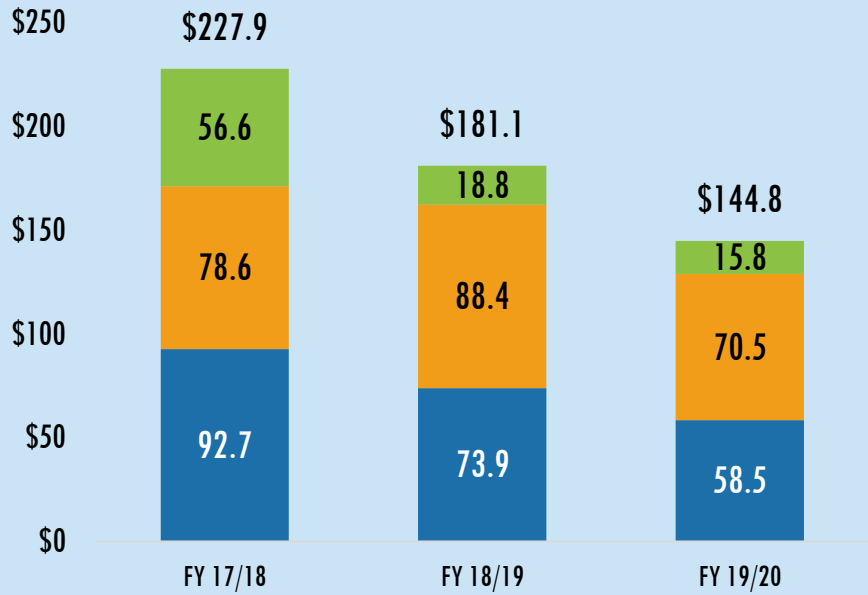
Develop and manage the execution of cyber and C4I force development activities, including the analysis, experimentation and validation of joint capabilities, enablers and force structures to be integrated and implemented into the CAF, while ensuring interoperability with domestic and international allies and partners.

Program Activities

- Strategic analysis and concept/doctrine development
- Coordination and oversight of architecture
- Research and development
- Experimentation and training development
- Force structure integration
- Identifying lessons learned
- Designing and assessing alternative capabilities
- Project development and oversight

Program Expenditures

Cyber Forces Expenditures FY 17/18- FY 19/20 ($ millions)[1]



Program expenditures for each Program only go back to FY 2017/18, as illustrated in the chart. To note, FY 2019/20 figures represent planned expenditures.

In FY 2019/20, the Cyber Forces were supported by 1309 full-time equivalents in total, with 671 for Program 1.5 (blue), 602 for Program 2.6 (orange), and 36 for Program 4.6 (green).

[1] Expenditures and Planned Spending by Program from 2014-15 to 2022-23 ($) [last accessed on Oct 23, 2020].

PROGRAM PROFILE

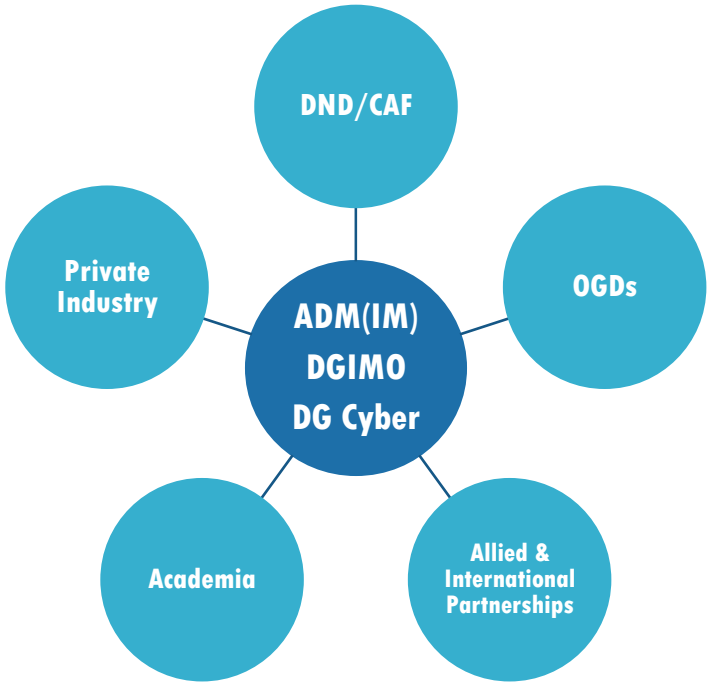
PROGRAM STAKEHOLDERS

DND/CAF: Assistant Deputy Minister (Human Resources - Civilian), Assistant Deputy Minster (Infrastructure and Environment) (ADM(IE)), Assistant Deputy Minister (Materiel) (ADM(Mat)), Assistant Deputy Minister (Policy), Assistant Deputy Minister (Public Affairs), ADM(RS), Assistant Deputy Minister (Science & Technology) (ADM(S&T)), Chief of Force Development (CFD), Chief of Military Personnel, Judge Advocate General, Strategic Joint Staff (SJS), Vice Chief of the Defence Staff (VCDS), Canadian Army (CA), Royal Canadian Air Force (RCAF), Royal Canadian Navy (RCN), Canadian Special Operations Force Command (CANSOFCOM), Canadian Forces Intelligence Command (CFINTCOM), Canadian Joint Operations Command (CJOC).

Other Government Departments (OGD): Canadian Security and Intelligence Service, Communication Security Establishment (CSE), Defence Construction Canada, Department of Finance, Innovation, Science and Economic Development, Privy Council Office, Public Safety, Public Services and Procurement Canada, Public-Private Partnerships Canada, Royal Canadian Mounted Police, Shared Services Canada (SSC), Treasury Board Secretariat (TBS).

Allied & International Partnerships: Include: CYBERCOM – United States of America (USA), National Security Agency – USA (NSA), North American Aerospace Defence Command (NORAD), North Atlantic Treaty Organization (NATO), Five Eyes Partners (USA, United Kingdom, Australia and New Zealand) .

Private Industry & Academia: There are approximately 275 firms that have been identified as related to cyber defence and cyber security in Canada, and 91 academic institutions with computer science degrees.



The Cyber Task Force was launched in 2010 and has evolved over time.

Creation of the Cyber Forces

- DG Cyber transferred to ADM(IM)
- 6 SSE Initiatives * linked to cyber (63, 65, 87, 88, 89, 90)
- Chief of the Defence Staff (CDS) Cyber Initiating Directive released
- Creation of the cyber operator trade

The Cyber Forces in DND/CAF

* Link last accessed on Oct 23, 2020.

PROGRAM PROFILE

The Cyber Mission Assurance Program

The evaluation assessed the development of the Cyber Mission Assurance Program (CMAP), which falls within the authority of the Cyber Forces. The CMAP forms a large portion of the development of the Cyber Forces and was created in response to SSE initiative 87. CMA incorporates the concepts of "cyberspace" and "mission assurance," which is the ability of an organization, service, infrastructure, platform, weapons system or equipment to operate in contested cyberspace and accomplish its mission.[2]

The CMAP is a DND/CAF-wide endeavour led by DG Cyber to create a cyber resilient defence team. It is specifically designed to address the cyberspace resilience of people, process and technology from cyber-associated threats with five lines of activities:

1. **Policy**
2. **Governance**
3. **Stakeholder Engagement & Collaboration**
4. **Education & Training**
5. **Reporting**

CMAP is working to establish a structure of centralized oversight with decentralized execution for cyber mission assurance to enable and empower Level 1s (L1) with the appropriate Accountabilities, Responsibilities and Authorities (ARA) to do their part to ensure cyber mission assurance and cyber resilience at every level of DND/CAF. In short, the concept of CMA is everyone's responsibility.

