CF Cyber Operations in the Future Cyber Environment Concept

Melanie Bernier
DRDC CORA

Joanne Treurniet
DRDC Ottawa

DRDC CORA TM 2009-058
December 2009

Defence R&D Canada
Centre for Operational Research & Analysis

Joint Staff Operational Research Team

National Defence Défense nationale

Canada

CF Cyber Operations in the Future Cyber Environment Concept

Melanie Bernier
DRDC CORA

Joanne Treurniet
DRDC Ottawa

Defence R&D Canada – CORA

Technical Memorandum
DRDC CORA TM 2009-058
December 2009

Principal Author

Original signed by Melanie Bernier

Melanie Bernier

Joint Studies Operational Research Team

Approved by

Original signed by Charles Morrisey

Charles Morrisey

A/Section Head – Joint & Common OR

Approved for release by

Original signed by Dale Reding

Dale Reding

Chief Scientist – Centre for Operational Research and Analysis

The information contained herein has been derived and determined through best practice and adherence to the highest levels of ethical, scientific and engineering investigative principles. The reported results, their interpretation, and any opinions expressed therein, remain those of the authors and do not represent, or otherwise reflect, any official opinion or position of DND or the Government of Canada.

Defence R&D Canada – Centre for Operational Research and Analysis (CORA)

Abstract

As the world becomes increasingly network-enabled, the Canadian Forces must adapt to meet the challenges that come with this technology. These include a new set of threats, and a new set of capabilities that have yet to be formally defined and explored. It is possible that the founding of an entirely new environment, the cyber environment, may be the most suitable way ahead in developing these new capabilities. This paper describes cyber operations and how they fit into the DND/CF concept construct. The capabilities provided by operations in the cyber environment and the supporting functions of cyber operations are discussed for each functional domain. Risks related to the cyber environment are listed, along with potential mitigations. The implications in terms of the PRICIE construct are discussed, and relevant activities within DND and the Government of Canada are listed. This paper may be used to advise on the future development of the cyber environment concept, and to muster appreciation of the contributions of the cyber environment to operations across all environments.

Résumé

Les technologies réseaucentriques se répandent partout dans le monde, et les Forces canadiennes doivent s'adapter pour relever les défis qui découlent de ces nouvelles technologies. Elles doivent notamment faire face à une nouvelle série de menaces, et définir et examiner une nouvelle série de capacités. Il est possible que la création d'un environnement tout à fait nouveau, le « cyber-environnement », soit le meilleur moyen de développer ces nouvelles capacités. Le présent document décrit les cyber-opérations et comment elles s'intègrent à la structure conceptuelle du MDN et des FC. Les capacités fournies par les opérations dans le cyber-environnement et les fonctions liées aux cyber-opérations sont examinées pour chaque domaine fonctionnel. Les risques associés au cyber-environnement sont énumérés, avec les mesures d'atténuation possibles. Les répercussions du cyber-environnement sur le concept PRICIE des FC sont examinées, et les activités touchées au MDN et dans le gouvernement du Canada sont énumérées. Le présent document peut être utilisé pour donner des conseils sur le développement futur du concept de cyber-environnement, et pour expliquer quelle sera la contribution du cyber-environnement aux opérations dans les trois armées.

This page intentionally left blank.

Executive summary

CF Cyber Operations in the Future Cyber Environment Concept

M. Bernier; J. Treurniet; DRDC CORA TM 2009-058; Defence R&D Canada – CORA; December 2009.

The Canadian Forces (CF) is transforming to meet the challenges of new concepts in war-fighting, as described by the Canada First Defence Strategy and the Strategic Capability Roadmap. As part of the transformation, the CF is considering expanding the traditional environments (Maritime, Land and Air) to include Space, Cyber and Cognitive environments. The focus of this work is the cyber environment.

Network technologies are becoming globally accessible. With their increased prevalence, we face a new set of threats, as well as a new set of capabilities that have yet to be formally defined and explored. This paper was written to assist in the development of the Cyber Environment concept by exploring computer network operations (CNO) in the context of military concepts and constructs. CNO has been defined as being composed of three distinct activities: computer network defence (CND), exploitation (CNE), and attack (CNA). CNO activities cannot be so easily separated, however; the blurring of the lines between these three activities is highlighted and discussed in-depth herein. We refer to the set of all potential CNO activities as *cyber operations*.

Cyber operations fit naturally into the DND/CF concept construct as a tactical/enabling concept. In joint operations, cyber operations can contribute to the other environments by providing a capability or as a supporting element. Likewise, operations in the traditional environments can support and provide capabilities to cyber operations. The capabilities provided by operations in the cyber environment and the supporting functions of cyber operations are discussed for each functional domain (command, sense, act, shield, sustain, generate).

Risks related to the cyber environment are listed, along with potential mitigations. The risks discussed include policy barriers, vulnerabilities, standards, information sharing, and cyber effects in terms of battle damage. The potential implications that the future cyber environment may have on the CF are discussed in terms of the PRICIE construct, and relevant activities within DND and the Government of Canada are listed.

This paper may be used to advise on the future development of the cyber environment concept, and to muster appreciation of the contributions of the cyber environment to operations across all environments.

Sommaire

Les cyber-opérations des FC dans le futur concept de cyber-environnement

M. Bernier; J. Treurniet; RDDC-CARO TM 2009-058; R&D pour la défense Canada – CARO; Novembre 2009.

Les Forces canadiennes (FC) sont en train de se transformer pour faire face aux défis qui découlent des nouveaux concepts d'opérations de combat, tels que décrits dans la Stratégie de défense *Le Canada d'abord* et la Feuille de route des capacités stratégiques. Dans le cadre de cette transformation, les FC songent à élargir leur champ d'action en ajoutant aux environnements traditionnels (mer, terre et air) l'espace, le cyber-environnement et l'environnement cognitif. Le présent document traite essentiellement du cyber-environnement.

Les technologies réseaucentriques deviennent de plus en plus accessibles partout dans le monde. À cause de leur prévalence, nous sommes confrontés à une nouvelle série de menaces, et nous devons définir et examiner une nouvelle série de capacités. Le présent document a pour but de faciliter le développement du concept de cyber-environnement en examinant les opérations de réseau informatique (ORI) dans le contexte des concepts militaires. Par définition, les ORI comportent trois activités distinctes : défense des réseaux informatiques (CND), exploitation de réseau informatique (CNE), et attaque contre les réseaux informatiques (CNA). Ces activités ne peuvent pas être séparées aussi aisément, cependant. Le présent document souligne que les lignes sont floues entre ces trois activités, et il les examine en détail. Ces activités sont désignées sous le nom de *cyber-opérations*.

Les cyber-opérations s'intègrent naturellement à la structure conceptuelle du MDN et des FC, en tant que concept tactique/habilitant. Dans les opérations interarmées, les cyber-opérations peuvent appuyer les autres armées en leur fournissant une capacité ou un élément de soutien. De la même façon, les opérations dans les environnements traditionnels peuvent appuyer les cyber-opérations et leur fournir des capacités. Les capacités fournies par les opérations dans le cyber-environnement et les fonctions liées aux cyber-opérations sont examinées pour chaque domaine fonctionnel (commandement, détection, action, protection, maintien en puissance, mise sur pied de capacités).

Les risques associés au cyber-environnement sont énumérés, avec les mesures d'atténuation possibles. Parmi les risques examinés, il y a les obstacles politiques, les vulnérabilités, les normes, le partage de l'information, et les cyber-effets en termes de dommages de combat. Les répercussions possibles du futur cyber-environnement sur le concept PRICIE des FC sont examinées, et les activités touchées au MDN et dans le gouvernement du Canada sont énumérées.

Le présent document peut être utilisé pour donner des conseils sur le développement futur du concept de cyber-environnement, et pour expliquer quelle sera la contribution du cyber-environnement aux opérations dans les trois armées.

Table of contents

List of figures

List of tables

Acknowledgements

For comments on v1.0 and consultations, the authors are indebted to: LCol K. Schramm, LCol M. Drapeau, LCol A. Boucher, LCol M. Purcell, LCdr D. Harnett, LCol W. Yee, S. Leblanc, LCol F. Castonguay, LCol J. Blythe, M. Froh, L. Beaudoin, R. Heide and the CFD/DFSA/ICDT-2 team.

This page intentionally left blank.

1 Introduction

Malicious cyber activities are growing both in number and in complexity [2]. Symantec reports annual increases in new threats; the number of new threats in 2008 has increased to 80 times the number detected in 2002 [2]. The Future Security Environment [3] predicts that cyber attacks will continue to be a significant threat, and some sources predict that cyber warfare (i.e. cyber operations undertaken by nation-states as an act of force for political gain) is imminent if not ongoing, e.g. [4][10]. The DND/CF has integrated information technology into all aspects of it business, from client/server applications to communications via the Internet. The SCRv1.0 [5] states that by 2028 technologies currently in their infancy will become fundamental to our future capabilities. These technologies include: networked devices that are small, light, inexpensive, and highly energy efficient; autonomous networks; ubiquitous networks; and permanent, mobile connection to the future Internet. As we head toward a more network-enabled force, maintaining freedom of actions within the cyber environment will be essential for all phases of CF operations and consequently cyber operations will have an even greater contribution to all CF operations.

The combination of our increasing current and future reliance on these technologies and the growth of the threats to them reinforces the importance of operations in the cyber environment. This is recognized in the Canada First Defence Strategy [1]:

> *In such a complex and unpredictable security environment, Canada needs a modern, well-trained and well-equipped military with the core capabilities and flexibility required to successfully address both conventional and asymmetric threats, including terrorism, insurgencies and cyber attacks.*

Consequently, the Canadian Forces (CF) needs to be prepared to transition into cyber warfare, adapting its concepts, technology, doctrine and organization to optimize the exploitation of cyberspace and enable cyber warfare. This process must begin with establishing a common vision for cyber operations throughout DND and the CF.

The cyber threat is gaining recognition government-wide and the CF needs to prepare for full-spectrum cyber operations for its role in defending Canada against the cyber threat. Although it now appears that there is a wider military recognition of the need for cyber operations, it is apparent that there is still confusion surrounding how the military intends to integrate this concept. The CF is exploring the avenue of expanding the traditional environments (Maritime, Land and Air) to include Space, Cyber and Cognitive [6][7]. The need to command, act, shield, sense, sustain and generate in these areas in order to realise desired outcomes is essential for success in these complex battlespaces.

1.1 Purpose and Scope

The purpose of this document is to describe how the CF might employ the ability to operate in the cyber environment in future operations. The intended audience for this document is the Director General Capability Development, who is responsible for producing the Strategic Capability Roadmap, and the Capability Domain managers, who are responsible for assessing capability options and developing capability goals that will shape the future force structure of the CF. It will also be relevant to other operational environments in that it highlights the joint aspects of

cyber operations, i.e. how they support cyber operations, and how cyber operations can support their operations.

The intended uses of this paper are:

- To inform the continued development of the strategic capability roadmap;
- To provide context for the development of the institutional, operating and enabling concepts;
- To provide context for ongoing scenario development and analysis; and
- To provide guidance for follow-on concept development and experimentation.