CMAP Objectives[2]

- **Enable informed, timely and effective risk-management decisions and action at both the pan-DND/CAF level and within the supporting Programs**
- **Establish standing information feeds from a diverse range of sources to inform risk-management activities**
- **Enhance collective action with allies and OGDs and agencies**
- **Improve cyberspace resilience of CAF force elements**
- **Improve cyberspace protection of DND/CAF critical infrastructure and services**
- **Enhance materiel acquisition and support (including supply chain and operational sustainment) assurance**
- **Close risk gaps within and between existing programmatic boundaries**
- **Establish standing surveillance for the development of vulnerabilities and indications that adversaries are seeking to access vulnerabilities**

"Protect critical military networks and equipment from cyber-attack by establishing a new Cyber Mission Assurance Program that will incorporate cyber security requirements in the procurement process" – SSE Initiative 87

[2] *Draft Program Charter CMAP (2020).*

EVALUATION CONTEXT

This report presents the results of the evaluation of the Cyber Forces, conducted during FY 2019/20 by ADM(RS) in compliance with the 2016 Treasury Board *Policy on Results*. The evaluation examines the performance of the Cyber Forces over a three-year period, FY 2017/18 to 2019/20 and was conducted in accordance with the DND/CAF Five-Year Departmental Evaluation Plan. The findings and recommendations in this evaluation may be used to inform management decisions related to program design, delivery and resource allocation, as well as serve as a baseline for future evaluations.

Photo credit: MCpl Simon Duchesne, VL2015-0010-003

The Cyber Force was newly created upon the establishment of the Departmental Results Framework (DRF) in 2017.

- The Cyber Forces have not been evaluated previously; however, DND/CAF was part of the *Horizontal Evaluation of Canada's Cyber Security Strategy* * *(2017)* completed by Public Safety. "The Strategy is built on three pillars: securing Government of Canada systems; partnering to secure vital cyber systems outside the Government of Canada; and helping Canadians to be secure online."[3] The Horizontal Evaluation examined:
  - The extent to which the horizontal governance structure was effective in overseeing the Strategy's implementation;
  - The extent to which participating departments and agencies implemented the Strategy's funded activities; and
  - The extent to which planned activities contributed to achieving the Strategy's main objectives.[3]

[3]Public Safety Canada
Horizontal Evaluation of Canada's Cyber Security Strategy Final Report (2017)

*Link last accessed on Oct 23, 2020

PROGRAM IMPLEMENTATION & MANAGEMENT

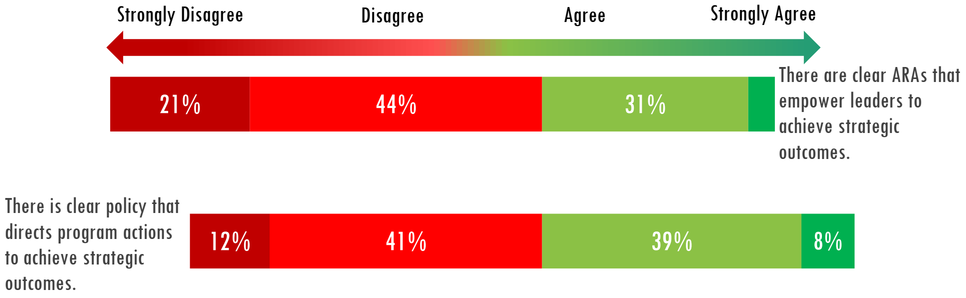
The Cyber Forces lack direction without clear ARAs and a sufficient voice to inform decision making.

FINDING 1: Unclear ARAs, the current organizational construct of ADM(IM), and the lack of a Cyber Champion [redacted] of the Cyber Forces for the CAF and the ability to inform senior management decision making.

Unclear ARAs

- The majority of program stakeholders believed that ARAs associated with cyber are still unclear in terms of direction and responsibilities.
- The concepts of Information Technology (IT), Operational Technology and Platform Technology (PT) have been used to delineate cyber Functional Authority (FA) to ADM(IM), ADM(IE) and ADM(Mat). However, in practice, stakeholders acknowledged that not all technology can easily fit into these concepts and further clarification is needed.
- DGIMO and DG Cyber have been working to further define ARAs, for example, determining responsibilities between cyber defence (Canadian Forces Network Operations Center (CFNOC)) and cyber security (Director IM Security (DIM Secur).
- Senior program management acknowledges that many ARAs concerning cyber are still unclear; however, they anticipate that new Defence Administrative Orders and Directives (DAOD) will help clarify them as the Cyber Forces mature.

Survey results indicate that senior cyber stakeholders do not believe there are clear ARAs .



The Organizational Context

- Having cyber resident within ADM(IM) has resulted in challenges for the cyber forces:
  - ADM(IM) exists outside the operational Chain of Command, and as such, does not have command authority.
  - ADM(IM), with its corporate, department-wide, proactive and long-term focus [redacted]
  - Although oversight of the CMAP is conducted within ADM(IM), the Functional Authority is held by VCDS. This has resulted in delayed approvals, according to program managers.
- Interviews with senior program managers and survey responses highlighted the important synergy between cyber and networking activities, indicating that separating them would have negative repercussions.
- Senior managers have suggested establishing a military commander within ADM(IM) with the appropriate ARAs. However, to prevent negatively impacting cyber operations, this would require additional staffing resources similar to the staffing levels of other operational commands.

PROGRAM IMPLEMENTATION & MANAGEMENT

The Cyber Forces lack direction without clear ARAs and a sufficient voice to inform decision making.

FINDING 1: (Continued)

The Lack of a Cyber Champion

- Interviews with program managers have raised concerns that there is an insufficient voice representing cyber at the senior-most levels.
  - Review of meeting minutes from the last year (2019) of the Information Management Board, the IM/IT Capability Development Board, the Programme Management Board and the Defence Capability Board revealed little to no evidence of cyber discussion at these high-level committees.
- The CFC ARAs have not been formalized, nor have they been exercised.
  - The CFC role is one of five roles of COS(IM) that is without staff support. As a result, cyber initiatives have not been able to be prioritized or raised at senior decision-making meetings.
  - Although the CFC is supposed to have a direct link to the CDS, this role is not commonly exercised, which causes delays in actioning of military cyber initiatives.
  - Interviewees have suggested that the role of the CFC is that of an advisor and not a commander, which is why they do not have the same ARAs as a commander.
  - Interviewees believe the ARAs of a full commander are required to effectively operationalize the Cyber Forces. This could be compared to the establishment of the Intelligence Commander in CFINTCOM or the Space Commander in the RCAF.

Photo credit: MCpl Patrick Blanchard, IS2014-3024-02

R1 **To make Cyber Forces management more effective, ADM(IM) should review, update and promulgate cyber relevant ARAs across DND/CAF to ensure their awareness.**

PROGRAM IMPLEMENTATION & MANAGEMENT

Cyber is currently integrated into existing governance bodies, but has none of its own.

FINDING 2: There is no cyber-specific internal governance body. The cyber domain utilizes the existing ADM(IM) governance bodies of the Department, supported by Working Groups which tend to be informational. Stakeholders are responsible for developing their own cyber strategies.

- All cyber stakeholders and program managers have acknowledged that there are no distinct cyber governance bodies.
- There are a number of Working Groups that have been effective information-sharing bodies, but there is no evidence that there are authoritative decisions being made, nor that there are associated FA that would enable such decisions.
- As part of the CMAP, all cyber stakeholders are expected to develop their own cyber strategies. The Army, Navy and Air Force are presently developing their respective strategies with no overarching CAF cyber strategy.

- Some program managers stated that cyber is already considered in a number of existing formal governance bodies and does not need a specific governance body. In this way, cyber issues are being integrated into high-level governance bodies.
- On the other hand, other program managers have argued that the Cyber Forces should have an independent governance body.
  - This would be in line with the strategic direction that the Cyber Force is a specific domain.
  - According to an interview with a senior program manager, a Cyber Force Council should meet on a regular basis.
  - An internal governance body could address concerns with cyber not being present at high-level governance bodies and a lack of strategic direction, as discussed in Finding 3.

R2 Review the current governance framework to determine whether the cyber domain requires a distinct structure.

PROGRAM IMPLEMENTATION & MANAGEMENT

There is evidence of strategic planning and insight into program development.

FINDING 3: Although there are a number of strategic documents for the planning of the Cyber Forces, awareness and use are not evident across DND/CAF.

A number of foundational documents concerning cyber, Cyber Forces development and Cyber Mission Assurance were reviewed. Some of these included the following:

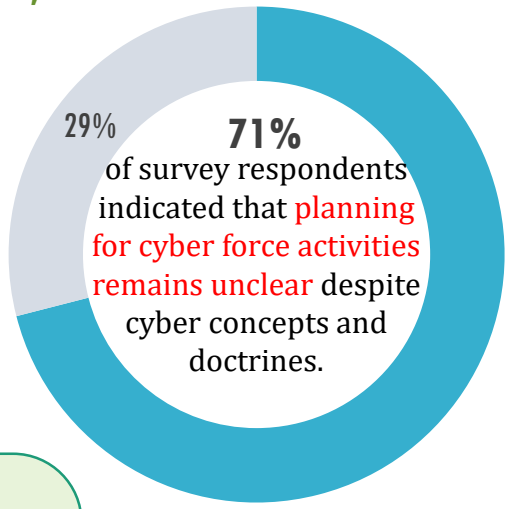
- CDS Initiating Directive (2017);
- Cyber Joint Doctrine Note (2017);
- CMAP Mandate (2018);
- Defensive Cyber Operations Concept Note (2019);
- [Draft] CMAP Charter (2019); and
- Defence Terminology Database updates.

Additionally, program managers have identified considerable work that is underway in the development of other concepts and doctrines, such as the renewal of the Joint Doctrine Note, as well as the drafting of new DAODs.

DG Cyber has produced and necessarily continues to produce multiple sources of foundational doctrines and concepts for the cyber domain…

…However, in spite of doctrines and concepts, there is still a lack of clarity.

Evidence indicates that there is still a lack of clarity regarding the cyber domain in areas that have already been established by the program managers, for example, agreed upon terminology. Interviews with program stakeholders indicated that despite the documents created, they are not well understood or promulgated across DND/CAF. This is a limiting factor for stakeholders seeking to implement and engage with cyber initiatives across the Department.



Improvement Strategies

During interviews, senior program managers agreed that there is a lack of clarity with regard to cyber. DG Cyber has plans to more thoroughly include cyber awareness and understanding into Officer and Non-Commissioned Members professional development. However, they acknowledge that developing training could take a long time.

- Additionally, increased dissemination measures could be explored to ensure that a wider audience in DND/CAF has received and is aware of these strategic documents.

R See Recommendation 1

PROGRAM IMPLEMENTATION & MANAGEMENT

Implementation of the Cyber Mission Assurance Program has been delayed.

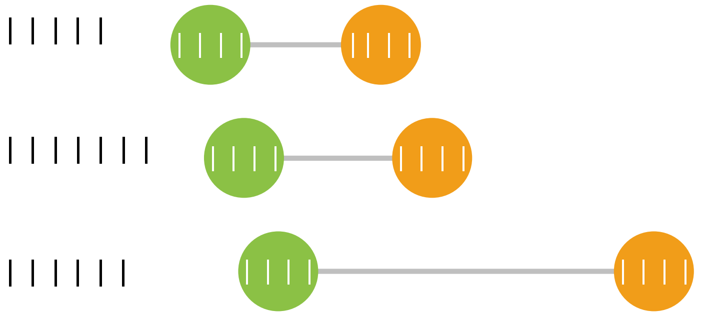
FINDING 4: Implementation of SSE 87 will [redacted] as support for Cyber Mission Assurance is not universally prioritized across DND/CAF.

"CMA requires not only the IM Group, but also the VCDS and other affected L1s to take it on board"

As mentioned previously, the CMAP is a key component of the cyber domain for all of DND/CAF. The importance of CMA was noted and acknowledged by all interviewees; however they also [redacted]

Program managers agreed with these concerns, referring to a number of challenges in the implementation of CMAP initiatives. In particular, [redacted]

The implementation of the CMAP scoping, establishment and steady-state timelines [redacted]



Personnel

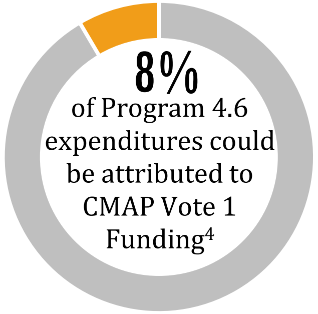
- Cyber responsibilities are often assigned to staff who have a number of other pre-established roles. As a result, CMA cannot always be a priority task to be undertaken.
- Cyber groups across DND/CAF are usually [redacted]
- [redacted]

Signs of Progress

- The recent establishment of a permanent team lead for the CMAP has led to improved progress and stability.
- Work is underway for the CMAP Charter to enable more reliable funding levels as the program is formalized.
- ADM(Mat) has played a very significant role in undertaking development and implementation activities for CMA and materiel procurement processes for supply chain resilience.

Funding

- Initial funding in FY 2018/19 was not allocated for SSE 87 (CMAP) because budgets for the program are not yet identified due to the experimental nature of the domain; however, this has made planning and implementation restrictive as limited funding is distributed (e.g., hiring contractors to conduct program development becomes difficult).
- The extent and complexity of CMAP does not reflect current levels of funding
  - During FY 2019/20, CMAP had a budget of $1,467,000 Vote 1 funds and $0 in Vote 5 funds.
  - There is little indication of budgeting or funding dedicated specifically to CMAP implementation activities by other L1s.



[4] GC Infobase [last accessed on Oct 23, 2020], [Draft] CMAP Program Charter (2020).

See Recommendation 1

PROGRAM IMPLEMENTATION & MANAGEMENT

The Cyber Forces have not identified required levels of preparedness.

FINDING 5: The responsibility for defining cyber readiness [redacted] with the exception of the Navy which has made some progress.

Suggestion for follow-up: Examine the formalization, direction and compliance of cyber readiness

- Defined cyber readiness levels are becoming increasingly important as the demand for cyber activities continues to grow, indicating future readiness challenges.
- Readiness will not work the same for cyber as for other operational domains. The terrain is constantly changing and a Cyber War concept is challenging to formally identify. Cyber preparedness may be a more descriptive terminology.
- There is disagreement among cyber managers as to whether cyber readiness standards need to be defined before personnel qualifications are established or vice versa. Currently this is very ad hoc, identified individually or as a team, and reported upwards instead of receiving top-down direction. This is discussed further in Finding 12.
- While it is important to ensure cyber components are integrated in Force Posture & Readiness (FP&R), it is too early to do this since the Cyber Forces are still in development. [redacted] as discussed in Finding 9, it was reported that the Cyber Forces [redacted]
- With respect to the responsibility for the setting of readiness standards, the strongest arguments are for the Cyber Forces to set them to ensure technical standards are established and technical connections to external organizations remain current. This is as a challenge for the IM Group to do as they were perceived by senior managers during interviews to be more focused on corporate demands versus operational.
- In the [redacted] the Navy is in the process of developing its own cyber readiness levels within three combat readiness requirements.