The scope of this paper is guided by the vision of the Government of Canada as described in the Canada First Defence Strategy [1] as well as the Chief of Force Development (CFD) in the Strategic Capability Roadmap Version 1.0 (SCRv1.0) [5]. The pertinent aspects of these strategies are as follows:

- A change of focus from state-on-state conflict to the asymmetric threat of non-state actors (including terrorist organizations and organized crime);
- Focused and integrated effects in a comprehensive approach to operations, including armed forces, other government departments (OGDs) and agencies, non-governmental organizations (NGOs), and allies; and
- Seamless information and knowledge sharing enabled by a networked environment.

Based on the above, future CF cyber operations must have a strategic focus on operations that are effects-based, comprehensive and network-enabled. This paper will discuss the cyber environment and the concept of cyber operations in terms of computer network operations (CNO). It will discuss the types of operations that take place in the cyber environment, and the interdependencies between the cyber environment and the traditional environments. It will then discuss the role of cyber operations in each of the six functional domains (command, act, shield, sense, sustain and generate), in terms of supporting operations in other environments, and in terms of delivering an operational capability unto itself.

Further, this paper will discuss some of the risks in implementing cyber operations and how they might be mitigated, and list some activities supporting cyber operations that are ongoing in DND and the Government of Canada.

1.2 Types of Operations

Cyber operations can provide capabilities in the full spectrum of possible military operations, from support to the civil authority and search and rescue, to peace support operations up to and including warfighting. Given the enduring nature of the mandate of the Canadian Forces, the fundamental types of military operations that could be expected to take place in the future include:

- Domestic Operations (Defend Canada);
- Continental Operations (Defend North America); and

- International Operations (Contribute to International Security)

Interoperability is an issue for all operations, however the problem space varies. While in an international operation interoperability must be addressed among nations, in domestic operations interoperability must exist between government departments, NGOs and agencies.

The main targets of interest in Canada and around the world are the public and private critical infrastructures. Public Safety Canada lists these as being Energy and Utilities; Information and Communications Technology; Finance; Health; Food; Water; Transportation; Safety; Government; and Manufacturing [11]. These are attractive targets because they consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments and businesses in Canada.

Domestically, one of the ten Canadian critical infrastructure sectors is the Information and Communications Technology sector [11], which has a high degree of interdependence with the other sectors. The increased reliance on information and communication technology stresses the importance of protecting our critical infrastructures.

1.3 Critical Assumptions

Critical assumptions upon which this report is dependent:

- Canadian government policy will not change the fundamental roles of the CF.
- Canada will mostly likely continue to operate as part of a coalition or in a multi-national context, except in domestic operations.
- Canada will remain in good standing with its present allies in the developed world.
- The Comprehensive Approach and Network Enabled Operations concepts will endure to become CF doctrine.[1]
- DND/CF will maintain an internal capability and capacity to follow, apply and rapidly exploit science and technology (S&T) advances, knowledge and information in order to ensure optimized capability that address critical mission outcomes.

[1] See Section 3 for definitions of these concepts.

2 The Current Cyber Environment

There is no approved definition of the Cyber environment, or Cyberspace, for the DND/CF. Under consideration is the US Department of Defence definition of "a global domain within the information environment consisting of interdependent network information technology infrastructures, including the Internet, telecommunication networks, computer systems and embedded processors and controllers."[30] This definition, however, lacks consideration for the software and information that reside on the network: these are targets in a cyber attack and should be included in the environment.

2.1 Cyber Threats

Computer/Cyber attacks have been around since the late 1980's where computer viruses were more of a game, something kids did for fun [8]. The first PC-based virus was introduced in 1986 and was called "©Brain" [9]. These types of viruses were distributed manually using diskettes until 1999 when the first email virus/worm appeared, called "Happy99" [9]. It used the email address book to send itself to other addressees and then in early 2000 computer viruses/worms used IP addresses to travel from one host to another. Cyber attacks continued to evolve where viruses were then used by organizations or individuals for criminal activities such as credit card fraud and other methods of financial gain [8]. Today, cyber attacks are increasingly used as a political protest in times of war/conflict or even as an act of war [10]. Cyber attacks are a daily occurrence [2] and cyber espionage is becoming more and more a reality [22].

As defined in [12], cyber threats are any Internet-borne activity that may harm or have potential to harm a computer or network and compromise the confidentiality, integrity or availability of network data or systems. This is not unique to DND/CF. A compromise in confidentiality is information leakage, e.g. the unauthorized access of classified information. A compromise in integrity is an intentionally incorrect or unapproved change to data, e.g. the vandalism of web sites. A compromise in availability is the destruction or degradation of data or a system, or disruption of the mechanism to retrieve data. Availability can be compromised via software vulnerabilities or through physical means [13].

A typical scenario to compromise confidentiality or integrity may include the following steps:

1. Reconnaissance;

2. Exploit vulnerability to obtain system access at higher privilege; repeat as necessary;

3. Obtain/modify information.

The reconnaissance stage can be carried out actively or passively. Actively, a scanner is used to send probes to the target to build a network map based on the responses to the probes. Passively, a line is tapped to collect all data exiting the target network and a network map is inferred. War-driving can be used to passively detect wireless access points. Both can be accomplished without detection. When the reconnaissance identifies vulnerable software, an exploit is launched to escalate privilege levels. From there, the attacker can penetrate further into the network until the

location of the information is reached and can be read and modified. At any point, a "backdoor" may be inserted to allow easy access in the future. The process is somewhat different if carried out by an insider. An insider already knows the network's configuration and safeguards, and will likely not require a reconnaissance phase.

A compromise in availability can be destruction of data, which may follow the above process, or it can affect the availability of a service by degrading or denying the service to users. Availability may be affected by:

- Denial of service (DoS): A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computer with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet [14].
- Distributed DoS (DDoS): A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target [14]. A DDoS makes use of a "botnet", a collection of compromised hosts scattered throughout the Internet that act as slaves. Often these are unwitting insecure home computers.
- Electromagnetic disturbances.
- Physical destruction of hardware.

The following is a list of known threat agents/actors in the cyber environment:

- Criminal Groups (e.g. organized crime organizations and international corporate spies): These groups have the ability to conduct industrial espionage and large-scale monetary theft as well as the ability to hire or develop hacker talent [14].
- Hackers: These groups or individuals crack into networks usually for the thrill or challenge as well as for bragging rights within the hacker community [14].
- Hacktivists: These groups or individuals are politically motivated and attack publicly accessible web pages and e-mail servers. They overload e-mail servers and hack into web sites to send political messages [14].
- Insiders: The insider threat includes disgruntled or disloyal employees and is of concern due to their knowledge of and access to the target systems [14].
- National Governments and Foreign Intelligence Services: Also known as the "State" threat, these are official actions sanctioned by other countries' governments. Some countries are developing cyber-war capabilities [14][16].
- Terrorist Groups: These groups aim to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence [14].

The following are recent examples of cyber attacks and cyber exploitation:

- Hezbollah–Israeli conflict: In 2006 during the Hezbollah-Israeli conflict, parties on both side used cyber technologies to their advantage. Cyber psychological operations that aim to

directly attack and influence the attitudes and behaviours of soldiers and the general population were used [17]. Lebanese newspapers reported that the major television and radio stations had been compromised and were used to broadcast messages that Hezbollah's leader was a liar. Computers compromised in Europe and Russia had been used to send anti-Semitic and anti-Arabic hate mail. Israeli-based denial of service attacks against Hamas and Hezbollah websites had effectively crippled portions of the Internet infrastructure on both sides of the conflict [18].

- Denial of Service events in Estonia: In April 2007, Estonia experienced distributed denial-of-service attacks which targeted prominent government websites along with the websites of banks, universities, and Estonian newspapers. These cyber attacks were launched as a protest against the Estonian government's removal of the Bronze Soldier monument in Tallinn, a Soviet war monument erected in 1947 [19].
- Damaged DND property: In July 2007, two disgruntled sailors were charged with sabotage for modifying a desktop icon, which limited the ability to search classified data on missile launches and other space-related information. The sabotage charges were dropped and the sailors were found guilty of a lesser charge of damaging military property [15].
- Human rights violations in Burma: In September 2007, the Burmese government severed connections to the Internet to prevent the transmission of videos and photos of protests against government-sanctioned human rights violations. The Psiphon censorship circumvention software, developed by the Citizen Lab at the University of Toronto, allowed the Burmese people to connect to the Internet [20].
- Russia–Georgia conflict: In August 2008, Russian troops crossed into South Ossetia vowing to defend what they called "Russian compatriots". As this was taking place, a multi-faceted cyber attack began against the Georgian infrastructure and key government web sites. The types of cyber attacks included: defacing of web sites, cyber psychological operations, and distributed denial of service [21].
- GhostNet cyber espionage network: From June 2008 to March 2009, the Information Warfare Monitor (a joint venture between The SecDev Group in Ottawa and the Citizen Lab at the University of Toronto) conducted an investigation focused on allegations of Chinese cyber espionage against the Tibetan community which led to the discovery of a malware-based cyber espionage network that they called GhostNet. They documented evidence that GhostNet had infected at least 1295 computers in 103 countries where 30% consisted of high-value diplomatic, political, economic, and military targets. Although they were not able to identify who was responsible for GhostNet, they were able to track the control servers to commercial Internet access accounts located on the island of Hainan, People's Republic of China [22].

With time, the attacks and methods used on the Internet have become more complex and more frequent. Because we have become so dependent on computers and networks, we are vulnerable in the cyber environment.

2.2 Cyber Operations

The cyber environment, also known as the cyberspace domain, is often described in two ways, one strict and one liberal, and the definition remains an unresolved issue. The strict interpretation

views cyber to include information, systems and computer networks (both wired and wireless) [6][7] while the liberal interpretation also includes everything in the electromagnetic spectrum [23]. Since the electromagnetic spectrum is already well represented in the DND/CF Electronic Warfare (EW) field, then this paper will assume the strict definition. In this case, cyber operations are considered to be and are more commonly known as Computer Network Operations (CNO). CNO consists of three activities: Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defence (CND).

- **Computer Network Operations (CNO):** actions taken to defend, exploit and/or attack information resident on Information Systems (IS) and/or the IS themselves; and is comprised of the combined disciplines of Computer Network Defence, Computer Network Exploitation, and Computer Network Attack. [30]
- **Computer Network Defence (CND):** an activity conducted through the use of one's own computer networks to protect, monitor, detect, analyze, and respond to unauthorized activity within computers or computer networks. [30]
- **Computer Network Exploitation (CNE):** a directed, covert activity conducted through the use of computer networks to remotely enable access to, collect information from, and / or process information on computers or computer networks. [30]
- **Computer Network Attacks (CNA):** a directed activity conducted through the use of computer networks to intentionally disrupt, deny, degrade, or destroy adversary computers, computer networks, and / or the information resident on them. [30]

CND is required for all operations where networks are used in any manner, whereas CNA and CNE may be required to varying degrees depending on the nature of the operation (see section 1.2 for the types of operations of the CF). For example, CNE and/or CNA may be employed domestically as a course of action to counter a terrorist attack aimed at a critical infrastructure via the networks, whereas a search and rescue mission would likely not require such action. In the case of CND, the defence of both strategic and tactical networks from various threat agents is a constant requirement.