Photo: Corporal Braden Trudeau, Trinity - Formation Imaging Services, RP24-2019-0043-002

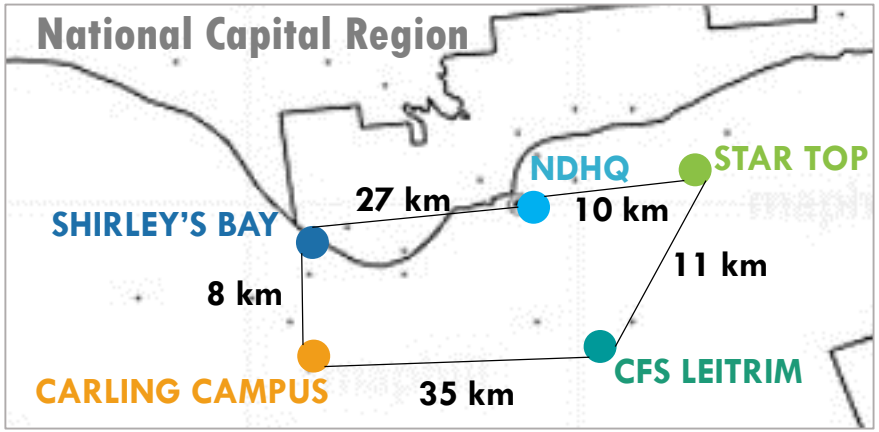
Until the force structures are in place, Cyber Readiness will continue to lack direction and formalization.

PROGRAM IMPLEMENTATION & MANAGEMENT

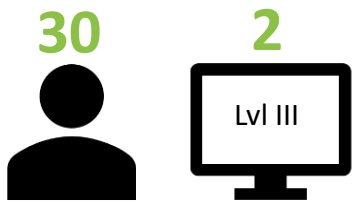
Lack of cyber-ready workspace is impeding both operations and training.

FINDING 6: [redacted]

- The draft CMA Program Charter (2020) states, "It is anticipated that suitable accommodation spaces for required staff can be found within existing DND facilities." However, no further details were given, [redacted]
- Certain personnel have to travel between five separate locations across the National Capital Region in order to access the appropriately cleared networks, as the main buildings housing cyber personnel outside of Canadian Forces Information Operations Group (CFIOG) [redacted] This can result in up to $200 in taxi fares a week for one person.
- Interviewees indicated that [redacted] Survey responses echoed this concern over physical infrastructure limitations.
- [redacted]
- While the fit-for-purpose National Defence Secure Campus may eventually be a solution, in the meantime, operations, personnel and daily activities are experiencing inordinate inefficiencies.
- At the January 2020 Defence Capability Board, the CFD indicated that "the National Defence Secure Campus is a critically important capability and it must be expedited wherever possible." The topic was discussed at the Project Management Board in March 2020.



Map courtesy of Maphill.com



- [redacted]
- Survey respondents were [redacted]
- The Cyber Collaborative Imperative by Canadian Association of Defence and Security Industries (CADSI) noted that the leading collaboration functions, policies and practices from Canada's Allies include Cyber Experimental Ranges and Capability Testing Environments. This "offers an environment where emerging solutions can be tested against known challenges…"

[redacted]

R3 Create an institutionalized, centralized, serviced cyber range with classification adaptability and remote access.

RESEARCH & DEVELOPMENT

DND/CAF Cyber projects are not sufficiently nimble to cope with changes in the threat environment.

FINDING 7:

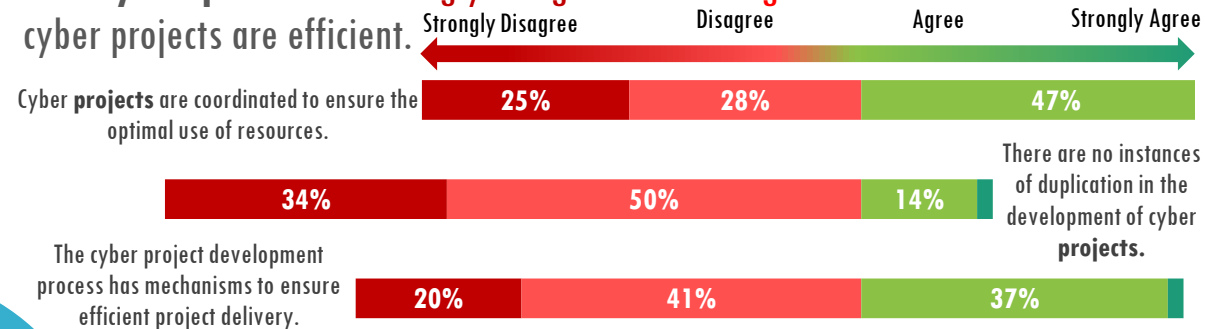
Force Generators and Force Employers[5] indicated that due to the current procurement process.

All interviewees noted the

Cyber is now part of every defence capability – there is a need to have governance bodies across DND/CAF engaged and energised. Platform CMA is tied to the capital procurement process; if this process is unclear with respect to cyber,

Many projects currently underway began before cyber requirements were considered, necessitating timely and costly amendments to include the cyber requirements.

Survey Respondents strongly disagreed and disagreed that cyber projects are efficient.



Projects that remain under $5 million can move through the procurement process more quickly and lower the threats and risks associated with changing technologies, as well as elevate the opportunity to capitalize on opportunities that technology provides.

ADM(IM) is discussing options with TBS in order to review capital project process with the goal of finding efficiencies, according to interviewees.

ADM(S&T) can inform what can be done throughout prototype development to show stakeholders the type of functionalities they should be looking for when buying off the shelf.

Implementing a funded program in order to allow the procurement of necessary tools quickly rather than project by project. The crypto program in ADM(IM) is one example of this, and CANSOFCOM is implementing capability-based procurement to address this same issue.

A properly integrated CMAP could mitigate the impact of changes in technology and the inclusion of cyber considerations.

[5]Force Generators are responsible for organizing, training and equipping forces for force employment. Ex: (CA, RCN, RCAF).
Force Employers are responsible for the command, control and sustainment of allocated forces. Ex: (CJOC, CANSOFCOM)

RESEARCH & DEVELOPMENT

The Cyber Forces are extensively engaged with numerous stakeholders.

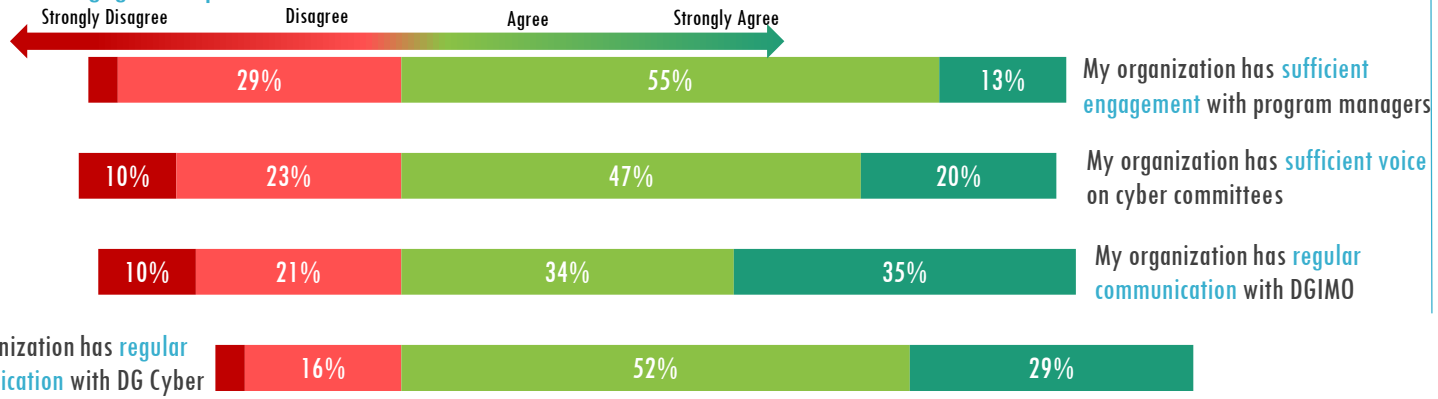
FINDING 8: The program design has incorporated relevant knowledge from DND/CAF, OGDs and allied stakeholders; however, engagement with private industry and academia has been a challenge.