It is important to highlight that there exist strong interdependencies between the three CNO disciplines. For example, before you can attack a network you must first exploit the network and gather intelligence of that network in order to create your plan of attack. Similarly, before attacking a network you need to first protect/shield your network against counter attacks. Figure 1 depicts these relationships.

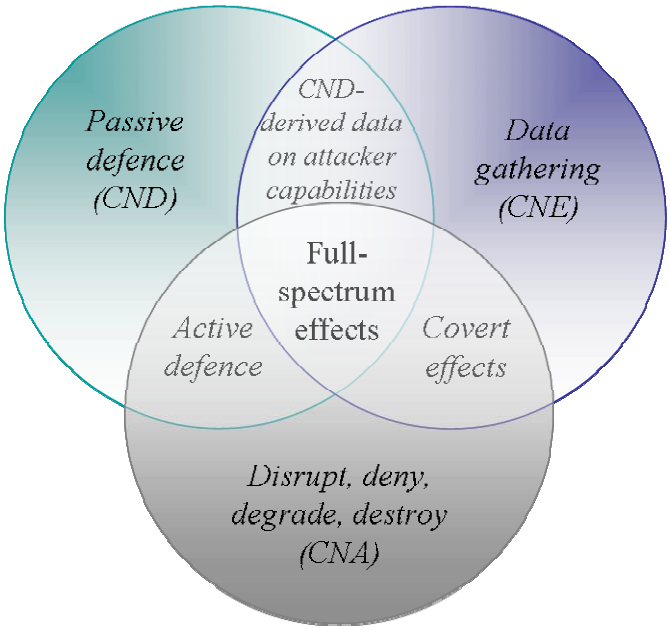


Figure 1: Interdependencies between Computer Network Operations disciplines[2]

Below are examples of activities which could fall within the intersection of more than one CNO discipline:

- CND ∩ CNE: CND-derived data on attacker capabilities. CND contributes to CNE through deriving data about the attacker's capabilities from the sensor logs. Also CND monitoring activities may reveal unusual network activity that can help cue CNE activities toward a particular target. [13]
- CND ∩ CNA: Active defence. CNA contributes to CND with active defensive countermeasures, where it may be necessary to counter-attack using CNA-type activities in order to protect the network. [13]
- CNA ∩ CNE: Covert effects. Often CNA is required to gain access to a system for data gathering in CNE. Also the aggressive and covert nature of some CNE activities could be perceived as CNA in nature in the event that they were discovered. [13]
- CND ∩ CNE ∩ CNA: Full-spectrum effects. An imminent attack requires a response that would be CND in nature but may require a CNA ∩ CNE technique such as insertion of a trojan. [13]

It should be noted that within the SCRv1.0, CNO is already recognized as a deficiency for the DND/CF, i.e. CNA is identified as deficiency Act 7, CNE as deficiency Sense 4, and CND as deficiency Shield 7 [5]. These three deficiencies are described in detail in Table 1.

[2] Diagram is a modification of the CNO Model found in [6] and [13].

Table 1: Description of deficiencies related to computer network operations

Deficiency Number	Title	Description
SCR2008 Sen 4	Inability to conduct surveillance and reconnaissance of cyberspace	There is no capability to conduct joint surveillance and reconnaissance of activities in and conditions of cyberspace. There is also no capacity for joint surveillance, reconnaissance or intelligence collection on virtual constructs and their underlying information infrastructure and identities. [24]
SCR2008 Act 7	Inability to provide Computer Network Attack activities	The CF current network operations are not established to conduct offensive network operations. The ability to disrupt and/or disable enemy networks could have an impact on mission success. [25]
SCR2008 Shd 7	Inadequate capability to detect, access and defend against cyber threats	The CF CND capability to counter increasing cyber threats (from virus infiltration to more sophisticated incidents) is inadequate. The existing Defence in Depth[3] framework is fragmented, mainly reactive, poorly sustained and lacks the flexibility and scalability to adjust to a very dynamic and rapidly evolving environment. Without the appropriate resources, capabilities, policies and procedures in place, adversaries can exploit weaknesses to achieve information superiority. [26]

[3] The Defence in Depth framework represents the use of multiple computer security techniques to help mitigate the risk of one component of the defence being compromised or circumvented.

3 Cyber Operations in the Future Environment

The future military environment will be defined by the implementation of various DND/CF concepts shown in Figure 2. Generally, a military concept is a notion or statement of an idea, expressing how something might be done or accomplished, which may lead to an accepted procedure. More specifically, "a military concept is the description of a method or scheme for employing specified military capabilities in the achievement of a stated objective or aim. This description may range from describing the employment of military forces in the broadest terms and at the highest levels to specifying the employment of a particular technology system or the application of a particular training system." [32][33][34][35][36][37]

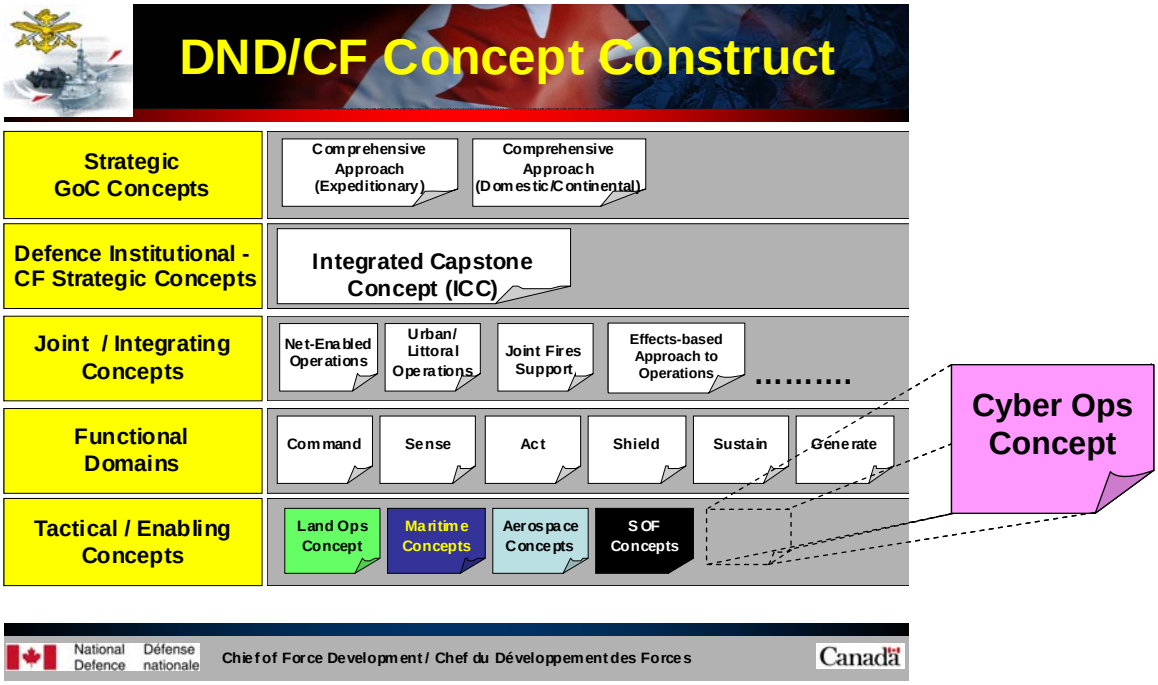


Figure 2. The (proposed) DND/CF Concept Hierarchy including the cyber operations concept[4].

Figure 2 highlights where a cyber operations concept might fit into the DND/CF concept hierarchy. Recall that in section 1.3, we stated the assumption that future military operations will follow the network-enabled, comprehensive and effects-based approaches. These concepts are still in development therefore the definitions described below may change as the concepts mature.

- **Comprehensive Approach:** In the application of this approach, the CF will form part of an integrated defence and security team, including other government department and members from the interagency security community. The intent is to combine the efforts of the DND/CF and those of OGDs and agencies, and to be able to work with non-governmental organizations (NGOs), industry and others to produce a coherent, multi-faceted effort

[4] Modified from [32][33][34][35][36][37].

supporting Canadian interests. An effective comprehensive approach includes being pro-actively involved in pre-crisis activities in order to shape events at the earliest possible opportunity. [5]

- **Effects Based Approach:** integrated sets of actions undertaken to achieve desired effects to improve our ability to shape the behaviour of both adversaries and neutrals minimizing unintended consequences. [28]
- **Network Enabled Operations (NEOps):** an evolving concept aimed at improving the planning and execution of operations through the seamless sharing of data, information and communications technology to link people, processes and ad hoc networks in order to facilitate effective and timely interaction between sensors, leaders and effects. [29]

The six capability domain concepts (Command, Sense, Sustain, Act, Shield, and Generate) that form part of the proposed DND/CF Family of Concepts in Figure 2 are defined in Table 2. The domain concepts are subordinate to the strategic Government, strategic Institutional and Joint/Integrating Concepts. The domain concepts are not mutually independent, but the interdependencies have not been studied in detail and are left to follow-on work. Finally, future concepts should be validated by rigorous debate and experimentation. The suggestions described here is the result of best effort and expertise in the time allotted and included neither extensive consultations nor any experimentation.

Table 2: Capability Domain Definitions

Domain	Definition [27]
Command	The human dimensions of command embedded within competency, authority, and responsibility; the creative expression of human will necessary to accomplish a mission; the establishment of common intent; and, the structures and processes necessary to manage command. As an operational function, *Command* sits as the nexus for the four other operational functions [Sense, Act, Shield, and Sustain. (Generate was added later)].
Sense	A single comprehensive entity that collects, collates, analyses, and displays data, information, and knowledge at all levels. Tactical, operational, and strategic assets are integrated into a single continuum.
Act	The use of a capability to influence events across the spectrum of conflict and in either or both of the physical and moral domains. Act reflects an integration of capabilities from a variety of sources – tactical, operational, or strategic.
Shield	Force protection measures taken to contribute to mission success by preserving freedom of action and operational effectiveness through managing risks and minimizing vulnerabilities to personnel, information, materiel, facilities and activities from all threats.

Sustain	A grouping of all functions necessary to generate, deploy, employ, and redeploy a force. As an operational function, the term is to be taken in it broadest possible context. Sustainment concerns are loosely grouped into three subordinate functions: materiel, personnel, and engineering.
Generate	The process by which military forces are assembled, equipped, trained, certified, and deployed to meet a force employment requirement.

The future cyber environment is under development by CFD and is discussed in [7]. For the purpose of this paper, we will consider how cyber operations will be conducted in the future military environment, where CF operations will be net-enabled, comprehensive, and effects-based. The following section will describe how cyber operations relate to the six capability domains, Command, Sense, Act, Shield, Sustain and Generate.

3.1 Capability Domains

Cyber operations are ubiquitous, and therefore cyberspace should be treated as an independent operational domain with its own inherent capabilities, as proposed in [6] and [7]. The cyber environment as a battlespace will consist of joint cyber operations that touch all the other environments (land, sea, air, space, human/cognitive). Cyber operations can contribute to the other environments by providing a capability or as a supporting element in a joint campaign plan. Likewise, operations in the traditional environments can support and provide capabilities to cyber operations.