DND/CAF

There is significant evidence of internal engagement and involvement from other L1 organizations and Environmental Commands:

- All of the 12 internal DND/CAF cyber stakeholder organizations who were interviewed indicated that they were engaged in the development of the Cyber Forces in their respective areas and continue to be engaged with DG Cyber through Working Groups. In particular, the Cyber Steering Committee facilitates knowledge transfer; however, it is not a governance body.
- ADM(Mat) is sufficiently engaged in talks concerning PT and leverages ADM(S&T) to integrate cyber support systems.
- ADM(S&T) identifies, tests and prioritizes cyber requirements for capabilities that cannot be bought off the shelves. It also demonstrates linkages between IT and PT for the Environmental Commands.
- ADM(IE) is engaged in talks concerning Operational Technology as they work to develop and implement cyber strategies for defence infrastructure.

Survey results indicate that a majority of DND/CAF cyber stakeholders agreed and strongly agreed that they experienced effective engagement practices.



OGDs

Overall, interviews with program managers highlighted the various relationships with OGDs. DND/CAF is present at a number of interdepartmental committees, such as the DG Cyber Strategic Committee.

- CSE was identified as a significant OGD partner with DND/CAF as the key deliverer of the Canadian Centre of Cyber Security.
  - There are promising initiatives for increased collaboration between the organizations, such as training. However, the differences in corporate cultures between CSE and DND sometimes lead to miscommunication that may hinder collaborative opportunities.
- DND/CAF is regularly engaged with Public Safety, which leads a number of Government of Canada forums on cyber.
- ADM(S&T) sits on a number of cyber research bodies, such as the one run by ISED concerning workforce in training.
- A few interviewees noted, however, that there is a need for increased clarification of ARAs with SSC.

RESEARCH & DEVELOPMENT

The Cyber Forces are extensively engaged with numerous stakeholders.

FINDING 8: (Continued)

Allies

DGIMO and DG Cyber have numerous relationships with international partners and allies, which have been a source of best practices to incorporate into the Cyber Forces. In some instances, allied relationships have been more active than OGD relationships:

- OUTCAN liaison positions act as conduits with allies for information-sharing; however, [redacted]
- Particular to the US, there are regular Cyber Coordination Committee briefings between the CAF Cyber Forces and US CYBERCOM to enable effective information-sharing and the identification of best practices.
    - The US Cyber Safe Program was identified as a model for the protection and security of information, which could be emulated.
- DND/CAF participates in US Cyber Flag group training exercises to learn and exchange strategies in the development of Cyber Force training with Five Eyes partners.
- DND/CAF is also a participant in various NATO cyber initiatives and other multinational conferences.

Private Industry

There are 275 cyber firms in Canada, of which 250 are related to cyber IT security and 25 are specific to cyber defence.[6] Industry has a lot to offer, such as innovation and agility, which may be used to further enable the Cyber Forces. The DND MINDS program brings DND and industry to the table and may be the quickest way to incorporate cyber into DND/CAF operations and activities. However, there are a number of barriers which limit increased partnerships:

- A lack of research funding, according to industry;
- DND's delayed engagement with industry due to current procurement processes;
- The lack of capacity for a permanent liaison position between DND and industry;
- Differing scopes of vision between DND and industry;
- Rules dictating departmental involvement in regard to contracts for capability development and capability procurement; and
- Overall security concerns due to:
    - Ownership and protection of Intellectual Property of DND cyber defence capabilities; and
    - Risks of firms being sold or failing.

Academia

There has been very little engagement with academia except with the Royal Military College (RMC), where engagement is robust, providing science and technology, and research and development perspectives in the cyber domain. Interviews with senior program managers identified some challenges with engaging academia:

- Inherent security risks in partnering with academia; and
- A lack of available Vote 10 grant funds to use for research.

"RMC is filling the gaps but it is not a scalable solution"

[6] *The Cyber Collaboration Imperative, CADSI (2019)* *[last accessed Oct 23, 2020]*

PERSONNEL GENERATION

The Cyber Forces have a sufficient number of positions; however, filling the positions has proved to be difficult.

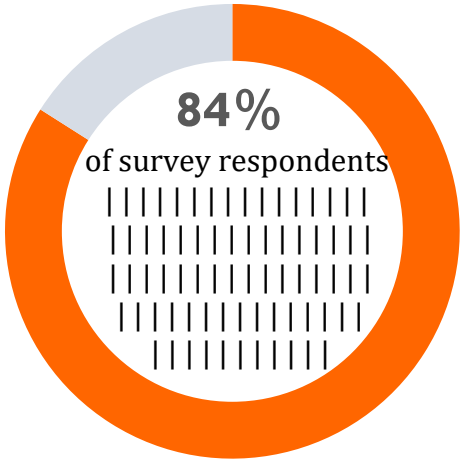
FINDING 9: Cyber positions are being allocated across DND/CAF

- Attracting and retaining cyber personnel for both military and civilian personnel was
- Additionally, by ADM(IM) corporate resource requirements.
- In a cyclical fashion, as indicated in the survey.
- Progress has recently been made in developing stronger relationships with educational institutions, by attending attraction events and using the Subsidized Training Education Plan as an opportunity to entice applicants.
- CFNOC reported that they were at at the time of the evaluation.

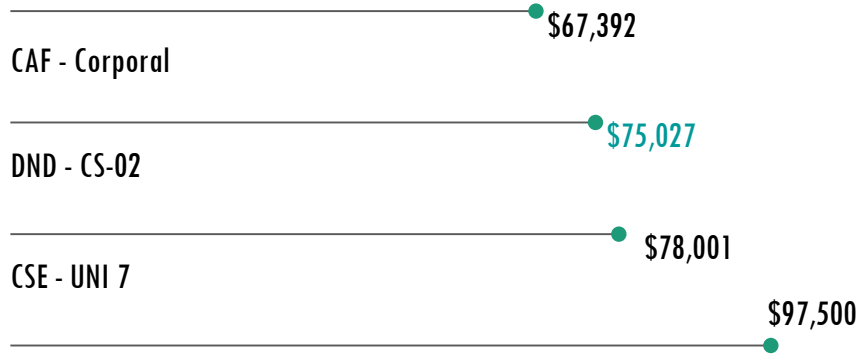
Civilian Cyber Force

- Civilian personnel are particularly challenging to attract and retain due to the competitive nature of cyber employment opportunities.
- 93 percent of survey respondents and the majority of interviewees agreed that DND/CAF would benefit from the hiring of (more) civilian cyber personnel, stabilizing the institutional memory.
- Hiring civilian cyber personnel will remain a challenge due to current financial compensation models, tied to classification, which has constrained the growth potential for technical personnel. This has also led to retention issues of military personnel once they become cyber-trained. The Computer Science (CS) classification is not thought of as adequate for cyber-related activities.
- "…[I]f you promote them to increase compensation, then by the job definition, they will not be doing the actual work you hired them to do." Interviewees also indicated that many technical personnel do not want to be in management roles.

"We're not competitive in a competitive environment."



DND/CAF is unable to be **financially competitive with respect to analysts' salaries** in the Cyber domain



[7] neuvoo.ca based on 53 salaries [last accessed on Oct 23, 2020]

A lack of cyber personnel is a risk to successful program implementation.

PERSONNEL GENERATION

Military cyber professional development has room for improvement.

FINDING 10: Career development opportunities for cyber personnel have been limited, although signs of positive progress are evident.

- A lack of planned career progression was signified as a challenge by survey respondents, potentially impacting the retention of cyber operators. Although retention concerns are largely theoretical at this point due to the small size of the occupation and newness of the Cyber Forces, retention issues from related occupations pose an extrapolated concern for the Cyber Forces.
- The Cyber Forces are reliant on career managers to provide personnel with a cyber skillset on an ad hoc basis. This poses a risk if the career managers are not aware of an interest or technical skill, or the Cyber Force grows beyond the current easily manageable small community. A Cyber Officer Occupation Study is one initiative planned to address this situation, which is further discussed in the Case Study conducted for the evaluation.
- "Skill fade" occurs rapidly in the cyber realm. Those that are posted in and out of the cyber domain quickly lose their technical expertise which takes years to develop.
- To compare, CADSI 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.
- Technical cyber personnel working in management jobs has led to demotivation and attrition. Conversely, the most experienced cyber personnel working for those who have little cyber experience is also frustrating, according to interview and survey data.
- The composition and development of the cyber workforce remains to be completed as the eventual size of the entire Cyber Force continues to evolve.
- Despite these challenges, questionnaire respondents have highlighted that career development is improving as personnel occupying cyber positions are now able to access job opportunities needed to advance their career. A CAF-wide call for interest in cyber positions was also recently posted, allowing the forces to leverage the skills of members.

"The ad hoc employment structure… does not address [the] challenge of ensuring that the right people receive the right training and are then operationally-employed in the cyber domain." – Cyber Operator Occupation Briefing

Suggestion for Follow-up: Examine the career progression opportunities of Cyber Operators.

63% of survey respondents indicated that there is no effective career management for the cyber operator occupation.

In order to keep pace with both Allies and adversaries, DND/CAF need to ensure cyber personnel remain current and employed within the cyber domain.

PERSONNEL GENERATION

Opinions remain mixed on the need for a Cyber Officer occupation.

CASE STUDY: Cyber Officer

Why: The evaluation conducted a case study of a quasi-Cyber Officer, after the topic arose during scoping interviews, to determine whether the expectations and technical requirements of a Cyber Operator warranted the possibility for a Cyber Officer position. As it is too early to make an informed opinion to this regard, the evaluation analyzed present opinions and context around a potential Cyber Officer Position.

How: The evaluation interviewed the case subject, queried survey and questionnaire respondents and discussed with interviewees.

Analysis Highlights

- The role of an officer has additional responsibilities that revolve around management as well as the strategic planning and implementation of initiatives.
- There is an expected level of cyber technical knowledge and understanding which takes years to develop, to be functional in the cyber domain.
- The case subject reported that current responsibilities of Cyber Operators, specifically on Active Cyber Operations, require higher levels of initiative and resourcefulness than those usually associated with roles of typical operators but more similar to roles typically associated with officers.
- If cyber is a domain of its own, to be fully developed as all other domains, such as land, sea and air, it was argued that a Cyber Officer should exist to enable further development of the Cyber Forces.
- Even with projected growth over the next few years, there may not be enough personnel to warrant a specific Cyber Officer role to oversee the Cyber Operator cadre, where career progression would be limited by available positions.
- A more generalized officer role has been argued by some interviewees, to ensure that they are not too focused on "cyber" and losing the big picture of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, and network operations. This pool would likely draw from the overarching Communications Electronics Engineering and Signals Officer occupations.

84% of survey respondents believe that DND/CAF would benefit from the creation of a Cyber Officer occupation. The majority of these respondents were at the tactical and operational levels.

However, the majority of interviews with senior management disagreed.

- 66 percent of interviewees thought there was no need for a Cyber Officer position.

- Regardless of the opinion on the need for a Cyber Officer opinion, 53 percent of interviewees referenced a need for better career management within the cyber domain, discussed further in Finding 10.

Suggestion for Follow-up:
Examine the results of the Cyber Leadership study conducted by D Cyber Ops FD, slated to begin in March 2020, which will examine this issue

PERSONNEL GENERATION

Delays in security clearances negatively affect the Cyber Forces.

FINDING 11: Security clearances processes and timelines

- Overwhelming evidence indicates that the security clearance process and timelines for both civilian and military members
-
- Interviewees reported that they are unable to attend necessary meetings due to security clearance requirements.
- Senior managers report being unable to recruit through certain channels such as Federal Student Work Experience Program students and co-op students, as they cannot show them the actual work they might be interested in doing due to the limitations of not having the proper security clearance requirements in place, However, interviewees reported that OGDs are able to bring in several hundred students each summer, and have them screened within a month to the Top Secret level with polygraph. This could be further investigated by the Cyber Forces.
- The issue is two-pronged – security clearances are slow, and the work needs to be accurately classified. Interviews indicated that a lot of activity is purportedly done at the Top Secret level that does not need to be, creating a self-imposed problem. Secret and unclassified work could be maximized to reduce the burden on limited security-cleared infrastructure, discussed in Finding 6.

82% of senior manager survey respondents indicated that security clearance approvals

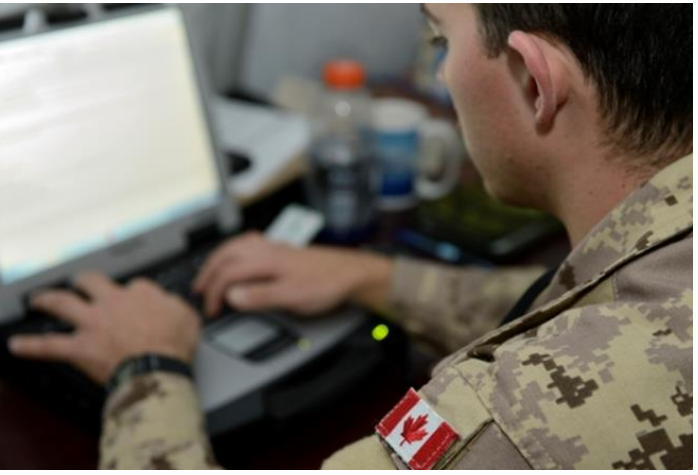
72% of survey respondents noted that security clearance approvals

PERSONNEL GENERATION

CAF training is unable to keep pace with cyber needs; however, third-party cyber training lacks standardization and validation.

FINDING 12: As cyber training continues to be developed and formalized, [redacted]

- Interviewees agreed that due to the complexity and constant evolution of the cyber domain, CAF training is not agile enough to keep pace. Third-party training is preferred by 91 percent of survey respondents but requires standardization and validation.
- One interviewee noted that "[t]he Canadian Forces School of Communication and Electronics (CFSCE) alone cannot sustain the training of cyber." This is supported by the *Cyber Operator Occupation Briefing* (2017) which noted that the Cyber Forces currently have a "Just enough just in time" training model.
- Third party training is thought to be more cost effective and may better enable the Cyber Forces to react to the rapid advancement seen in this realm.
- Comments from survey respondents further highlighted this gap in training, as respondents were concerned that the lack of standard expected skillset paired with the absence of third-party course validation poses a risk that operators may not be meeting the level of skill required.
- As discussed in Finding 9, [redacted] This presents the CAF with the alternative to choose between conducting cyber operations or providing training to the cyber force to build up necessary skill sets. Evidence shows that operations were prioritized.