As described in section 2.2, CNA, CNE, and CND are closely coupled[5]. As a result, they cannot be categorized individually into the capability domains. For example, CND does not exclusively fall under the shield domain, CNA under the act domain, and CNE under the Sense domain. CNO has links into each of the six capability domains. It can be both a capability and/or a support element. Figure 3 depicts the relationships (as capability or support links) between CNA, CNE, CND and the six capability domains of Command, Sense, Act, Shield, Sustain, and Generate. A dashed line indicates that a CNO element is supporting a domain, and a solid line indicates that a cyber capability exists in a domain. Note that the sustain and generate domains are grouped together in Figure 3. This is because in the cyber environment it is difficult to distinguish between sustainment issues/elements and force generation. This will be explained in their corresponding sections.

In discussing the capabilities in each functional domain, the intention is to give a flavour of what is possible rather than to provide exhaustive lists, which would require extensive research, development and experimentation.

[5] Similar to interactions between the Command, Sense and Act domains (refer to the Domain Concept Papers [32], [33], and [34]).

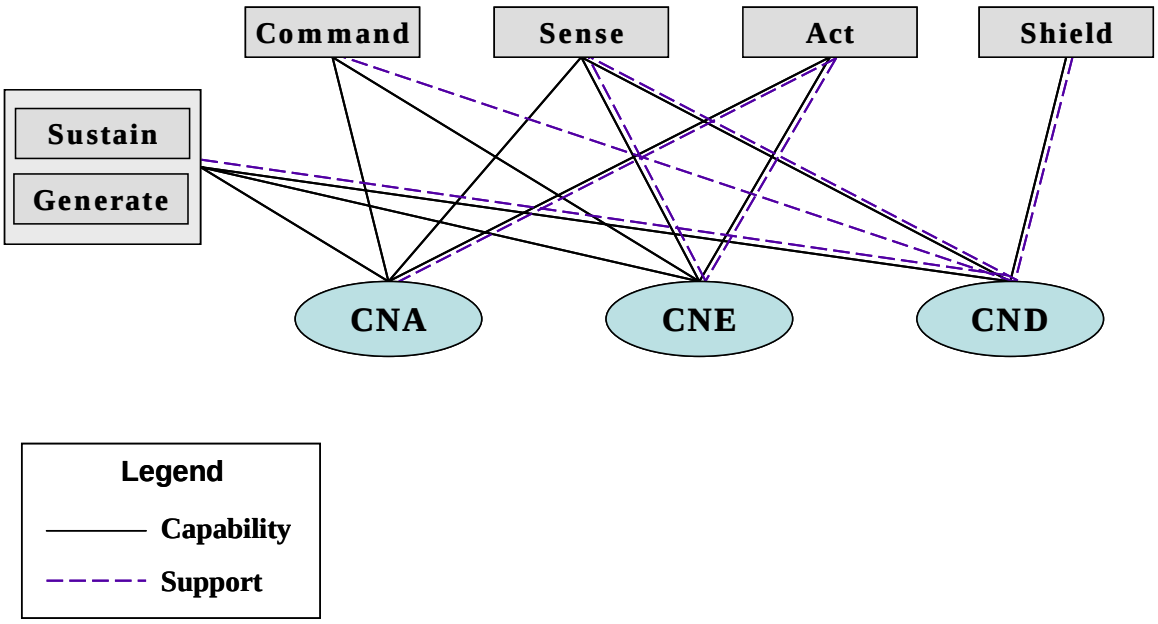
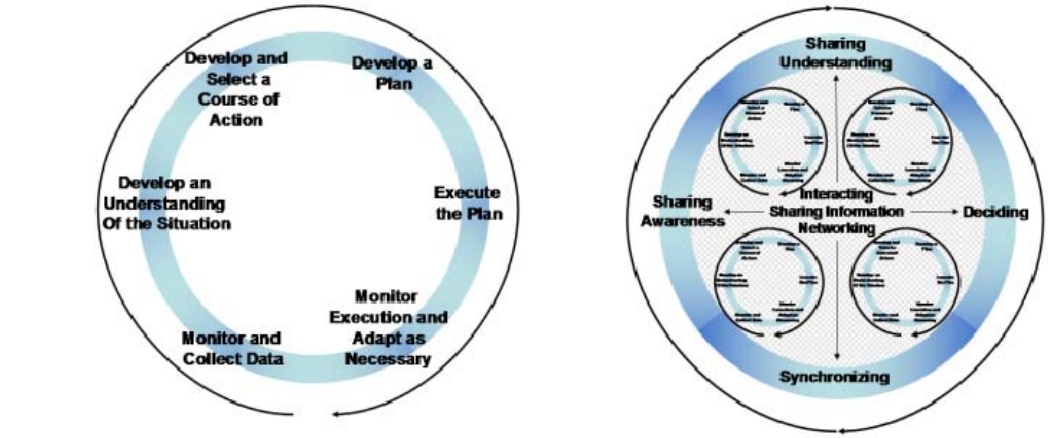


Figure 3. CNO and Capability Domain Relations. The solid lines imply that a cyber capability in CNA/CNE/CND exists in the domain. The dashed lines indicate that the domain capabilities are supported by the elements of cyber operations.

3.1.1 Command

Command, as defined in Canadian Military Doctrine [31], is "the authority vested in an individual of the armed forces for the direction, coordination, and control of military forces". Nearly everything commanders do is driven and governed by their vision, goal, or mission and the will to realize or attain that vision, goal, or mission. As such, "command" is the purposeful exercise of authority over structures, resources, people, and activities. "Control" is inherent in command; to control is to regulate forces and functions to execute the commander's intent [31]. The command capabilities include Command Support, Communications and Joint Effects Targeting and consist of a set of functions that need to be fully mastered and exercised in order to make command more effective.

The CF guiding principles [31] indicates that to meet future challenges, our forces need to be command centric and continue to develop and exemplify mission command leadership. This means that commanders need to have the right information at the right time to produce the desired effect and that subordinates need a clear understanding of the overriding commander's intent. Below, Figure 4(a) depicts the basic Command and Control (C2) process and Figure 4(b) illustrates a future collaborative C2 process model [32].



(a) (b)

Figure 4: (a) Current C2 Process. (b) Future Collaborative C2 Process Model. Note that the C2 process found in (a) is embedded in each of the four quadrants of (b).

This implies a change from a need-to-know to a need-to-share information philosophy that is required to achieve the comprehensive approach and is the basis for network-enabled operations. This proposed future collaborative model is predicated on Information Operations being fundamental to mission success and would be heavily reliant on a robust communications network, which increases the risk of network attacks.

3.1.1.1 Cyber Command Capabilities

Situational awareness of the battlespace enables the C2 process, in particular, the Command Support capability. In the cyber environment, understanding the battlespace requires situational awareness of all networks involved in operations. These may include our own networks, both strategic and tactical, service provider networks, and enemy networks. Information acquired about these networks by using CND and CNE sensor technologies (see 3.2.2 "Cyber Sense Capabilities") must be fused to give the commander an understanding of the cyber battlespace. This information should be presented in the cyber portion of a Collaborative Operational Picture (COP), enabling planning in the cyber environment.

A COP that includes cyber information such as knowledge of the adversary's CNO capabilities, (e.g. cyber weaknesses, and CNA capabilities) will allow for the targeting of enemy assets in the cyber battlespace, providing the Joint Effects Targeting capability.

Additionally, for international operations, sharing cyber information in a multi-national COP enables coordination and improved defence for all nations involved, which is an activity under the Communications capability.

3.1.1.2 Command Capabilities Supported by Cyber Operations

Including cyber information in the COP enhances planning activities in the other environments. For example, when the commander knows that a cyber asset containing information involved in their decision process may have been compromised, it will affect the outcome of the decision process. Also, if a critical network service is known to be highly at risk to attack, alternate strategies can be planned in the case that the service is lost.

Through CNE, intelligence information about an adversary's plans may be obtained if they are stored on a computer. Planning is enhanced with knowledge of the adversary's CNO capabilities, for example, knowledge of the enemy's cyber weaknesses, and what their CNA capabilities are. If the network could be penetrated as far as the enemy C2 systems, one could access their operational plans and commander's intent. This knowledge could also be gained by using network counter-surveillance operations (NCSO) [45]. Such information comes from the Sense domain and directly influences the decision cycle. More detail on this aspect can be found in section 3.1.2.1 "Cyber Sense Capabilities".

The cyber environment contributes CNA to the arsenal of weapons from which the commander can choose when forming a plan. More detail on this aspect can be found in section 3.1.3.1, "Cyber Act Capabilities".

Having the right information at the right time implies that the information required by Command staff (or, in the comprehensive approach: CF, OGDs, agencies, NGOs, and allies) must be available, its transmission confidential, and it must be stored in such as way as to ensure its integrity. Sharing information with a COP, whether national or with allies, requires secure communication and storage to ensure confidentiality, integrity and availability, which is enabled by CND operations. This is closely interrelated with the Shield domain. More detail on this aspect can be found in section 3.1.4.1 "Cyber Shield Capabilities".

The cyber environment also enables the social networking required to plan operations among individuals at different locations by providing software and mobile devices.

3.1.2 Sense

In the Sense Domain Concept paper [33], Sense is defined as "the ability to perceive the physical and non-physical environment in order to comprehend the information and to project possible futures". Fulfilling the Sense capabilities of Intelligence, Surveillance and Reconnaissance (ISR) will allow commanders to appreciate and consider the adversary's intent and actions and will provide sufficient warning of threats to allow for pre-emptive action [5].

The comprehensive approach to operations will involve the CF operating with OGDs and agencies, NGOs and allies and will require the ability to share information between them. Each player in the operation will need to contribute and also have access to the integrated Sense information. Being net-enabled will provide the means of achieving this objective. It enables all people and all systems on the network to post information to the network and retrieve information from the network, and make decisions within the limits of their authority [33]. Policies, processes and protocols will be required to ensure the information's availability and reliability. This is for both the accuracy and timeliness of the information (i.e. the validation and verification of what is

being posted) and the protection of the information (i.e. protection against attacks that attempt to change the information).

3.1.2.1 Cyber Sense Capabilities

The essential capability of the Sense domain is to provide the decision-maker with intelligence information that has been assessed and interpreted in the proper context [33]. The first step is defining the information required by the decision-maker with respect to the cyber environment. When these have been defined, the data required to supply said information can be identified. In a cyber operation, the decision-maker needs information to answer questions like:

- What are the threats to my network? Are there indications that an attack is pending or in progress? From whom?
- What on my network is critical to my cyber operation? Is its confidentiality, integrity or availability vulnerable to an attack?
- What do we know about the enemy's capabilities and location in the cyber environment?

This is not an exhaustive list. The raw data needed to create intelligence products may include:

- IT infrastructure, including services, applications, network links, and the dependencies among them, and the logical (connectivity) and physical locations of network devices.
- Network management information such as bandwidth consumption and outage events.
- Security information such as the safeguards in use, vulnerabilities that exist on the networks, and security alarms.

Typically, network traffic data is analyzed at various taps and inside the boundaries of one's own network to provide persistent monitoring of the network. The traffic can be processed by a variety of tools, including network management and security tools, network discovery tools, and advanced traffic analysis tools. Such tools give a picture of the real-time structure of one's own network, and the activities taking place upon it, including known patterns of attack. When an attack is detected, the threat agents and their locations in Cyberspace can be marked for special attention. Open Source Intelligence (OSINT) data can be obtained from publicly available Internet sources for technical information regarding vulnerabilities.