Canadian Forces Combat Camera, DND, IS2014-7532-11

The draft CMA Program Charter (2020) states "It is anticipated that some specialist training will be required to develop the necessary skill sets to enable this program - the nature of which will be determined during options analysis."

In FY 2020/21, the CMAP is expected to complete a training needs analysis, formalize training and awareness framework, and issue common training guidance, all of which are reported to be on track.

Without knowing whether cyber operator training is achieving an expected standard, cyber effects may face unintended consequences.

R4 **Assess the feasibility of standardizing third-party training with training validations.**

Conclusions

As a new group, the Cyber Forces are actively engaged in numerous activities to establish Canada's position in the cyber domain of warfare. DG Cyber and DGIMO, as the leads for cyber in DND/CAF, have produced and are currently working on various initiatives to set in place the foundational components needed for an effective Cyber Force in the future. However, unless appropriate attention is given to the cyber domain, the rate of implementation will continue to be constrained.

The Cyber Forces' program design theory is robust. Extensive strategic planning and insight into the development of the Cyber Forces is apparent through the production of cyber concepts and doctrines, as well as the formalization of terminologies. Further, DG Cyber and DGIMO have maintained extensive engagement to ensure that relevant knowledge and stakeholder engagement were included in the Cyber Forces' design. Continued regular engagement with stakeholders as well as the incorporation of best practices and lessons learned will enable an effective Cyber Force.

The Cyber Forces need DND/CAF-wide support and investment to ensure a holistic and effective implementation of CMA and other cyber initiatives. DND/CAF must undergo a cultural shift to recognize the importance of CMA, as it is critical to all DND/CAF activities and operations. Pan-DND/CAF cyber initiatives cannot be implemented without the support of L1s and their respective cyber teams, and processes may need to evolve in order to effectively enable the Cyber Forces. Presently, cyber implementation activities are at risk of delays and constraints without the appropriate resources to facilitate their efforts across the Department.

Cyber stakeholders require greater strategic guidance. In spite of a robust program theory, cyber stakeholders have indicated that increased strategic direction is needed to guide their respective implementation of cyber initiatives. Instead, cyber stakeholders are acting without guidance (e.g., cyber readiness). During the evaluation period assessed, there was no overarching DND/CAF Cyber Vision.

Early program developments indicate signs of progress for training of the Cyber Forces. The creation of the Cyber Operator trade required rapid development of courseware and professional development to support the new trade. Additionally, initiatives to increase awareness and knowledge of the cyber domain among military and civilian members have been rolled out across the country.

ANNEX A—MANAGEMENT ACTION PLAN

ADM(RS) Recommendation	Management Action 1

1. To make Cyber Forces management more effective, ADM(IM) should review, update and promulgate cyber relevant ARAs across DND/CAF to ensure their awareness.	• ADM(IM) recognizes the Armed Forces Council decision of February 2018 that endorsed the ARAs for the creation of CFC, Chief of the Cyberspace Staff (C Cyber) and the Joint Force Cyber Component Commander (JFCCC). The C Cyber position was established by DM/CDS in NDHQ Organization letter in February 2018.
	• Three part action plan as follows:
	  • **1.1:** Determine the status of the Cyber Force leadership positions such as CFC, C Cyber, JFCCC, and take necessary steps to ensure that the positions are properly established;
	  • **1.2:** Upon further strategic direction, work with L1 stakeholders to determine the proper ARAs for each role (Force Management, Force Development, Force Generation, Force Employment) within the Cyber Force at the senior leadership level; and
	  • **1.3:** Promulgate ARAs using appropriate organisational instruments including DAODs, doctrine and DND policies.
	OPI: C Cyber/DGICFD
	Target Date: March 2021

ADM(RS) Recommendation	**Management Action 2**

2. Review the current governance framework to determine whether the cyber domain requires a distinct structure.	• C Cyber and Directorate General Information Capability Force Development (DGICFD), in consultation with the VCDS and other L1 Authorities will develop, evaluate and make recommendations on whether or not the cyber domain requires a distinct governance structure. The recommendations will consider:
	  • **2.1:** Matching governance mechanisms for the cyber domain with land, maritime, air and space domains in line with the CAF approach to Pan Domain Force Employment Concept;
	  • **2.2:** Ensuring that the governance of the CMAP reflects the pan-CAF/DND nature of cyber resilience in people, processes and technology leading to CAF mission success in any cyber contested domain; and
	  • **2.3:** The organizational design of governance systems to ensure they are practical and sustainable.
	OPI: C Cyber/DGICFD
	Target Date: June 2021

ANNEX A—MANAGEMENT ACTION PLAN

ADM(RS) Recommendation	Management Action 3

3. Create an institutionalized, centralized, serviced cyber range with classification versatility and remote access.	• The C Cyber and DGICFD acknowledge the concerns with the limited access to cyber ranges used for simulations and training, as well as the physical infrastructure to access them.
	• Three part action plan as follows:
	  ◦ **3.1:** Formally accept the Collaborative Security Test Environment/Interim Cyber Training Environment as the interim CAF cyber-immersive training environment;
	  ◦ **3.2:** Determine the CAF's cyber-immersive training environment requirements in coordination with all L1s; and
	  ◦ **3.3:** Determine if a capital project is required as the cyber range permanent solution.
	
	OPI: C Cyber/DGICFD
	Target Date: March 2022

ADM(RS) Recommendation
 	
4. Assess the feasibility of standardizing third-party training with training validations.
	Management Action 4
	• As C Cyber and DGICFD develop the cyber training and where third-party training is considered, it is being validated in conjunction with the Cyber Training Authority (Chief of Military Personnel/Military Personnel Generation Training Group (CMP/MPGTG)). Some existing third party training is the industry standard (certification or qualification), which does not require validation.
	• Three part action plan as follows:
	  ◦ **4.1:** In conjunction with the Cyber Training Authority, DGICFD will continue to validate third-party training. We will leverage third-party training, including allies as required where there is a training gap;
	  ◦ **4.2:** Continue working the CAF-ACE program to recognize admissible Post-Secondary Institutions; and
	  ◦ **4.3:** Continue working with the Government of Canada (GC) Cyber Skills Workforce Development Working Group that is examining holistic cyber training across the GC, utilize common areas of interest for cyber individual training and education, and, where possible, share validation and lessons learned.
	
	OPI: C Cyber/DGICFD
	OCI: CMP/MPGTG
	Target Date: Validation process ongoing / GC Cyber Skills Working Group output, July 2021

ANNEX B—GENDER-BASED ANALYSIS PLUS (GBA+)

As per the TB *Directive on Results* (2016), Mandatory Procedures for Evaluation, this evaluation took into account the government-wide policy on GBA+ as it was deemed relevant.

The Evaluation Matrix included a Key Performance Indicator dedicated to GBA+: "GBA+ considerations are included in the hiring process"

The Cyber Forces Survey that was distributed included various GBA+ questions:

- Within the Self-Identification section, for the purpose of disaggregation of data, we asked whether respondents were military, civilian or ex-military; their age; primary and secondary language; sex; gender-identity; and ethnic origins.
- The questions below were included in the Training section:

Cyber Forces Survey Questions	% Agree
The planning and implementation of the Cyber Forces takes into consideration DND/CAF diversity and inclusion initiatives.	96%
Cyber Forces policies incorporate GBA+ considerations.	85%
GBA+ considerations are included during the hiring process for cyber personnel.	87%
Gender and diversity initiatives are taken into consideration in the development of training for cyber operators.	77%

- While the survey results were positive regarding GBA+ considerations, interview responses were varied. Many voiced that there were no unique GBA+ factors incorporated during planning or hiring, and no metrics are being tracked.
- One questionnaire response noted that DG Cyber is an equal opportunity employer and will hire anyone with various identity factors as long as they meet the educational and technical qualifications and can obtain the required security clearance. That same response indicated that they are currently assessing whether access to their services have any barriers to equality for those of differing abilities.

Status of Women in Canada defines GBA+ as:
an analytical process used to assess how diverse groups of women, men and non-binary people may experience policies, programs and initiatives. The "plus" in GBA+ acknowledges that GBA goes beyond biological (sex) and socio-cultural (gender) differences. We all have multiple identity factors that intersect to make us who we are; GBA+ also considers many other identity factors, like race, ethnicity, religion, age, and mental or physical disability.

Only approximately **5 percent** of respondents to the Cyber Forces Survey identified themselves as women, and the majority of those were military members. In reflection of the CDS' initiative to increase the presence of women in the CAF, certain initiatives could be explored to align with that intent. In the Office of the CDS *Canadian Armed Forces Diversity Strategy* (2016), it states "it is imperative that the Canadian Armed Forces (CAF) reflect the society it serves if we are to connect with Canadians and retain our relevance as a national institution. … Moreover, our operational experiences have demonstrated that diversity is a force enabler that enhances our operational effectiveness." According to SSE Initiative 10, DND/CAF will fully leverage Canada's diversity by promoting diversity and inclusion as a core institutional value across the Defence team.

Of respondents to the Cyber Forces Survey, for primary language statistics, 81 percent indicated English, 18 percent listed French, with 1 percent noting Mandarin. Approximately 15 percent of the respondents indicated an ethnicity other than white, illustrating a certain level of diversity in the Cyber Forces.

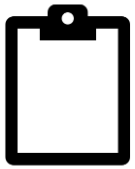
Awareness of differing identities should be actively included in all facets of the Cyber Forces to ensure an inclusive and diverse force structure.

ANNEX C—EVALUATION METHODOLOGY

Data Sources

The findings and recommendations of this report were informed by multiple lines of evidence collected throughout the conduct phase of the evaluation. These lines of evidence were triangulated with each other and verified with program managers to ensure their validity. The research methodology used in the scoping and conduct of the evaluations are as follows:

Literature Review: As part of the planning phase of the evaluation, a preliminary document review was conducted to develop a foundational understanding of the Cyber Forces and Cyber Mission Assurance to determine the scope of the evaluation. This was expanded upon during the conduct phase of the evaluation, as other documents were examined to find data that would help in the assessment. Documents included: government websites; departmental administrative reports, program documents, both in draft and finalized; and external reports.



Short-Form Questionnaire: During the conduct of the evaluation, particular issue areas were identified for further clarification and information. As a result, a number of short form questionnaires (2 – 3 questions) were sent to key points of contact through email. Organizations contacted included: DGIMO, ADM(IE), VCDS, as well as the Communications Electronics Engineering and Signals Officer career managers.

Case Study: The evaluation team conducted a case study concerning the necessity of a cyber officer trade. This study drew upon military documentation, survey data, interview notes and administrative data. Further information concerning the case study can be found in the report.

Interviews: The evaluation team conducted over 30 interviews with organizations internal and external to DND/CAF. These responses were aggregated to inform opinion and perspectives in support of the evaluation. Unless otherwise noted, reference to "senior program managers" only refers to those who are at the director level and above in DG Cyber and DGIMO. Organizations interviewed included:

- ADM(IM)
  - DG Cyber
  - DGIMO
  - CFIOG
  - Director Project Delivery Command and Control
  - DIM Secur
- ADM(S&T)
- ADM(Mat)
- SJS
- VCDS
- CA
- RCN
- RCAF
- CANSOFCOM
- CFINTCOM
- CFSCE

External to DND/CAF

- CSE
- CADSI

ANNEX C—EVALUATION METHODOLOGY

Survey:
The evaluation team conducted a survey over the month of October 2019. Certain questions were targeted for key individuals, such as senior managers, military members or cyber stakeholder organizations external to DG Cyber and DGIMO. Charts throughout the report reflect these population nuances in their titles. Unless otherwise stated, "survey respondents" refers to the entire survey population.

In order to engage a wide population for opinions, perspectives and GBA+ data, the evaluation developed a survey in English and French. Certain questions in the survey were developed for targeted members of the population, for example, senior managers, CAF members only, or responses from cyber stakeholders external to the Cyber Forces. These nuances are reflected in the charts illustrating the data throughout the report.

The survey was administered to targeted organizations and individuals who work within the cyber domain or have connections to the Cyber Mission Assurance Program across DND/CAF. Survey distribution relied on the Points of Contact identified through research of the DND Directory. These individuals would then pass the survey to other relevant individuals or subordinates in their Chain of Command.

The survey remained online for approximately one month, and had a total of 120 responses from ADM(IM), ADM(S&T), ADM(Mat), ADM(IE), JAG, SJS, VCDS, CFINTCOM, CJOC, CANSOFCOM and the Environmental Commands (CA, RCN, RCAF). To note, additional respondents from OUTCAN positions submitted surveys through Microsoft Word, as they did not have access to the DWAN.

Site Visit: The evaluation team visited CFS Leitrim and conducted five interviews with individuals working at CFIOG, this included the Commander of CFIOG. Due to limited security clearances, the team was unable to get a tour of the site, but a number of presentations and briefings by CFIOG units were given to the evaluation team.

Benchmarking: The evaluation team conducted a comparative analysis by benchmarking Canada's Cyber Force with the military cyber groups of the United States, the United Kingdom and Australia. Using various indicators, data was collected from various online sources, such as government websites, to enable comparison.

Focus Groups: The evaluation undertook a number of focus groups to capture data from targeted populations within the program areas of the population. In particular, a focus group was held with Director Information Management Engineering and Integration.

ANNEX D—EVALUATION LIMITATIONS

The limitations encountered by the evaluation, and mitigation strategies employed in the evaluation process.

Limitation	**Security Clearances** The nature of the Cyber Forces puts much of its business in the Secret and Top Secret realm.	**Survey Access** The survey that was distributed was not able to be accessed electronically by all cyber personnel, in particular those in OUTCAN postings.	**Nascent Programs** Due to the fact that the Cyber Forces are new and thus a formative evaluation was conducted, many documents were amended and updated as the evaluation progressed.	**Survey Selection Bias** Bias could arise based on the selection of the individuals or organizations chosen for the survey, which could skew survey results.	**Interview Bias** Bias could arise based on the subjective impressions and comments of interviewees, which could lead to biased views.	**Global Pandemic** Due to the outbreak of COVID-19 on a global scale and within Canada, the evaluation was unable to complete the final round of high-level stakeholder engagement.
Mitigation Strategy	The evaluation was kept at the unclassified level, scoping out areas that would not meet this criteria, specifically C4I content, as described in the Evaluation Scope.	Upon receiving information about such challenges, the evaluation team sent Microsoft Word versions of the survey and manually inputted their response data to be included in analysis.	The evaluation team kept in regular contact with program stakeholders to obtain current drafts of pertinent documentation.	All organizations that are connected to Cyber were contacted for the purposes of the survey. Respondents were selected from units from within the respective member organizations.	Interview comments were corroborated with other sources to ensure validity. Interview notes were conducted by more than one individual to confirm understanding of discussions and decrease the likelihood of bias.	Evaluation team members conducted the final phase of the project remotely.