Information about the adversary's networks and the Internet at large can be obtained using similar traffic analysis techniques and other active probing tools (CNE activities). It is important to understand the enemy's cyber vulnerabilities and the criticality of their network assets [41]. This may require penetration of the network to give visibility behind routers and firewalls. Signals Intelligence (SIGINT) data, processed from intercepted network traffic, can also give a picture of the structure and activities of the enemy's networks. Over time, information can be collected from CND sensors that can reveal patterns in the enemy's tactics and assets. CNA methods can cause the enemy to react to a cyber attack, thereby revealing their capabilities in the cyber environment [41]. Human Intelligence (HUMINT) can be applied via infiltration of the Blackhat (unethical hacker) community, and OSINT via publicly-available Internet sources for both technical information and for actors.

In Defence Administrative Orders and Directives 8002-1 [42], Counter-Intelligence is defined as "… activities concerned with identifying and counteracting threats to the security of DND

employees, CF members, and DND and CF property and information, that are posed by hostile intelligence services, organizations or individuals, who are or may be engaged in espionage, sabotage, subversion, terrorist activities, organized crime or other criminal activities." In cyber, this equates to a capability to detect network probes and infiltrations from external networks, and a capability to detect covert channels and other subversive activity.

Information can be acquired about an attacker's goal, objectives and capabilities by using network counter-surveillance operations (NCSO). In NCSO, the attacker is allowed to continue the attack in a risk-managed environment where his actions are observed [45].

There are issues that are peculiar to the cyber environment. First, in the cyber environment it is very difficult to positively attribute an activity with a person or nation, or with a physical location. Second, policy for CNE/CNA activities outside of one's own network boundaries is currently undefined and is a potential barrier to CNE/CNA in cyber operations. As an example, portions of the Internet are owned and controlled by privately-owned Internet Service Providers, who may object to surveillance activities being carried out via their property.

3.1.2.2 Sense Capabilities Supported by Cyber Operations

In all environments, the ISR capabilities require secure links to protect the confidentiality of the data, whether collecting or disseminating. Secure storage is needed to ensure the integrity of the data (i.e. to protect it from being modified). Any information exchanged via network links, wired or wireless, must be protected by an appropriate level of encryption. Such a network would ideally be capable of handling multiple classifications and multiple caveats over the same links. The information must remain available for when it is needed by the Command domain.

If the enemy has stored operational plans on a network, such intelligence information may be obtained through CNE.

Commanders in all environments rely on the cyber environment to carry the intelligence products of the other environments to the COP. Thus, commanders in all environments require situational awareness of the cyber environment, as described in the previous section.

3.1.3 Act

In the Act Domain Concept paper [34], Act is defined as "the military use of capability to achieve desired effects in support of national policy". The comprehensive approach to operations implies that Act capabilities (Aerospace, Land, and Maritime Effects Production, Special Operations, and Non-Kinetic Effects Operations) will need to be integrated with OGDs and agencies, NGOs, and allies in all the environments (physical, cognitive, space, and cyber) and will be convergent in both time and space in order to produce maximum effect to achieve national goals [34].

Whether Act capabilities in the cyber environment would be best situated in the capability framework as a Special Operations capability (for discussion see [41],[40]), a Non-kinetic Effects Operations capability or as a Cyber Effects Production capability is beyond the scope of this document. Here we will simply discuss what the cyber environment can offer to the Act domain. Any Special Operations functions involving reconnaissance are considered to be covered in the

Sense domain, and the cyber-specific Special Operations counter-terrorism function is discussed separately in section 3.1.3.3.

3.1.3.1 Cyber Act Capabilities

Assuming that the activities that can be carried out in the cyber environment to produce effects in the cyber environment are entirely within the auspices of CNA, the activities are limited to operations that deny, degrade, disrupt or destroy the integrity, availability or accessibility of information on the enemy's systems. Some examples of how the enemy may be engaged to produce effects in the cyber environment are modified from [41][45]:

- Create a virtual diversion to occupy the focus of the enemy command and control.
- Degrade the network-based communication systems of the enemy.
- Deny a secure communication service so that unencrypted communication must be used.
- Modify information in the cyber portion of the enemy command and control systems to mislead them into, or keep them in, a vulnerable position.
- Insert false information on a friendly system in order to allow the enemy to find it during an enemy reconnaissance activity.

Example techniques of accomplishing effects in the cyber environment include:

- Denial of service (to deny access),
- DNS cache poisoning (to redirect),
- Insertion of malware (to install a "backdoor" for repeated access),
- Gaining access with a high level of privilege (to modify information), or
- Network counter-surveillance operations (to observe the attacker).

3.1.3.2 Act Capabilities Supported by Cyber Operations

As discussed in the Command domain, the cyber environment adds CNA to the arsenal of weapons from which the commander has to choose when forming a plan. To provide the weapons, the network must also be reliable, which in turn requires CND.

Similar to the list in the previous section, the following examples show how the enemy may be engaged in the cyber environment to produce effects in *other* environments:

- Create a virtual diversion to occupy the focus of the enemy command and control.
- Degrade the command and control systems of the enemy.
- Deny a secure communication channel so that a more exploitable communications means must be used.
- Modify information in the enemy command and control systems to mislead them into a vulnerable position in the Land, Maritime or Air environments.

Some examples of how the enemy may be engaged in the other environments to produce effects in the cyber environment are:

- Physically destroying a server or communication link.
- Implanting hardware such as a network tap or keyboard sniffer.
- Using EW capabilities to deny wireless network access.
- Using psychological operations to encourage the enemy to disclose network information or inject malicious code.

In the psychological space, one may influence behaviour by dispersing information via Internet radio, web sites, e-mail. One may send false information by using these same avenues. Denial of service tactics can be used to deny or disrupt information to the enemy, and one can provide alternate routes to the Internet to those for whom Internet access has been blocked. The recent incidents in Iran are an example, as well as Burma [20].

3.1.3.3 Counter-Terrorism in the Cyber Environment

Who handles the counter-terrorism function in the cyber environment may depend on departmental mandates; for the CF, this is consists of a Special operations function. The counter-terrorism function requires CND to defend networks, particularly those related to critical infrastructure, against terrorist attacks. These may include attacks on the confidentiality or integrity of the information therein, or on the availability of the networks themselves. The Internet backbone is one critical infrastructure, however other critical infrastructures (e.g. power and water) rely on networked systems for their control.

Terrorist activities can also be affected by using CNA to deny their capability to communicate with one another and with the public at large to spread their ideals. Through CNE, one can gather information about the people involved in the terrorist group's social networks.

3.1.4 Shield

In the Shield Domain Concept paper [35], Shield is defined as "the comprehensive approach to the protection of tangible and intangible elements through the integrating activities of pre-emption, detection, assessment, warning, defence (active and passive), and recovery". The shield capability is that of Force Protection. The future shield system is based on a vulnerability and risk analysis approach designed to deter, prevent and pre-empt hazards before they pose a risk, and to detect, deflect or otherwise counteract the direction of potential attacks on critical weak points using active, integrated and layered responses [35]. The SCRv1.0 [5] states that "cyber defence will need to be a critical component of the shield suit".

The comprehensive and net-enabled approach to operations implies that the DND/CF shield system will be integrated with the shielding capabilities of OGDs and agencies, NGOs, and allies. Rather than mass protection, the future shield system must be more adaptive in nature and be capable of adjusting the level of protection to meet changing requirements, where and when it is required. It will be based on prioritizing what we are going to secure and rapidly deciding how we are going to protect it using vulnerability and risk analysis.

3.1.4.1 Cyber Shield Capabilities

The primary activities in the Shield domain in the cyber environment are CND operations, and it refers only to the protection of DND/CF network assets. In order to adjust according to the level of protection needed under changing requirements and changing threats, the Shield domain requires situational awareness (SA) of the cyber environment. The Sense domain gathers and processes cyber SA data including IT infrastructure, security alerts, vulnerabilities present on the network, and what each asset on the network is being used for (see Section 3.1.2.1).

Assessment of threats posed by the enemy's cyber capabilities may already be available from the processed Sense data. Vulnerability assessments of one's own network are one of the sources of raw data in the Sense domain, as are the results of formal threat and risk assessments (TRA). It is not always clear at what point a Sense function transitions to become a Shield function. The Sense Domain Concept [33] states that "the domain concepts are not mutually independent, but the interdependencies have not been studied in detail and are left to follow-on work". Threat assessment is a clear example of where this sort of study will be required.

When threats and vulnerabilities have been assessed (i.e. processed relative to the criticality of the exposed and vulnerable devices and relative to the capabilities of the enemy), proactive remediation (e.g. application of patches) can begin as a proactive[6] Shield capability.

When an attack has been detected, for example through an intrusion detection system or advanced traffic analysis, defensive measures can be taken. Depending on the nature of the attack, the response may be:

- Physically unplugging the target device.
- Blocking related traffic using a firewall.
- Redirecting the attacker into a "honeypot" to observe their techniques and intent [38], or conducting NCSO [45].
- Conducting CNA to disable the attacker.

The recovery process may require: restoring a device from a known clean backup image; decontaminating one or more hosts from a virus infection; and investigating possible changes to prevent a second occurrence of the attack. This might correspond to the Sense domain's "battle damage assessment", an Intelligence activity.

A part of defending against threats is educating the users about the role that they play in the security of the network, and the potential real effect of disregarding security procedures. It only takes one user to insert an infected USB drive into an inside host to introduce a backdoor into the network for the enemy, from which point the entire network may be vulnerable to information leakage or destruction.

[6] Caution must be used when defining the scope of the term "proactive". The Treasury Board Secretariat defines proactive defence as "controlling a situation through actions in order to prevent, defend or resist an attack" [44]. These actions may or may not include CNA elements.

3.1.4.2 Shield Capabilities Supported by Cyber Operations

With the increasing use of network-enabled technologies, the Shield functions of "Assess Threats" and "Defend Against Threats" increasingly require activities that take place within the cyber environment. Threat assessments often require information that is accessed from a networked data source. This implies a need for assurance of the integrity and availability of the data, and for accessibility of the data via the network links. Protecting the data and the network are enabled by CND. Countering intelligence operations, particularly by denying information to the opposing forces, is enabled by CND.

3.1.5 Sustain

The Sustain Domain Concept proposes the following definition and scope for Sustain:

> "Sustain is the capability to maintain fighting power." As the CF continues to operate in the ever increasingly complex world, the definition of sustain will have to evolve as well. This definition is offered with the following scope: Sustain underpins the military contribution to the national effort by providing a framework of material, personnel, and information support systems that enables the fulfillment of CF/DND responsibilities – both at home and abroad, during periods of peace as well as times of war. By doing so, it helps maintain the moral, physical, and intellectual pillars that comprise fighting power. [36]

The current Sustain capabilities include Movement and Transport Support, Services Support, Engineer Support, Health Services Support, Policing Support, and Theatre Activation - Deactivation. The future Sustain concept requires the CF to be able to proactively adapt, reconfigure/reorganize and reprioritize support, for domestic and expeditionary operations in a joint, combined and interagency environment. It is a highly adaptive, agile, and flexible network of people, organizations, and technologies that integrates all sustainment capabilities, systems and processes around the globe. The CF could take advantage of its own assets, established arrangements garnering access to coalition assets, arrange for delivery directly from industry, hire charters and contractors, or employ a hub-and-spoke approach using strategically positioned regional hubs as staging bases. Distributing information to users wherever they may be located and using network architecture are all in keeping with the intelligent, global network[7] proposed in the Sustain Capability Domain Concept [36].

3.1.5.1 Cyber Sustain Capabilities

The sustain definition proposed above highlights that "providing a framework of material, personnel, and information support systems enables the fulfillment of CF/DND responsibilities". At the core of this framework are the underlying information and communication technology and its supporting networks. Therefore, sustain in the cyber environment is the capability to maintain the networks which consists of the cyber shield capabilities described in section 3.1.4.1. The CF's

[7] The intelligent, global network is a highly adaptive, agile, and flexible network of people, organizations, and technologies that integrates all sustainment capabilities, systems and processes from around the globe [36].

ability to meet these demands is not a question of mandate but one of resources [13]. As for all capabilities, personnel resources are key to their sustainment; however, the fast rate of change of technologies in cyber capabilities leads to difficulties in differentiating between Sustain and Generate [13][40]. The details on personnel resources can be found in section 3.1.6.1, Cyber Generate Capabilities.

3.1.5.2 Sustain Capabilities Supported by Cyber Operations

In support of the Sustain domain capabilities, the cyber environment must provide protection for theatre- and personnel-related information and the networks that store such information. For example: the locations of personnel, equipment and supplies must be protected; the private information of personnel must be protected, including health records and pay and benefits; and the information systems that support materiel management must remain accessible. Radio frequency identification (RFID) is increasingly being used in tracking supplies, and the security and reliability of those systems must be ensured. The sustain capability concept [36] states that the disruption of the lines of communication is the greatest risk to sustainment. If a line of communication exists in the cyber environment, it must be secured appropriately for confidentiality, integrity and availability.

3.1.6 Generate

In the Generate Concept Paper [37] Generate is defined as "the method by which Defence recruits, trains and develops personnel, procures equipment, infrastructure and services, and all are made ready in order to meet the defence mission". Based on this definition Generate capabilities consist of Personnel, Procurement, and Readiness. The future generate concept proposes that under the effects-based, network-enabled and comprehensive approaches, the CF must be adaptive, agile, and flexible to meet ever-changing Defence requirements.

3.1.6.1 Cyber Generate Capabilities

In order to meet the requirements of the cyber environment it is important to hire and retain the right people with the right capabilities for the entire CNO spectrum (to conduct CNA/CNE/CND). The personnel resources required to support cyber capabilities need a high level of expertise in their field which is not supported by with the CF's career management cycle where personnel are rotated every two to four years. Therefore, by the time military personnel have gained enough expertise to be proficient in their role it is almost time for them to move on to their next post [38][13]. As we move towards more network-enabled and comprehensive operations the need for cyber expertise will increase. Expertise can be obtained in part through training initiatives which are expensive and time consuming. Because of the fast rate of change in cyber technologies, training becomes an almost constant requirement. This highlights the importance of retaining these individuals and consequently the need for revising the career management structure for the cyber-trained military personnel. Hiring more civilians (e.g. Computer Scientists, Computer Engineers, IT professionals) can also be an option to help in this regard, however the need for military personnel will always be there. The personnel resources can leverage expertise in other departments as the vision of the comprehensive approach is realized.

The training infrastructure for the CF is also not well tailored for the required cyber related positions. LCol Castonguay reported in his thesis [13] that there are currently initiatives trying to address this issue through the Royal Military College (RMC) at the graduate level for officers and through the Canadian Forces School of Communications and Electronics (CFSCE) for new military occupational specialties and courses to address the CNO demands for officers and non-commissioned members (NCMs). However these are still being developed and are necessary for the continued sustainment and growth of the cyber resources required by the CF/DND [13]. There are other training programs under development in the Government of Canada that may be leveraged in the future, such as the Canadian National Cyber-Forensics Training Alliance. As we head to the future and technologies/capabilities change, training will need to evolve along with them.

It will also be imperative that we are able to easily procure the devices required to keep us up to date in order to defend against new attacks. Because the technologies evolve far more quickly in cyber than in other environments, we have to be able to adopt leading-edge technologies without being hampered by the procurement process.

Readiness in the cyber environment will be attained by continuous training due to the fast rate of change in technologies and exploits. This includes simulated war-gaming and live exercises, for example in the scenario of an unexpected cyber attack.

3.1.6.2 Generate Capabilities Supported by Cyber Operations

By maintaining the freedom to operate in the cyber environment it ensures that the information and communication infrastructure is available for online services and also allows access to resources that can be achieved remotely. This allows for the use of the cyber environment for recruitment, training, and procurement.

4 Risks and Mitigations

This chapter identifies risks to developing capabilities in the cyber environment and discusses some possible mitigation strategies for each identified risk. The risks and their possible mitigations are shown in Table 3. These risks were already highlighted in four of the six CFD domain concept documents (referenced in Table 3); they are brought together here to provide the complete view for the cyber environment. The risks identified also involve the strategic and joint/integrating concepts assumed in the development of this report.

Table 3: Risks Related to Cyber Environment

No:	Risk	Description
1	Policy and legislative barriers	Scientific and technological advances are moving faster than the accountability and responsibility control mechanisms, and faster than the ability to implement public policy and legislation, which adequately protects individual rights, but enables the nation to defend itself from attack [34]. Departmental policy frameworks and behavioural norms lag behind the requirement to share and exploit information, as well as undertake offensive network information operations [35].
2	Cyberspace is vulnerable to attack by state and non-state actors	Cyberspace is an environment where computer networks are continually under attack [34]. As previously stated, the Future Security Environment states that cyber attacks may become the attack of choice for non-state actors since the cost is relatively small [3].
3	Lack of central regulating agency to monitor cyberspace	Detection of proliferation of hostile technology, intent and behaviour is more complicated due to the extent of the cyber environment. Even when a threat is detected, preventive actions (both in the physical and cyber domains) are difficult due to legislative context, anonymity of the users, and the use of free hosting services. The absence of a central regulating agency also precludes a central law enforcement agency. [35][44]

4	Lack of a common network and standards	Cyber security also bears risk from the lack of a common network and/or an effective information sharing capability between allies and OGDs. This deficiency puts the Comprehensive Approach directly at risk. [32]
5	Sharing of information	The institutionalization of restrictive policies and barriers concerning information and intelligence is a result of the mindset of "need to protect" rather than the more productive "need to share". The risk is that necessary information will not get to the right people at the right time, and that they will remain information "deprived" and therefore unable to consistently engage in effective decision making. [35]
6	Effect-based operations	Traditional battle damage assessment is still very relevant in effects-based operations in order to determine the immediate effects that result from cyber and local actions. However, under this framework, it must be recognized that these actions will also produce non-physical, long-term, and global effects. [33]
Applies to:	**Mitigation**	**Description**
1	Create working networks among Govt Departments and Agencies.	Government departments and agencies will develop trusted working relationships while the policy and legislative frameworks evolve. Information management systems that support the Comprehensive Approach will be developed with common standards and common exchange formats to support exchange of information, when and if authorized. [34]
1&2	Increase appreciation, awareness and education	Our policy makers at all levels need to be conscious that the mechanics of cyber defence, exploitation and attack will require changes in the policy realm. This implies a commitment to provide those policy makers with the necessary education to raise awareness. [35]
2	Treat Cyberspace as another Environment	DND/CF in collaboration with OGDs and industry must develop offensive and defensive capability in cyberspace. [34]

3	Create a national central regulatory agency and influence allies to do the same	With a national regulatory agency, we can monitor activities within our borders. Excessive regulation will likely not be possible due to the commercial aspects of the Internet, however. OGDs, agencies and NGOs can be self-regulating entities. On an international level, agreements can be made to share information on international activities. International cyber laws may then be created and enforced. [44]
4	Implementation of trusted networks, while IM/IT continues R&D	Trusted networks or enclaves will be established with secure identity and access management. Network users will be able to collaborate and share information in a secure environment. [34]
5	Adopt a "need to share" culture	To mitigate risk of leakage involving sensitive information, we must recognize that not all information needs to be protected equally, and we need to develop and institutionalize tactics, techniques and procedures (TTPs) that reflect the "need to share" attitude. Developing mutual respect across organizational boundaries (in a coalition environment) will contribute to appropriate information sharing, thereby strengthening the shield network. [35]
6	Assessment of non-physical effects	There needs to be an augmented Sense capability that can assess these nonphysical effects. As well, a change of mindset is required when approaching effects assessment. There needs to be ways of applying the same notions of detecting, identifying, classifying, etc., to non-physical effects. Research in cyber, cognitive, and social systems may provide some insight in how to do this. [33]

5 Implications

This section identifies and describes potential implications that the cyber environment may have for the Canadian Forces and future capability development. The implications are categorized based on the PRICIE construct (**P**ersonnel, **R**esearch and Development/Operational Research, **I**nfrastructure/Environment and Organization, **C**oncepts/Doctrine/Collective training, **I**nformation Management and Technology, and **E**quipment and Support).

5.1 Personnel

The network-enabled approach emphasises the need for effective computer network defence in order to maintain workflow and operations. Training of personnel in network-enabled operations will be required. Education will also be needed to enhance the awareness of the risk of cyber attacks. There will be an increase in the demand for skilled personnel in computer network operations and some elements of cyber operations such as CNA will require training in new field of expertise. Consequently there will be a need to recruit and retain individuals with the requisite skills. Section 3.1.6.1 discussed programs at RMC and CFSCE that are currently being developed to address the training needs. However, in the future as we become more and more network enabled and technology dependent, these cyber expertises will be in greater demand. The CF will need to revaluate their occupational structure and consider adding cyber related trades and specialties for both officers and NCMs.

The comprehensive approach is very applicable to cyber operations as cyber attacks are often focussed on targeting critical infrastructures which can involve other government department and agencies as well as non-government department. These operations will require changes in the attitude and mindset as many of the operations will not be led by the CF but the CF would provide a supporting role. New tactics, techniques and procedures will need to be developed and training will be critical for this to be successful.

5.2 Research and Development/Operational Research

DRDC is in a strong position to support the development of concepts foe the cyber environment and cyber operations for DND/CF. The Defence S&T Strategy identifies CNO as a technical challenge area in the Communications Networks area of S&T expertise [43]. DRDC is fully aware of the challenges of exploiting the opportunities offered by the Information Age and the increasing threats of cyber attacks. The Canadian Forces Information Operations Group (CFIOG) in conjunction with ADM(S&T) are currently developing a CNO S&T Strategy that will guide S&T efforts supporting the development and sustainment of cyber capabilities of the CF. The CNO S&T Strategy will enable the CF to stay abreast, if not ahead of new cyber developments through active Defence Research programs and partnership with academic institutions, industry and our allies.

Other government departments and non-government organizations are also contributing to the research and development in the cyber environment, among which are the Communications Research Centre, Royal Canadian Mounted Police, Canadian Security Intelligence Service,

Public Safety Canada, and Communication Security Establishment Canada. From the academic side, the Canadian Forces College has been publishing research theses in the cyber field[8] through their Masters of Defence Studies program and the Royal Military College of Canada has also been conducting research in various aspects of CNO under the Computer Security Laboratory of the Electrical and Computer Engineering Department[9].

5.3 Infrastructure/Environment and Organization

The cyber environment may be considered as a battlespace which would involve changes in both organization and infrastructure. Currently cyber operations are slotted under the Command domain; however we have shown that cyber operations touch all of the domains. This demonstrates that cyber operations are a distinct capability element, much like air, land and naval operations. A Directorate of Cyber Development (DCyberD), analogous to DSpaceD, may also be considered.

The comprehensive approach implies a need for organization changes to improve the linkages between DND/CF and OGDs and agencies, NGOs, and allies. The network-enabled approach will require new infrastructures that will promote the agility and flexibility of our forces. Education on security protocols and risks will be important if we make use of trusted networks and rely on self-regulation for low critical systems.

5.4 Concepts, Doctrine and Collective Training

Treating the cyber environment as a battlespace will challenge current doctrine and will involve further concept development and experimentation. A cyber strategy and campaign plan will need to be developed followed by concepts and doctrine for cyber operations including cyber attack, cyber exploitation and cyber defence. These will need to be thoroughly tested by means of modeling, simulation and experimentation. The Strategic Joint Staff is currently developing new policies for CNO however the same will be needed for cyber operations especially for integrated operations.

The comprehensive approach adheres to a need-to-share philosophy, but there are currently legislative limits that prevent the DND/CF from sharing operational information with and receiving operational information from OGDs and agencies, NGOs and allies [44]. There are also legislative limits on how the DND/CF can handle information gathered while conducting CNE types of operations, for example human rights to privacy.

5.5 Information Management and Technology

The networked-enabled approach requires the transmission and processing of high volumes of information, which poses significant technological challenges to the information management infrastructure. It will therefore place significant demands upon scarce battlefield communications

[8] Search through the CFCS database at http://www.cfc.forces.gc.ca/en/cfcpapers/index.php. For example, [13] and [40] can be accessed through this website.
[9] Research by Knight and Leblanc can be accessed at http://tarpit.rmc.ca/, e.g. [39][41][45].

bandwidth and security; command and control infrastructure; and vulnerability assessment and protection.

The need-to-share versus need-to-protect philosophy of the comprehensive approach poses significant technological challenges to the information management infrastructure. There will be a need for integrated databases on trusted networks that will be accessed by the DND/CF, OGDs and agencies, NGOs, and allies, depending on the type of operation.

5.6 Equipment and Support

The development of a cyber capabilities and the increase in cyber attacks has strong equipment and support implications for the DND/CF. There is a need for the design and development of command and control systems that integrate cyber situational awareness and the development of sensor systems for cyberspace will be critical in providing the cyber situational awareness. The comprehensive approach and network enabled approach will require that these systems be interoperable with OGDs and agencies, NGOs, and allied systems.

6 Current Initiatives and Future Work

6.1 Current Initiatives in the DND/CF

The current initiatives within DND/CF all focus on improving DND/CF CND activities. Currently, information is manually correlated to understand the cyber environment. The process is improving with the use of a shared database of information, so that the information does not have to be gathered from disparate sources. DRDC Ottawa's Joint Network Defence and Management System Technology Demonstrator Program (JNDMS TDP), which has just completed, has shown that situational awareness for CND can be more efficiently provided by using a data model shared across DND's networks. This work has motivated the creation of the Network Command and Control Integrated Situational Awareness Capability (NetC2-ISAC) project. Sharing network event data regarding our own networks with the other domains is currently accomplished using the CommandView application; however this does not give a view of the cyber environment. The NetC2-ISAC project is in a definition phase, with the goal of integrating CF network information into a single data model for improved situational awareness of the cyber environment. Which data needs to be shared in a coalition has not been determined in a rigorous manner; the NATO RTG IST-081 "Coalition Network Defence Common Operating Picture" hopes to advise on a standard for information sharing.

Other DRDC research applicable to this capability includes the Automated Computer Network Defence (ARMOUR) Technology Demonstrator (TD) and the CND Decision-Making Applied Research Program (ARP). The TD Program seeks to make recommendations for the optimal course of action for an attack in progress. It will demonstrate the capability to proactively deal with vulnerabilities, minimizing the risk of attacks on the networks. It will also allow operators to react more quickly to on-going attacks. The ARP seeks to improve CND decision making capabilities by addressing existing deficiencies with sensors, organizational processes and information analysis tools. This ARP proposes to develop a simulated CND environment where decisions, policies and strategies can be trialed. It will also investigate automation of simple and repetitive tasks, resulting in a better use of scarce resources.

There currently are few known open source initiatives investigating CNA, apart from limited work conducted at the RMC Computer Security Laboratory on reverse http tunnels[10] and hardware-based trojan horse devices. There may also be some initiatives on CNE occurring in the intelligence domain that we are not aware of but this would be classified and will not be covered in this paper.

6.2 Current Initiatives in the Government of Canada

Government of Canada (GoC) initiatives include the Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) which is responsible for monitoring threats and coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents. Public Safety Canada has also developed a National Cyber

[10] HTTP tunneling is a covert channel technique by which communications performed using various network protocols are encapsulated using the HTTP protocol usually to bypass firewalls or proxy servers.

Security Strategy. Another GoC initiative is the Treasury Board of Canada Secretariat's Proactive Cyber Defence project. The proactive cyber defence project is a government wide initiative that seeks to provide the capability to better protect GoC critical systems and reduce the risk of major cyber incidents. It implies that proactive cyber defence will allow departments and the GoC to better protect systems by obtaining a greater understanding of GoC critical systems and their interdependencies; providing an ability to assess the state-of-security; and establishing a central organization and authority capable of prioritizing efforts and taking government wide mitigating actions [44].

On the R&D side, there is the Public Security Technical Program (PSTP), led by Defence Research and Development Canada's (DRDC) Centre for Security Science (CSS). PSTP's mission is to strengthen Canada's ability to prepare for, prevent, respond to, and recover from high-consequence public safety and security events by employing S&T as a strategic enabler and lead investment for the federal government's public safety and security agenda. Within its Critical Infrastructure Protection domain PSTP has established a cyber security component. As part of this initiative a PSTP Cyber Security Community of Practice (CoP) has been created to gain an initial understanding of the various mandates relating to cyber security, assess the required capabilities, identify gaps that need strengthening; and identify the S&T areas that will address such gaps. There are currently two studies being funded under PSTP. The first will be developing a better understanding of cyberattacks employing "botnets" and the second is on the use of artificial intelligence to model complex information systems and analyze the security risks.

6.3 Future Work

It is evident from the synthesis of the work presented in this paper that the DND/CF requires the development of a cyber strategy in order to drive future efforts in cyber Concept Development and Experimentation. This would include Canadian concepts on CNA/CNE/CND activities.

Based on the recommendation from CFD/DG Cap Dev presented at the C4ISR Science and Technology Oversight Committee, the urgent areas that R&D needs to focus in the cyber environment is within cyber security operations. Two areas were presented: SA of cyberspace and effects of command decisions; and cyber Command and Control capability for CNA/CNE/CND. Other areas of importance are the protection of Canadian critical infrastructures and the improvement of our ability to respond to threats.

7 Conclusions

This document is meant to describe how the Canadian Forces might employ cyber capabilities in operations in the future. As such, it is necessarily a living document that will continue to be revised and refined as policy and technology advance. The intent of this paper is to provide a starting point to help guide the department in future cyber concept development. Elements of the cyber environment at present are a deficiency in all of the DND domains. There is a wider military recognition of the need for cyber operations in the CF, however there is still confusion surrounding how the military intends to integrate cyber operations into operations in general. In this paper we stated the current proposed definition for the cyber environment and we discussed the impact of the cyber environment in each domain (Command, Sense, Act, Shield, Sustain, Generate), and in particular addressed the cyber capabilities and how the cyber environment supports the domain in other environments (i.e. physical, human/cognitive, space). We also identified potential risks and some possible mitigation strategies for each of them and discussed the current and future implications of each element of the PRICIE construct. Force developers are encouraged to investigate and discuss this proposed concept paper to further evolve our collective understanding and effectiveness to improve our response to the asymmetric threats of the future.

References

[1] Department of National Defence, *Canada First Defence Strategy*, 2008.

[2] Fossi, M. et al., *Symantec global Internet security threat report: Trends for 2008, volume XIV*, Symantec, Inc., April 2009, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, accessed 23 November 2009.

[3] Department of National Defence, *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*, Chief of Force Development, 27 January 2009.

[4] Kurtz, P. et al., *Virtual Criminology Report 2009 –Virtually Here: The Age of Cyber Warfare*, McAfee, Inc., 2009, http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf, accessed 25 November 2009.

[5] Department of National Defence, *Strategic Capability Roadmap Version 1.0*, Chief of Force Development, July 2008.

[6] Department of National Defence, *Integrated Capstone Concept Draft*, Chief of Force Development, Director of Future Security Analysis, 30 June 2009.

[7] Department of National Defence, *Nature of Future Environments: Cyberspace Environment Version 1.0*, Chief of Force Development, Director of Future Security Analysis, March 2009.

[8] Rothschild, M., *The threat from within: the evolution of cyber attacks*, Computer Technology Review, 1 March 2006.

[9] Oldfield, P., *Computer viruses demystified*, Aylesbury, Sophos, 2001.

[10] Bruno, G., *Backgrounder: The Evolution of Cyber Warfare*, The New York Times, 27 February 2008, http://www.nytimes.com/cfr/world/slot1_20080227.html, accessed 19 November 2009.

[11] Public Safety Canada, *About Critical Infrastructure*, Government of Canada, http://www.publicsafety.gc.ca/prg/em/ci/about-eng.aspx, accessed 6 October 2009.

[12] Centre for Critical Infrastructure Protection, *What are the Cyber Threats?*, New Zealand Government, http://www.ccip.govt.nz/about-ccip/what-are-cyber-threats.html, accessed 6 October 2009.

[13] Castonguay, LCol F., *Evaluating Canada's Cyber Semantic Gap*, JCSP 35 Master of Defence Studies Research Project, Canadian Forces College, Toronto, June 2009.

[14] United States General Accounting Office, *Technology Assessment Cybersecurity for Critical Infrastructure Protection*, GAO-04-321, Washington, D.C., May 2004.

[15] Pugliese, D., *Court-martialled sailors handed minimum sentence*, Ottawa Citizen, 10 February 2009, http://www.canada.com/news/Court+martialled+sailors+handed+minimum+sentence/1271179/story.html, accessed 25 November 2009.

[16] Mulvenon, J., *PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability*, Chapter 8 of Beyond the Strait: PLA Missions other than Taiwan, Strategic Studies Institute, United State Army War College, Pennsylvania, April 2009.

[17] Thomas, T., *Hezballah, Israel, and Cyber PSYOP*, IOsphere, Winter 2007.

[18] Hoffman, M., *Israel, Hezbollah, and the Cyberwar of 2006*, DailyTech online magazine, http://www.dailytech.com/Israel+Hezbollah+and+the+Cyberwar+of+2006/article3589.htm, accessed 6 July, 2009.

[19] Vamosi, R., *Cyberattack in Estonia-what it really means*, CNet News, http://news.cnet.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html, accessed 6 July, 2009.

[20] Diebert, R., Rohozinski, R., *Ottawa needs a strategy for cyberwar*, Information Warfare Monitor, http://128.100.171.10/modules.php?op=modload&name=News&file=article&sid=2393, accessed 10 July 2009.

[21] Coleman, K., *Cyber War 2.0 -Russia v. Georgia*, Defense Tech, http://www.defensetech.org/archives/004363.html, accessed 6 July, 2009.

[22] Deibert, R., Rohozinski, R., *Tracking GhostNet: Investigating a Cyber Espionage Network*, Information Warfare Monitor, JR02-2009, March 2009.

[23] United States Department of Defense, Joint Chief of Staff, *National Military Strategy for Cyberspace Operations*, December 2006.

[24] Chief of Force Development-Capability Management, *Sense Capability Alternative Evaluation*, http://cfd.mil.ca/sites/page-eng.asp?page=4963, accessed 19 November 2009.

[25] Chief of Force Development-Capability Management, *Act Capability Alternative Evaluation*, http://cfd.mil.ca/sites/page-eng.asp?page=4962, accessed 19 November 2009.

[26] Chief of Force Development-Capability Management, *Shield Capability Alternative Evaluation*, http://cfd.mil.ca/sites/page-eng.asp?page=4961, accessed 19 November 2009.

[27] Chief of Force Development-Capability Management, *Capability Domains – Definitions*, http://cfd.mil.ca/sites/page-eng.asp?page=4281, accessed 1 May 2009.

[28] Graham, J. D., Smith-Windsor, B. A. *Effects Based Approach to Coalition Operations: A Canadian Perspective.* In 2004 Command and Control Research and Technology Symposium, Washington, D. C., http://www.dodccrp.org/events/2004_CCRTS/CD/papers/165.pdf, accessed 6 October 2009.

[29] Babcock, S., *DND/CF Network Enabled Operations Working Paper*, DRDC CORA TR 2006-001, Defence Research and Development Canada, January 2006.

[30] Department of National Defence, *Canadian Forces (CF) Computer Network Operations (CNO) Policy Draft Version 2.1*, 28 July 2009.

[31] Canadian Forces Experimentation Center, *CFJP 01 – Canadian Military Doctrine*, Canadian Forces Joint Publication, 2009-04.

[32] Chief of Force Development, *Command Capability Domain Concept Version 3.0*, December 2007.

[33] Chief of Force Development, *Sense Capability Domain Concept Version 3.0*, February 2008.

[34] Chief of Force Development, *Act Capability Domain Concept Version 1.0*, May 2008.

[35] Friesen, Shaye et al., *Capability Domain Concept – Shield Capability Domain*, DRDC CORA TM 2009-005, Defence Research and Development Canada, January 2009.

[36] Chief of Force Development, *Sustain Capability Domain Concept Version 3.4*, January 2008.

[37] Chief of Force Development, *Generate Capability Domain Concept Version 3.0*, January 2009.

[38] Treurniet, J., *An Informal Study of the CF Network Operations Centre (Protected B)*, DRDC Ottawa Letter Report File #2900-50, DMCS ref# 5155, January 2008.

[39] Leblanc, S. P., Knight, G. S., *Engaging the Adversary as a Viable Response to Network Intrusion*, Workshop on Cyber Infrastructure – Emergency Preparedness Aspects, University of Ottawa, Ottawa, 2005.

[40] Allen, Maj F.J., *CN(EH?) – A Recommendation for the CF to Adopt Computer Network Exploitation and Attack Capabilities*, CSC 28 Thesis, Canadian Forces College, 2002.

[41] Leblanc, S. P., Knight, G. S., *Choice of Force - Special Operations for Canada*. Chapter 11: Information Operations in Support of Special Operations. D. Last and B. Horn eds., McGill-Queen's University Press, Montreal, 173-185, 2005.

[42] ADM(Fin CS), *DAOD 8002-1, National Counter-Intelligence Program*, http://www.admfincs.forces.gc.ca/dao-doa/8000/8002-1-eng.asp, accessed 10 July 2009.

[43] Department of National Defence, *Defence S&T Strategy - Science and Technology for a Secure Canada*, December 2006.

[44] Treasury Board of Canada Secretariat, *Government of Canada Proactive Cyber Defence Project Report DRAFT V8*, Chief Information Officer Branch, Security and Identity Management, 26 June 2008.

[45] Leblanc, S. P., Knight, G. S., *When Not to Pull the Plug – The Need for Network Counter-Surveillance Operations*, Conference on Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, June 2009.

List of symbols/abbreviations/acronyms/initialisms

ADM	Assistant Deputy Minister
ARMOUR	Automated Computer Network Defence
ARP	Applied Research Program
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCIRC	Canadian Cyber Incident Response Centre
CF	Canadian Forces
CFD	Chief of Force Development
CFIOG	Canadian Forces Information Operations Group
CFNOC	Canadian Forces Network Operations Centre
CFSCE	Canadian Forces School of Communications and Electronics
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CO	Commanding Officer
CoP	Community of Practice
COP	Common Operational Picture
CORA	Centre for Operational Research and Analysis
CSS	Centre for Security Science
DCyberD	Directorate of Cyber Development
DDOS	Distributed Denial of Service
DG Cap Dev	Director General Capability Development
DND	Department of National Defence
DOS	Denial of Service
DRDC	Defence Research & Development Canada
DRDKIM	Director Research and Development Knowledge and Information Management
EW	Electronic Warfare

GoC	Government of Canada
HUMINT	Human Intelligence
IM	Information Management
IS	Information System
IT	Information Technology
JNDMS	Joint Network Defence and Management System
NATO RTG IST	North Atlantic Treaty Organization Research Task Group Information System Technology
NCMs	Non-Commissioned Members
NCSO	Network Counter-Surveillance Operations
NEOps	Network-Enabled Operations
NetC2-ISAC	Network Command and Control Integrated Situational Awareness Capability
NGOs	Non-Government Organizations
OGDs	Other Government Departments
OSINT	Open Source Intelligence
PRICIE	**P**ersonnel, **R**esearch and Development/Operational Research, **I**nfrastructure/Environment and Organization, **C**oncepts/Doctrine/Collective training, **I**nformation Management and Technology, and **E**quipment and Support
PSTP	Public Security Technical Program
R&D	Research & Development
RFID	Radio Frequency Identification
RMC	Royal Military College
SA	Situational Awareness
SCRv1.0	Strategic Capability Roadmap Version 1.0
SIGINT	Signals Intelligence
S&T	Science and Technology
TD	Technology Demonstrator
TRA	Threat Risk Assessment
TTP	Tactics, Techniques, and Procedures
USB	Universal Serial Bus

Distribution list

Document No.: DRDC CORA TM 2009-058

LIST PART 1: Internal Distribution by Centre

1 Ross Graham, DG CORA
1 Roy Mitchell, SH Maritime
1 Dean Haslip, SH Land
1 Denis Bergeron, SH Air
1 Charles Morrisey, SH Joint & Common
1 BGen P. Matte, CFD/DG Cap Dev
1 LCdr C. Dewar, CFD/D Mil CM 3 Command
1 LCol M. Barrett, CFD/D Mil CM 4 Sense
1 Col G. Loos, Commanding Officer, AMD(IM)/CFIOG
1 LCol K. Schramm, ADM(IM)/COS(IM)/J6 Coord
1 LCol J. Blythe, ADM(IM)/DGIMO/DCCI
1 LCol M. Purcell, SJS/Ops
1 LCol F. Castonguay, ADM(IM)/DGIMT/DGIMTPS
1 LCdr D. Harnett, CFD/DFSA
1 LCol W. Yee, CFD/DFSA
1 Maj. M. Setter, CFD/DFSA/
2 CORA Library (1 hard copy + 1 PDF)
2 Author – Melanie Bernier (1 hard copy + 1 PDF)

20 TOTAL LIST PART 1 (2 hard copies + 18 PDF)

LIST PART 2: External Distribution by DRDKIM

1 A. Vallerand, Director, DRDC CSS/DSTPS
1 Maria Rey, Director General, DRDC Ottawa
1 Julie Lefebvre, Section Head, DRDC Ottawa/NIO
1 Luc Beaudoin, DRDC Ottawa/NIO
1 Sylvain Leblanc, RMC/Department of Electrical and Computer Engineering
1 LCol A. Boucher, Commanding Officer, ADM(IM)/CFIOG/CFNOC
1 LCol S. Hall, CF School of Communications and Electronics, Kingston, ON
2 Author – Joanne Treurniet, DRDC Ottawa/NIO (1 hard copy + 1 PDF)

9 TOTAL LIST PART 2 (1 hard copy + 8 PDF)

29 TOTAL COPIES REQUIRED (3 hard copies + 26 PDF)

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – CORA
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

CF Cyber Operations in the Future Cyber Environment Concept

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Bernier, M.; Treurniet, J.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
December 2009	56	36

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – CORA
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CORA TM 2009-058	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

As the world becomes increasingly network-enabled, the Canadian Forces must adapt to meet the challenges that come with this technology. These include a new set of threats, and a new set of capabilities that have yet to be formally defined and explored. It is possible that the founding of an entirely new environment, the cyber environment, may be the most suitable way ahead in developing these new capabilities. This paper describes cyber operations and how they fit into the DND/CF concept construct. The capabilities provided by operations in the cyber environment and the supporting functions of cyber operations are discussed for each functional domain. Risks related to the cyber environment are listed, along with potential mitigations. The implications in terms of the PRICIE construct are discussed, and relevant activities within DND and the Government of Canada are listed. This paper may be used to advise on the future development of the cyber environment concept, and to muster appreciation of the contributions of the cyber environment to operations across all environments.

Les technologies réseaucentriques se répandent partout dans le monde, et les Forces canadiennes doivent s'adapter pour relever les défis qui découlent de ces nouvelles technologies. Elles doivent notamment faire face à une nouvelle série de menaces, et définir et examiner une nouvelle série de capacités. Il est possible que la création d'un environnement tout à fait nouveau, le « cyber-environnement », soit le meilleur moyen de développer ces nouvelles capacités. Le présent document décrit les cyber-opérations et comment elles s'intègrent à la structure conceptuelle du MDN et des FC. Les capacités fournies par les opérations dans le cyber-environnement et les fonctions liées aux cyber-opérations sont examinées pour chaque domaine fonctionnel. Les risques associés au cyber-environnement sont énumérés, avec les mesures d'atténuation possibles. Les répercussions du cyber-environnement sur le concept PRICIE des FC sont examinées, et les activités touchées au MDN et dans le gouvernement du Canada sont énumérées. Le présent document peut être utilisé pour donner des conseils sur le développement futur du concept de cyber-environnement, et pour expliquer quelle sera la contribution du cyber-environnement aux opérations dans les trois armées.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

cyber environment; cyber operations; computer network operations

Defence R&D Canada

Canada's Leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca