



Government
of Canada Gouvernement
du Canada

JDN 2017-02

Canadian Armed Forces Joint Doctrine Note



Cyber Operations

Custodian: D Cyber FD

Promulgated:

Canada

● te note est également disponible en français.

This joint doctrine note (JDN) is for official defence use only and its release to the public is not authorized. Some or all of its content may be exempt from release under sections 13(1) and 15(1) of the *Access to Information Act*. Requests for the public release of this publication must be staffed to the Joint Doctrine Branch, CF Warfare Centre, and the custodian. This JDN may be shared with partners in government, industry, academia, and allied and partner nations for defence purposes only.

To ensure you are using the current version of this JDN, refer to the joint doctrine DIN website at:
<http://cjoc-coic.mil.ca/sites/intranet-eng.aspx?page=5893>

Joint doctrine notes are expeditious in nature and provide initial guidance based on lessons identified. They are “interim doctrine” for the planning and execution of joint operations. Joint doctrine notes often span all levels of war, requiring the modification of multiple extant doctrines when implemented.

Joint Doctrine Branch
Canadian Forces Warfare Centre
Department of National Defence
Major-General George R. Pearkes Building
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

© Her Majesty the Queen as represented by the Minister of National Defence, 2017

FOREWORD

01. Over the past five decades there has been a transformational impact on global society by the rapid, quite literally exponential, increase in the capabilities and use of information technologies. The interconnection of a wide variety of information technology components has moved information technology from the lab into a potential human right and established what we and our allies now call cyberspace. We stand in the middle of that transformation, with a relatively poor understanding of its long term impacts – but an absolute imperative to not ignore its far reaching influence on the profession of arms.

02. Over the same period, but significantly accelerating in the past few decades, Western armies, including the Canadian Armed Forces (CAF), have invested heavily in technologies that have radically increased the speed and precision of modern combat operations. **Underpinning most of these incredible leaps in capability has been a reliance on cyberspace. Initially, this reliance was poorly understood and military capabilities were procured and developed with an implicit assumption that secure accessibility to cyberspace would be available to support them.**

03. **It is now clear that that implicit assumption is wrong.** Friendly access to, and use of cyberspace is not only potentially contestable – but actively contested. In addition, as militaries have discovered their own vulnerabilities in cyberspace they have come to discover those of their adversaries. The cyber domain is contested, and the CAF can expect to have its operations resisted through military cyber operations. **The CAF, working with its allies, will need to be ready to fight for its freedom of action in cyberspace.**

04. Although the concepts, doctrine, lexicon and nearly every other aspect of cyber operations remain areas of active discussion and debate, over the past decade or so a common perspective has coalesced. This doctrine note attempts to capture the core thoughts of that common perspective.

05. That said, there remains much in this joint doctrine note subject to heated debate and outright disagreement among experts. **It is far too soon to commit the CAF to a rigid doctrine for cyber operations; there remain too many areas for active intellectual development.** Nevertheless, it is also already late to put some basic concepts for conflict in the cyber domain into the hands of Canada's profession of arms to inform current operations and drive and frame the ongoing discussion and development of excellence in military cyber operations. Thus, **readers should note that the JDN reflects the state of cyber operations at the time of writing (December 2016) whereby those sections highlighted as mature reflect those aspects of general consensus and proven experience.** Those sections identified as concept and developing reflect areas of ongoing debate and development, but illustrate the direction in which the CAF is moving towards. With the rapid and ongoing evolution of the cyber domain, there may be areas of the document that no longer reflect reality, hence the requirement for ongoing concept and doctrine development that will lead to future iterations of the JDN until such time as a steady state can be achieved to allow for the publication of formal joint doctrine for cyber operations.

06. Finally, this document intentionally addresses the fullest range of cyber operations without reference to those that the CAF is authorized to undertake. Many of Canada's allies have formally and publicly indicated their capability and intent to use offensive cyber. Any even rudimentary understanding of the cyber domain must comprehend this aspect of operations.

JDN 2017-02
(PROMULGATION DRAFT)

07. I truly hope that those reading this document find it useful, ideally where it proves to be right to support directly and to inform their thinking and operations – but at a minimum, where it is wrong, to frame increasing accuracy and precision in our approach to warfighting in the cyber domain.

Dave Yarker
Colonel
Director Cyber Force Development

JDN 2017-02
 (PROMULGATION DRAFT)

Preface

Application

01. Policy is prescriptive as represented by Defence Administrative Orders and Directives (DAOD). Doctrine is not policy; however, it provides authoritative and proven guidance, which can be adapted to suit each unique situation.
02. Canadian Forces joint publications (CFJPs) represent authorized joint doctrine for the guidance of Canadian Armed Forces (CAF) operations. The joint doctrine note (JDN) for cyber operations takes, at its foundation, the *Integrated Capstone Concept* (Ref. H) and the *CAF Cyber Operations Primer* (Ref. L) as the logical precursors to definitive CAF cyber doctrine.
03. The guidance in this publication is authoritative; as such, **the mature elements of this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise.** It provides the doctrinal guidance for commanders and staff at all levels of command and applies to all Department of National Defence (DND)/CAF conducting or supporting cyber operations. **If conflicts arise between the contents of this publication and the contents of service publications, this publication will take precedence unless the Chief of the Defence Staff (CDS) has provided more current and specific guidance.** Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures that have been ratified by Canada. For doctrine or procedures that have not been ratified by Canada, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with Canadian law, Canada's international legal obligations, regulations, and doctrine.

Purpose

04. The aim of this JDN is to define key terminology and concepts¹ required to operationalize the fundamental principles of cyber operations as a distinct operational domain that will govern cyber operations within the DND/CAF. This iteration of the JDN is intended to engage DND/CAF cyber operations stakeholders to establish norms of comprehension and application such that cyber operations across the CAF are comprehensive, integrated, adaptive, and networked in collaboration with our government partners and allies. **Where possible, cyber operations doctrine will remain at the unclassified level, with classified material included in annexes.**
05. This JDN is based on current practices, concepts,² studies, and lessons learned from the joint strategic, operational, and tactical levels of our own forces and those of the Five Eyes community. The DND/CAF understanding of the cyber domain and cyber operations is evolving at a rapid rate, thus it was decided that the JDN would be published as an iterative document to allow for ongoing development while providing updated guidance to our cyber forces. As a new domain of warfare, the CAF are 'learning

¹ Key terminology will be aligned primarily with Five Eyes terminology and definitions, and should differ only where required by Canadian law, policy, and/or regulations.

² DND Service Paper. *A Concept for CAF Cyber Operations*; LCol D.R. Yarker, CFLO to USCYBERCOM; 16 Apr 2015.

JDN 2017-02
 (PROMULGATION DRAFT)

by doing' and this JDN will embrace this approach where best practices will evolve and mature into normalized operations. This approach to JDN development ensures that the entire CAF are moving in the same direction and have a consistent understanding of CAF cyber operations. Thus, if content needs to change as a result of policy, legislation and/or operational experience, the entire CAF can collectively shift their awareness and understanding accordingly. This will ensure that the developing cyber force has the initial doctrine required to define and establish their organizations, doctrine, processes and procedures for cyber operations such that they are consistent across the CAF.

How to Read and Interpret the JDN

06. Given the operational need to develop and publish cyber operations doctrine, it is a necessary requirement to develop that doctrine concurrent to our cyber forces gaining experience and best practices. As such, the JDN is a living document where the maturity of each section/topic will vary, noting that some of the content is also leaning forward to where cyber forces and cyber operations will be in the near future. The ability to lean forward is made possible by leveraging from the experience of our allies and from the tremendous work of our current cyber forces that are 'learning by doing'. This JDN is also influenced by scientific and academic studies included in the reference section of this JDN. If readers note the absence of specific references that should be considered in future iterations of the JDN, they are encouraged to provide those details to the custodian.

07. Each chapter will be structured as follows:

- a. **General** – An overview of what will be discussed in the chapter.
- b. **Key terms** – All new terms and key cyber terminology used in each chapter will be captured in this section. These terms will also be represented in the glossary that also includes the terms and definitions used by our allies and government partners.
- c. **Discussion** – This section will contain the content of the chapter.

08. The JDN will conclude with a final chapter on challenges and next steps. The purpose of this chapter is to illustrate some areas in which there are ongoing issues or inconsistencies that require time, additional research, and/or additional experience. This chapter is included to clarify and/or highlight gaps and/or lack of depth in certain areas of the JDN. It is important for commanders and their staff to appreciate these challenges as these areas will likely pose challenges in the planning and execution of cyber operations. Thus, as commanders and staff encounter some of these challenges, they should consult with the cyber component commander and the legal advisers. It is also recommended that any lessons observed and learned be passed to the custodian of this JDN for consideration. Once the challenges and next steps have been addressed through experience and validation, it is expected that the JDN will become formal doctrine.

09. To facilitate the understanding and application of this JDN, the maturity level of the content of each paragraph is identified as:

- a. **Mature.** Areas that reflect current processes, activities and operations. These sections should be considered as final.

JDN 2017-02
(PROMULGATION DRAFT)

- b. **Developing.** Areas that are still evolving and/or are subject to formal studies or development. These sections should serve as good indicators of where the doctrine is going noting that stakeholders will be involved in further development.
 - c. **Conceptual.** Areas that are still at the idea stage where options are still being considered. They are provided to illustrate where the doctrine may be going and to provide stakeholders with an opportunity to shape or influence potential developmental activities and/or the concepts themselves.
10. While the practice of identifying the maturity of the content is not common practice for doctrine, there is an immediate need to publish doctrine to:
- a. Ensure consistency of understanding across the CAF, partners and allies;
 - b. Provide guidance to commanders and staff for the conduct of cyber operations, and more specifically, to provide guidance on how cyber operations compare to and fit into joint operations to include operations planning process (OPP) and joint targeting processes; and
 - c. Provide the necessary guidance to DND/CAF organizations to enable the development of their organizations, structures, and procedures to support and/or conduct cyber operations.

Relationship to Joint Doctrine

11. Cyber operations must be viewed within the context of joint operations, and therefore the joint doctrine note (JDN) for cyber operations should be read in conjunction with the following joint publications:
- a. CFJP 01, *Canadian Military Doctrine* (Ref. N);
 - b. CFJP 2-0, *Intelligence* (Ref. O);
 - c. CFJP 2-1.1, *Intelligence Preparation of the Operational Environment* (Ref. P);
 - d. CFJP 2-7, *Joint Intelligence, Surveillance, and Reconnaissance* (Ref. Q);
 - e. CFJP 3-0, *Operations* (Ref. R);
 - f. CFJP 3-0.1, *The Law of Armed Conflict at the Operational and Tactical Levels* (Ref. S);
 - g. CFJP 3-9, *Targeting* (Ref. T);
 - h. CFJP 3-10, *Information Operations* (Ref. U);
 - i. CFJP 5-0, *The Canadian Forces Operational Planning Process* (Ref. V);
 - j. CFJP 5-1, *Use of Force for CF Operations* (Ref. W); and
 - k. JDN 03-2014, *Operations Security* (Ref. AB).

JDN 2017-02
(PROMULGATION DRAFT)

This page was intentionally left blank

JDN 2017-02
(PROMULGATION DRAFT)

Table of Contents

Foreword iii

Preface..... v

Chapter 1 – General

Introduction 1-1

Cyber Defence 1-2

Cyber Security 1-4

Allied Approaches to Cyberspace 1-6

Chapter 2 – Cyber Domain Fundamentals

Introduction 2-1

Key Terminology 2-1

The Cyber Domain 2-2

The Core Attributes of Cyberspace 2-5

Chapter 3 – A Domain for Military Action

Introduction 3-1

Key Terminology 3-1

Characteristics of the Cyber Domain 3-2

Taxonomy of Cyber Actions in a Military Context 3-7

CAF Approach to Cyber Solutions: Comprehensive, Integrated, Adaptive, and Networked 3-15

Chapter 4 – Defining Cyber Operations

Introduction 4-1

Key Terminology 4-2

Cyber Operations 4-3

JDN 2017-02
(PROMULGATION DRAFT)

Support Cyber Operations4-11
 Network Operations4-14

Situational Awareness4-17

Partnerships4-19

Chapter 5 – Cyber in the Operational Environment

Introduction5-1
 Key Terminology5-1

The Cyber Area of Operations5-6
 Control and Coordination of Resources5-6
 Risk Assessment.....5-7

Freedom of Action5-12
 Concentration of Force5-13

JDN 2017-02
(PROMULGATION DRAFT)

Operations Planning Process (OPP).....5-15
 Cyber Operations – Effects in the Operational Environment5-15
 Authorities5-17

Intelligence Requirements.....5-18
 Intelligence Support to Cyber Operations.....5-20
 Intelligence Gain/Loss (IGL)5-20

Areas of operations (AOs).....5-24
 Legal Considerations.....5-25

Chapter 6 – Command and Control of Cyber Operations

Introduction6-1

Chapter 7 – Challenges and Next Steps

Introduction7-1
 Policy and Doctrine7-1
 Characteristics of the Cyber Domain7-2

JDN 2017-02
(PROMULGATION DRAFT)

Glossary GL-1

List of Abbreviations LA-1

List of References..... REF-1

Figures and Tables

Figure 2-1. The Cyber Domain.2-2

Figure 3-1. Taxonomy of Cyber Actions Taken Against DND/CAF.3-9

Figure 4-1. Defending Beyond the Network.....4-2

Figure 4-2. Functional Overview of the Cyber Domain.4-12

Table 4-1. Network Operations v Cyber Operations.....4-13

JDN 2017-02
 (PROMULGATION DRAFT)

Chapter 1 General

Cyber power mirrors biology's 'punctuated equilibrium'—long periods of stability separated by short periods of rapid change, occasional plateaus of constancy between which everything changes. What may be happening now, however, is an increase in the frequency of oscillation to the point where plateaus of constancy do not last long enough to consolidate cyber policy.

— CSIS 2018 Security Outlook ³

Introduction

0101. [MATURE] The *Future Security Environment* (FSE) (Ref. AA) provides a baseline view of current and emerging geopolitical, economic, environmental, social, science and technology, and military trends through to 2040. The FSE concludes that a significant cyber dimension must be considered from both a security and defence perspective. Informed by the FSE, Canadian defence strategy explicitly states that “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.”⁴

0102. [MATURE] With a myriad of cyber threats, which include insiders, hackers, criminals, State and non-State actors and foreign militaries, today’s militaries are faced with persistent and daily challenges that threaten freedom of action within and through cyberspace. Where computers, networked systems, the associated data and repositories enable the full range of military capability that include situational awareness, effective command and control (C2), mission planning, synchronized effects, logistical services, business, and administrative support, cyberspace has become both a vital enabler and a significant vulnerability for the CAF, at home and abroad. Beyond traditional network and information technology systems, cyberspace is also critical to the delivery of many operational effects through the embedded controllers that run nearly all platform, weapon, and soldier system. There is no question, therefore, that the Department of National Defence (DND)/Canadian Armed Forces (CAF) freedom of action within the cyber domain is a critical operational requirement that all personnel, at tactical through strategic levels, must embrace in the planning and execution of operations.

0103. [MATURE] Historically, the design of components, equipment, and systems favoured the inclusion of broadly useful software features whose focus was efficiency over resilience. Thus, the architecture and instrumentation of these components, equipment, and systems are primarily the result of service provisioning vice defensibility and are inadequate to detect and respond to adversarial activities. Adversarial cyber operations are posing significant threats to allied missions in or through cyberspace where adversaries are able to deny or manipulate operational capabilities, conduct rapid and sustained intelligence collection, and conduct deception activities. The operational challenge, therefore, is to ensure the CAF’s freedom of action within cyberspace by defending CAF capabilities in support of military objectives.

³ CSIS 2018 Security Outlook: Potential Risks and Threats (Ref. AH), p. 80.

⁴ *Canada First Defence Strategy* (Ref. D).

JDN 2017-02
 (PROMULGATION DRAFT)

0104. [MATURE] CAF defensive cyber forces are currently engaged in countering adversarial actions in cyberspace 24 hours per day, 365 days per year. This responsive posture must be maintained in the face of what will certainly be an increasingly relentless cyber threat environment. As noted earlier, traditional network operations/network defence must shift from the historic practice of information assurance and what was known as computer network defence to that of mission assurance that considers weapon, platform, and soldier systems. This new focus requires the CAF to develop, generate, sustain, and employ cyber forces in support of military objectives.

Cyber Defence

0105. [MATURE] It is important to distinguish and understand the strategic difference between security and defence within the cyber domain. This distinction is vital to understanding and defining cyber operations and the associated cyber forces. In the cyber context, national and international documentation (military and civilian) often use the words security and defence interchangeably. For the sake of clarity within this joint doctrine note (JDN), cyber defence pertains to the defence mandate of DND/CAF. Strategically, cyber defence refers to military operations that are conducted in the cyber domain in support of military objectives, equivalent to sea, land, air, and space operations. To help understand the practical difference between cyber security and cyber defence, is to recognize that cyber defence requires a shift from network assurance (security) to mission assurance,⁵ where cyber defence is focused on the continuity of military operations whereas network assurance is focused on network availability and data confidentiality and integrity. Cyber defence focuses on sensing, detecting, orienting, and engaging adversaries to outmanoeuvre them and assist commanders in completing their missions successfully. This shift from security to defence requires a strong emphasis on intelligence, surveillance and reconnaissance, and the integration of staff activities to include intelligence, operations, communications, and planning.

0106. [MATURE] As depicted in Figure 1-1, cyber operations are enemy-focused and founded on intelligence, protection, sustainment, fires, movement and manoeuvre, and C2. This military cyber operations capability is founded on effective operational, physical and network security in all phases of building, configuring, operating and maintaining DND/CAF cyberspace. This is no different than that of the traditional domains⁶ where operations are founded, if not dependent, on the effectiveness of underlying security practices such as force protection, perimeter lighting, hardening of equipment, and operations security (OPSEC).

⁵ The *MITRE Systems Engineering Guide* (Ref. BW) defines cyber mission assurance as “a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan...to sustain...operations throughout the continuum of operations.” It is executed through a “risk management program that seeks to ensure the availability of networked assets critical to department or agency missions. Risk management activities include the identification, assessment, and security enhancement of assets essential for executing national strategy.” Cyber mission assurance focuses on threats resulting from our nation’s extreme reliance on information technology.

⁶ The traditional domains are: maritime, land, air, and space.

JDN 2017-02
(PROMULGATION DRAFT)

0107. [MATURE] In June 2013, the Chief of Defence Staff (CDS) directed that the CAF “initiate the development of the cyber force required to conduct operations in the cyber domain, as it does in the land, sea, air, and space domains, to best support all *Canada First Defence Strategy* (Ref. D) mission areas.”⁷ The CAF authority to conduct cyber operations rests primarily on the exercise of the Crown prerogative and derives from the CAF authority to conduct mandated defence activities and operations approved by

⁷CDS guidance to the CAF (Ref. J).

JDN 2017-02
(PROMULGATION DRAFT)

the Government of Canada (GC)⁸. This authority is conditional on two criteria.

0108. [MATURE] The CDS is accountable to the MND for the control and administration of the CAF, which includes the conduct of cyber operations. Military cyber operations will be performed by specially selected and highly trained personnel who are equipped with the required technical tools and infrastructure. The conduct of these activities will be integrated with the delivery of other military effects, and fully coordinated with partners and allies. Collaboration, both nationally and internationally, will be critical as we move forward to define norms of behaviour and confirm how international laws, to include the law of armed conflict, apply to cyber operations.

Cyber Security

0109. [MATURE] Security sets the foundations for effective defence and has the primary responsibility for shaping the terrain to provide mission assurance across a broad threat base. For example, security can be in the form of physical security, personnel security, operational security, and cyber security, where cyber security refers to the ongoing provision of service and support for the day-to-day use of cyberspace for day to day business such as sending emails, using network-based applications and collaborating. Cyber security is based on industry best practices. The Assistant Deputy Minister (Information Management) (ADM[IM]) has the primary responsibility for ensuring cyber security for DND/CAF managed information technology systems and provides the linkage to Shared Services Canada (SSC) for information technology systems they are responsible for. The delivery of these cyber security services by ADM(IM), Assistant Deputy Minister (Materiel) (ADM[MAT]), Communications Security Establishment (CSE) and SSC provide the security backbone that protects the DND/CAF cyber domain.

0110. [MATURE] Supporting the foundation for effective defence, ADM(Mat), the Services and the other Level 1 organizations also play a critical role in defining, establishing, and maintaining cyber security measures and activities within their mandates and their platform and weapon systems. This critical role has been recognized and is one of the catalysts for the development of a DND/CAF mission assurance program that will include the development of a platform protection program.¹⁰

⁸ *Interim DND/CAF Policy on CAF Computer Network Operations* (Ref. F) establishes the framework for the development and conduct of cyber operations for the CAF. A new CAF cyber operations policy is being finalized at the time of publication of this JDN, which will replace this interim policy.

¹⁰ *DM/CDS Initiating Directive for Cyber Mission Assurance Program Development* (Ref. G) was signed on 17 Jan 2017. Cyber operations doctrine will need to incorporate the work developed as part of the Cyber Mission Assurance Program,

JDN 2017-02
 (PROMULGATION DRAFT)

0111. [MATURE] *Canada's Cyber Security Strategy* (Ref. A),¹¹ coordinated by Public Safety Canada, focuses on three pillars: securing Government of Canada systems; partnering to secure vital cyber systems outside of the federal government; and helping Canadians to be secure online. **The Strategy outlines a number of roles for the DND/CAF including the requirement to:**

- a. **strengthen the ability to defend DND/CAF networks;**
- b. **work with other government departments and agencies (OGDA) to identify cyber threats to Canada and possible responses; and,**
- c. **work with allies to exchange best practices and to establish the policy and legal frameworks for military aspects of cyber security.**

0112. [MATURE] *Canada's Cyber Security Strategy* (Ref. A) identifies seven government departments and agencies that have, as summarized below, key roles in cyber security. While the interrelationships at the strategic and operational levels are continually evolving, it is essential that commanders and staff have a basic understanding of the roles and responsibilities of the key departments and agencies to ensure that CAF cyber operations are comprehensive, integrated, adaptive, and networked.

- a. **Public Safety Canada (PSC).** PSC leads the coordination of Government's efforts to protect Canada's critical infrastructure and Canadians, including both physical and cyber dimensions, and is responsible for cyber emergency management. In collaboration with its federal, domestic, and international security partners, PSC:
 - (1) coordinates an integrated national strategic approach to cyber security and
 - (2) coordinates, through the Canadian Cyber Incident Response Centre (CCIRC) and, where required by the GC, the national response to cyber events of national interest.
- b. **Shared Services Canada (SSC).** SSC provides and protects the GC's information technology (IT) infrastructures under its mandate, to ensure the confidentiality, integrity, and availability of the information within these cyber systems and networks. **SSC, through the Security Operations Centre (SOC), provides the focal point for the coordination of cyber incident and threat detection, monitoring, containment/mitigation, and cyber incident response and recovery services, in collaboration with security partners, for SSC controlled systems and networks.** The role of the GC Critical Incident Response Team (CIRT), within SSC, is to coordinate the identification, mitigation, recovery, and post-analysis of IT incident with the GC.
- c. **Canadian Security Intelligence Service (CSIS).** CSIS collects information, assesses threats, produces intelligence, and advises the Government concerning activities that may constitute a threat to the security of Canada, including cyber security. **CSIS national security cyber investigations include cyber espionage, cyber terrorism, and threats to the IT supply chain.** The investigations are conducted in collaboration with domestic and international partners to determine attribution, motivations, and capabilities of the threat actors. CSIS is also mandated

¹¹ This strategy is currently under review and anticipated changes will likely influence future iterations of this JDN.

JDN 2017-02
 (PROMULGATION DRAFT)

- to undertake operational measures pursuant to s. 12.1 of the *CSIS Act* to reduce a threat, including the threat posed by cyber attacks, as defined in s.2 of the Act.
- d. **Communications Security Establishment (CSE).** CSE provides foreign signals intelligence from the global information infrastructure in collaboration with domestic and international partners. CSE provides advice, guidance, and services to help ensure the protection of electronic information and information infrastructures of importance to the Government. CSE provides technical and operational assistance, as required and appropriate, to federal law-enforcement and security agencies.
 - e. **Royal Canadian Mounted Police (RCMP).** The RCMP conducts and coordinates criminal intelligence gathering, crime prevention, disruption, and criminal investigations, including disruption of domestic and international cybercrimes.
 - f. **Canadian Radio-television and Telecommunications Commission (CRTC).** As the administrative tribunal that regulates and supervises telecommunications in Canada, the CRTC, conducts and may coordinate investigations with partners to enforce compliance with laws and may impose administrative monetary penalties relating to telecommunications, commercial electronic messages and other cyber technologies. The Spam Reporting Centre (SRC), under the CRTC, collects e-messaging reports and complaints.
 - g. **DND/CAF.** The DND and the CAF conduct operations within their networks to detect, defeat, and/or mitigate offensive and exploitive actions. DND/CAF collect intelligence on cyber threats to DND/CAF and regarding military cyber threats to the nation, including in support of GC-authorized military missions. **DND/CAF provide all-source intelligence assessments and analysis to the GC on cyber threats to DND/CAF and military cyber threats to the nation. DND/CAF provide advice and analysis to the GC on interventions against cyber risks, threats, events, and incidents. DND/CAF contributes to joint cyber security efforts with allied military organizations.**

Allied Approaches to Cyberspace

[...] nowadays almost all acts of physical violence come with an online component, exploiting social networks to manipulate opinion and perception. The tactics employed by Russia in Ukraine, Estonia and Georgia, include combinations of information warfare, cyber activity, counter-intelligence, espionage, economic warfare and the sponsorship of proxies. [...] Terrorism, Hybrid War, Compound threats and War in the Information Age need sophisticated all-of-government approaches [...] we cannot face these threats alone. The importance of achieving collective security through alliances is vital to any enterprise that needs to be conducted at scale. It is also vital to our ability to manage risk in a context in which we simply cannot afford a national inventory to face all threats.

— General Sir Nicholas Houghton¹²

0113. [MATURE] Our allies have publicly declared the need for strategic alignment and interoperability of cyber operations. To ensure consistency and alignment with them, **Canadian doctrine will be informed by,**

¹² General Sir Nicholas Houghton gives his personal views ahead of the 2015 Strategic Defense and Security Review. “Building a British military fit for future challenges rather than past conflicts.” (Ref. BR).

JDN 2017-02
(PROMULGATION DRAFT)

in order of priority, US, Five Eyes, and NATO doctrine, unless deviation is required due to Canadian law, Canada's international legal obligations, national policy, regulations, and/or operations.

0114. [MATURE] All Five Eyes nations have recognized the strategic importance of cyberspace and are aggressively developing cyber defence strategies, policies, doctrine, operations, and capabilities. All the Five Eyes strategic policies call for strong collaboration among the partners.

JDN 2017-02
(PROMULGATION DRAFT)

This page was intentionally left blank

JDN 2017-02
(PROMULGATION DRAFT)

Chapter 2 Cyber Domain Fundamentals

The Internet was designed to be collaborative, rapidly expandable, and easily adaptable to technological innovation. Information flow took precedence over content integrity; identity authentication was less important than connectivity. The Internet's original designers could not have imagined the extent of its vital and growing role...the global scope of networks and systems presents adversaries with broad opportunities for exploitation and attack.

— US DoD Strategy for Operating in Cyberspace¹⁵

Introduction

0201. [MATURE] Cyberspace, unlike the environments of sea, land, air, and space, is man-made and omnipresent within all other environments. **Although not exclusively a military domain, cyberspace is a multinational, joint, and integrated operational environment that enables CAF operations.** A critical enabler to a network-centric CAF, this operational environment overlaps the traditional maritime, land, air, and space domains, presenting significant vulnerabilities that can have catastrophic effects on operations. **It is essential that personnel understand cyberspace and the cyber domain, the potential threats and effects, and how the CAF will defend this operational environment, for the CAF to be successful in operations.**

0202. [MATURE] This chapter will illustrate the complex structure of the cyber domain and cyberspace using an information environment model utilized in various forms by our allies. This model was chosen because the information environment and the cyber domain are both interdependent and complementary. With the cyber domain defined, this chapter will introduce the core attributes of cyberspace that make operating in cyberspace such a complex challenge; providing both opportunities and vulnerabilities for threat actors to create a myriad of desired effects in or through cyberspace.

Key Terminology

0203. [MATURE] The following key terminology is introduced in this chapter:

- a. **Cyber domain.** “All infrastructure, entities, users and activities related to, or affecting, cyberspace.”¹⁶
- b. **Cyberspace.** “The element of the operational environment that consists of interdependent networks of information technology structures-including the Internet, telecommunications networks, computer systems, embedded processors and controllers-as well as the software and data that reside within them.”¹⁷

¹⁵ US DoD Strategy for Operating in Cyberspace (Ref. AP), p. 2.

¹⁶ DTB record 694360.

¹⁷ DTB record 694338.

JDN 2017-02
 (PROMULGATION DRAFT)

- c. **Cyber operation.** "An operation whose primary purpose is to achieve an objective in or through the cyber domain. Cyber operations consist of offensive cyber operations, defensive cyber operations and support cyber operations."¹⁸

The Cyber Domain

0204. [MATURE] CAF doctrine proposes that the cyber domain represents all factors that influence operations in cyberspace, to include the people (users) and infrastructure, much like the definitions of the maritime, land, air, and space domains. Cyberspace, on the other hand, represents an element of the cyber domain and represents the medium in or through which cyber operations take place, much like the ocean, land, and air, and space are the medium on or in which the other components operate. This complex concept is illustrated in a five layer model in Figure 2-1. Canada's primary allies use similar five layer models, noting that some models include a sixth layer, called a social layer. Canadian doctrine considers the social layer as part of the persona layer.

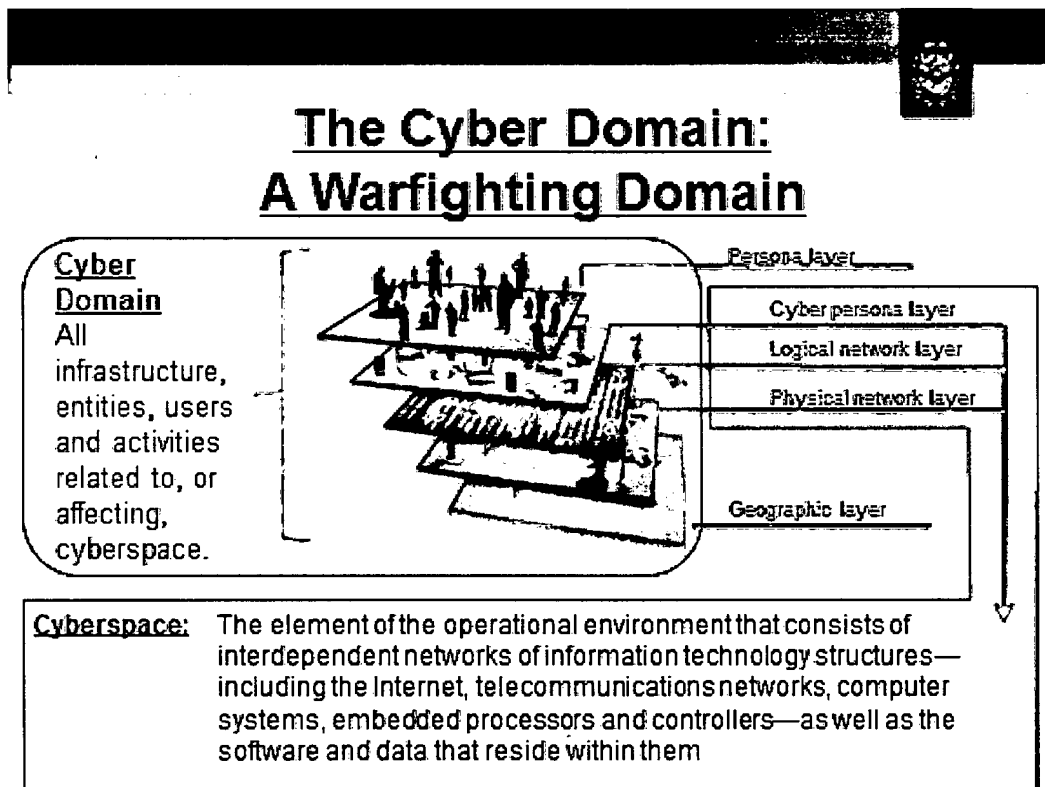


Figure 2-1. The Cyber Domain.

¹⁸ DTB record 694442.

JDN 2017-02
 (PROMULGATION DRAFT)

0205. [MATURE] This model can be used effectively to describe the cyber domain¹⁹ where the multiple layers help illustrate the complexities and interdependencies within and across these layers. Each of the layers is described as follows from bottom to top:

- a. **Geographical layer.** The geographical layer represents the physical location of elements of the network. The geographic location of physical items helps to give context to applicable laws and policies that apply to the cyber domain. It can also represent the geographic location of attack vectors (e.g. USB sticks containing malware), risk from natural threats (e.g. solar flares, earthquakes, and flooding) that can affect both the people and technology in those areas. Conflict within cyberspace may be linked across large geographical distances, thereby reducing the importance of physical separation. While geopolitical boundaries can easily be crossed in cyberspace at a rate approaching the speed of light, there is still a physical aspect tied to the other domains. Actions within cyberspace can have intended or unintended global, regional, or local effects. Cyberspace provides individual users with unprecedented access to key audiences and critical targets within the cyber domain.
- b. **Physical network layer.** The physical network layer is the foundation of cyberspace and is the easiest layer to grasp as it is both tangible and physical and exists in a specific location. It is composed of physical devices that include the hardware, personal computers and servers, supercomputers and grids, sensors and transducers, networks, communication channels, and storage devices. These devices can be wired, wireless, satellite, or optical. It also includes the physical connections such as wires, cables, radio frequency, routers, and switches. The network physical layer is considered the primary target for network intelligence gathering and exploitation through such means as theft, bypassing locks, cloning magnetic strip cards, physical destruction, and insertion of malicious code via counterfeit hardware or components. The physical network layer is the first point of reference for determining jurisdiction and application of authorities.
- c. **Logical network layer.** The logical network layer is known as the information layer in some allied doctrine. It consists of the logical connections that exist between network nodes (devices connected to a computer network). Nodes can be computers, personal digital assistants, cell phones, or various other network appliances. On an Internet protocol (IP) network, a node is any device with an IP address. Examples of the logical network layer include software applications (browsers, office products, etc.), operating systems (Windows, Unix, Android, iOS, etc.), machine language, communication ports, and protocols. Some examples of attack patterns within the logical network layer include the harvesting of usernames and user IDs, scanning of networks for vulnerable software, and distributed denial of service (DDoS) attacks.

¹⁹ One of the challenges in defining strategy, policy, and doctrine for cyber operations is the lack of consistent terminology within the international community. Numerous research papers articulate the inconsistent and interchangeable use of multiple terms between nations, and sometimes, within doctrinal or policy documents themselves. As an example, most allies use a similar model to that illustrated here, but the 'layers' are called dimensions and/or domains. Similarly, names of the layers (dimensions and/or domains) vary slightly by country/doctrine. However, their associated definitions and intent are all relatively consistent. Thus, regardless of which model is used, the overall applications are consistent.

JDN 2017-02
 (PROMULGATION DRAFT)

- d. **Cyber persona layer.** The cyber persona layer is used to represent the various ways that people can be represented in cyberspace such as **user accounts, user IDs, email accounts, web pages, and telephone numbers**. Any one individual may have multiple cyber-personas (for example, different email accounts and accounts on different computers), which is a common tactic used by threat actors to better hide themselves. Similarly, a single cyber persona can have multiple users. Cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, thus **significant intelligence collection and analysis capabilities are required for the joint forces to gain sufficient insight and situational awareness of a cyber persona to enable effective targeting and the creation of desired effects**. Consequently, attribution of any specific network event is a complex task that may lead to situational awareness expressed in degrees of confidence.
- e. **Persona layer.** The persona layer simply refers to the people (individual and social groups) that interpret and exploit the environment. **The persona layer comprises the individuals who, in the end, are responsible for the outcomes in the cyber domain**. Individuals have more power to cause effects than ever before through such means as social media that can have a lasting influence on behaviour of state leaders. Attack patterns in the persona layer can include social information gathering, target influencing via social engineering, the manipulation of system users, deception, and phishing.²⁰

0206. [MATURE] The original design of cyberspace rested on the assumption that actors in this space would conform to positive norms of behaviour. Security was not an integral part of the design. Though many have abandoned this assumption, the extant security design gaps create long-lasting implications for cyber operations. The resultant architecture of cyberspace creates an inherent ability to operate covertly and/or anonymously, or to masquerade as another actor. It is simple to manoeuvre through cyberspace while masking one's identity. It is also possible for multiple actors to operate within the same areas of cyberspace without necessarily observing each other or interacting directly. Military operations in the cyber domain must therefore consider all five layers and their interdependencies. As an example, an attack can take place at any of the given layers. The physical hardware can be destroyed, lost, or stolen; the logical network layer can be corrupted by a virus; the cyber persona layer can be compromised or corrupted through espionage; and people can be corrupted, coerced, or tricked (e.g. spear phishing²¹ email). While there are constant efforts to improve the resilience of systems, systems development practice has not drastically decreased the degree of system vulnerability. Vast defensive gaps, avenues of approach, and manoeuvre space will continue to exist. As such, **an understanding and awareness of cyberspace and the cyber domain within the operational environment is required, especially given that the enemy always has a say. The CAF must always stay ahead of the adversary, recognizing both the opportunities and vulnerabilities that this architecture presents.**

²⁰ [The use of] "falsified" e-mails to lead consumers to counterfeit Web sites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. *TermiumPlus* (Ref. AI)

²¹ "A phishing attack that focuses on a single user or department within an organization, addressed [apparently] from someone within the company in a position of trust and requesting information such as login IDs and passwords." *TermiumPlus* (Ref. AI)

JDN 2017-02
(PROMULGATION DRAFT)**The Core Attributes of Cyberspace**

0207. [MATURE] Cyberspace exists within the cyber domain and, consistent with its definition, is represented as the middle three layers of the cyber domain: the physical network layer, the logical network layer, and the cyber persona layer as depicted in Figure 2-1. Notionally, cyberspace represents the medium (terrain) in or through which cyber operations take place. Unlike the traditional domains where the ‘terrain’ is relatively constant and defined, cyberspace (a man-made terrain) is drastically different as depicted by the following three attributes:

- a. **Continuous and rapid change.** The pace of change within cyberspace demands highly educated²² and highly trained forces capable of maintaining situational awareness in a domain that is both continuously changing and evolving. Referring to the five layers of the cyber domain, an almost limitless number of changes can take place on any given layer that can have immediate, secondary, and third-order effects on the other layers. Unlike any other environment, effects can be realized across the entire environment or, in a physical sense, globally within a matter of seconds. This speed and range of reach can provide for near immediate operational effects, requiring an agile, robust, and swift acting adversary to effectively survive or counteract. **Due to the potential for third- or higher-order unintended effects, the short range between tactical to strategic effects, and the speed in which such effects can be achieved, there are a number of legal challenges that must be considered with any cyber operation.**
- b. **Convergence.** The *Oxford English Dictionary* (Ref. BX) defines convergence as “coming closer together.” Convergence is a core attribute of the cyber domain given the rapid and revolutionary pace at which the integration and merging of capabilities is realized and/or enabled within the cyber domain. “Cyberspace, at the logical level, is thus a series of platforms, on each of which new capabilities are constructed which in turn become a platform for the next innovation.”²³ As new platforms or capabilities are created in the physical and/or logical network layers, they are directly linked to the persona layer. As history has proven, cyber-related technologies can be exploited in ways not intended or envisioned by the developers. These innovations are creating convergences across and within the layers of the cyber domain and military forces are struggling to keep up with these rapid innovative changes that create both opportunities and vulnerabilities. For example:
 - (1) Many technologies have merged many capabilities into a single device or systems such as smart phones or control systems that now allow us to do many things on one device/system.

²² Highly educated infers specialized education. This can be high school with a heavy focus on math, college, and university programs focused on math, computer, or cyber specialties. **Work is progressing with the development and definition of the new CAF cyber operator trade where the specific educational requirements will be determined. Future work will be required for officer level education requirements.** “The purpose of **training** is to instill the knowledge, skills, and attitudes required to carry out specific tasks, while that of **education** is to lay down a base of knowledge and intellectual skills that can support the learner in interpreting information effectively and exercising judgment.” Maj Julie Maillé and Louise Baillargeon, “A Doctrine for Individual Training and Education” (Ref. AC).

²³ David Clark, “Characterizing cyberspace: past, present and future” (Ref. BN).

JDN 2017-02
(PROMULGATION DRAFT)

- (2) The evolution of control systems for weapon and platform systems is forcing the CAF to reconsider and redefine how network-enabled operations are conducted.
 - (3) Internet and social media have evolved from communication tools to social destinations, thereby having a direct impact on how information, influence activities and intelligence operations are conducted.
 - (4) Societal practices and expectations for privacy have changed in terms of how and to whom personal information is shared. As an example, with the advent of social media, people place significantly more personal information in the public domain than they would have even 20 years ago. This has affected basic security and, more importantly, OPSEC.
 - (5) Applications that are combined to create more complex services (such as the combination of word processors, databases, and the Web) allow dynamic content generation. Services such as Facebook are becoming launch pads for the development of new applications.
- c. **Vastness of information.** Probably the easiest attribute to accept and understand is that cyberspace holds a vast amount of information. Information in cyberspace includes music, videos, photos, data, and metadata. Data and information can be static, such as records, or dynamic, which is a combination of storage and computation. The vastness of information is creating issues of ownership, information management, authenticity, and dependability. While already vast, the amount of information is also increasing exponentially thereby increasing complexities and vulnerabilities within cyberspace. This has led Canada and its allies to recognize the inherent and unprecedented need for timely information sharing and collaboration to find, collate, analyze, and interpret that data and information in support of military operations. This requirement for information sharing and collaboration outside of the traditional military operations planning process (OPP) introduces a new layer of complexity in the planning and execution of military operations.

0208. [MATURE] The understanding of these three attributes should inform the development of policy, doctrine, and standard operating procedures and should also influence and inform military operations. The speed and rate of change, the evolution of tools, equipment, and systems that make use of, or form part of, cyberspace, and the incredible volume of information will continue to influence the operational environment.

JDN 2017-02
 (PROMULGATION DRAFT)

Chapter 3 A Domain for Military Action

The creation of cyberspace has simply offered another environment or domain within which to exercise the elements of national power...It is the integration of land, maritime, air, space, and cyberspace operations that achieves campaign objectives.

— Brett T. Williams²⁴

Introduction

0301. [MATURE] Canada, the US, NATO, most of our principal allies, and even our adversaries have recognized the cyber domain as an operational domain. As a new operational domain, the CAF must develop its cyber force and capabilities similar to that of the traditional operational domains. As such, the cyber domain requires the same functions of C2 to prepare, deploy, employ, and redeploy forces and capabilities in support of CAF objectives. A flexible, efficient, and responsive C2 of cyber capabilities must permit the delivery of comprehensive, operationally responsive, and decisive effects at the place and time of the commander's choosing. Operations within the cyber domain must be integrated, planned, and executed coherently within the DND/CAF, across OGDAs, and with our military allies and partners.

Defining the cyber domain as an operational domain is a critical organizing concept as it allows DND/CAF to organize, train, and equip themselves for cyber operations in the operational environment as we do in the maritime, land, air, and space domains, and is consistent with the national approaches of our allies.

Key Terminology

0302. The following key terminology is introduced in this chapter:

- a. **Cyber security event.** “The indication that a cyber vulnerability may exist, that a cyber threat may be planned or that a cyber security incident may have occurred, requiring analysis and a risk management decision to determine an appropriate course of action.”²⁵ Note this definition is too narrow in the military context as it does not consider military applications where events/incidents may not be limited to a computer network or system resource such as weapon, platform, or soldier systems. This gap is addressed in this chapter.
- b. **Cyber security incident.** “Any cyber security event (or collection of security events) or omission that results in the compromise for a GC IT system.”²⁶ Note this definition is too narrow in the military context as it does not consider military applications where events/incidents may not be limited to a computer network or system resource such as weapon, platform, or soldier systems. This gap is addressed in this chapter.

²⁴ Brett T. Williams, “The Joint Force Commanders’ Guide to Cyberspace Operations” (Ref. CK) p. 13.

²⁵ *The Government of Canada Cyber Security Event Management Plan* (Ref. C).

²⁶ *The Government of Canada Cyber Security Event Management Plan* (Ref. C).

JDN 2017-02
 (PROMULGATION DRAFT)

- c. **Significant cyber incident.** A cyber action in or through cyberspace, observable or not, that compromises or adversely impacts military operations or capabilities.
- d. **Cyber attack.**²⁷ A cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.²⁸
- e. **Cyber fire.** Cyber actions that seek to create first-order effects against a target’s capabilities. Note that fires include lethal and non-lethal means.²⁹
- f. **Intelligence, surveillance and reconnaissance (ISR).** “An activity that synchronizes and integrates the planning and operation of all collection capabilities with exploitation and processing to disseminate the resulting information to the right person, at the right time, in the right format, in direct support of current and future operations.”³⁰

Characteristics of the Cyber Domain

0303. [DEVELOPING] In comparison to other operating domains, the cyber domain holds several distinctive characteristics that can provide an operational advantage over a lesser capable adversary, but due to its ever-evolving man-made nature, requires exceptionally adaptable resources. The following examples illustrate the unique nature of the cyber domain as compared to the traditional operational domains:

- a. **Reach.** The cyber domain is pervasive and borderless, which enables both global and local operations.
- b. **Asymmetric effect.** An individual or relatively small organization with appropriate motivation, limited resources, and highly technical capability could conduct cyber actions resulting in a strategic and/or large-scale effect. By contrast, a State can also make use of cyber operations in an asymmetric fashion whereby the strategies and tactics of cyber operations are more representative of unconventional warfare where, for example, one of the actors can seize technological advantage over another.
- c. **Anonymity/attribution/deniability.** The process of attribution identifies the actor who conducted or sponsored a cyber action against another State, organization, or individual, and

²⁷ This is a conceptual definition taken from *Tallinn Manual 2.0* (Ref. BF) to illustrate the strategic need to clarify the term *cyber attack*. At present, a cyber attack is the term applied to any adversarial action within the cyber domain. However, it has become clear with the events such as the Sony attack in the US and the Russian actions in the Ukraine, that there is a need to define a cyber attack at the strategic level to clearly define when an attack on a State has risen to the level of an armed attack. Michael, Schmitt; “International Law and Cyber Attacks: Sony v. North Korea” (Ref. CB).

²⁸ Definition from Rule 92 of the Tallinn Manual 2.0. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Ref. BF), p. 415.

²⁹ Cyber fire is more commonly referred to as a cyber attack, however, an attack has a specific legal meaning in terms of LOAC and therefore not all cyber “attacks” constitute cyber attacks in the context of LOAC. Thus, the term **cyber fire is proposed with the intent of merging it (or a similar term) into allied lexicon and doctrine. The proposed definition has not gone through the rigour of review and is purely a starting point for discussion and is based on the land operations definition of attack provided in the DTB record 27514.**

³⁰ DTB record 30996.

JDN 2017-02
 (PROMULGATION DRAFT)

the intent behind it. Non-attributable attacks increase uncertainty and potentially reduce political risk and the opportunity for response. Attribution within cyberspace is difficult to prove and therefore provides actors with anonymity or plausible deniability.

d. **Timing.** There are two aspects to timing for cyber operations:

- (1) In cases where access, anonymity, collateral damage, or target complexity are not concerns, the preparation time for cyber operations can be relatively quick. Equally, the time can be long where these are important considerations.
- (2) The effects of cyber operations can be instantaneous, triggered, or purposely delayed. These lead to a potentially very high operational tempo and a constant state of change.

e. **Speed.** In the cyber domain, the offence has a distinct advantage over the defence with respect to speed,³¹ reach, and the potential for stealth, surprise, and anonymity. However, the effectiveness is largely a function of the offence's intelligence on the target system. Thus, intelligence must keep up with the speed at which cyberspace evolves, as even minor changes in cyberspace can adversely affect cyber operations capabilities, rendering them ineffective or marginalized. Thus, there are two aspects of speed that characterize cyber operations:

- (1) **Rapid effects.** An offensive action can have effects at multiple locations simultaneously by a small number of operations. In many cases, only a single attack has to be successful in one location to enable future operations.
- (2) **Long-term development cycle.** While cyber operations themselves can occur quickly, the intelligence and weapon development requirements can take a long period of time, thus cyber operators may not be able to shift focus on targets without substantial preparation.

f. **Versatility.** "Cyber weapons can have unparalleled versatility"³² in that they can be:

- (1) Used across the full range and phases of military operations to include shaping the environment through to destructive actions within or external to the cyber domain.
- (2) Reversible and/or tailored. Unlike munitions that are normally destroyed upon use, cyberspace activities can include code that can be saved, analyzed, and recoded. The capture, retooling, and reuse of cyber weapons are important concepts whereby cyber weapons can be used/reused by other actors. This characteristic can determine the degree to which services are affected. For example, an attack that prevents power from reaching a factory could be stopped, allowing the power to be restored and for the factory to resume working. Such reversible effects could reduce the amount of temporary collateral damage and therefore make cyber operations more politically and socially acceptable.

³¹ Most cyber attacks are complete within minutes or hours, during which the defence must first detect the attack and then respond to it. In many cases, the attack is complete before defensive actions can be effectively implemented.

³² Mauren Leed. "Offensive Cyber Capabilities at the Operational Level: The Way Ahead." (Ref. BU).

JDN 2017-02
(PROMULGATION DRAFT)

- (3) **One danger of versatility is the potential for an adversary to capture, analyze, and rapidly deploy a cyber effect for their own objectives.**
- g. **Complexity.** Cyber operations are complex operations in both a defensive and offensive context:
- (1) **Defensive.** Some of the significant challenges for defensive cyber capabilities include the detection, characterization of effects, identification of attack vectors and sources, and ultimately attribution. As an example, adversaries can apply tactics, operational art, and capabilities that can misattribute the event to another actor, thereby effectively masquerading offensive cyber activities or potentially remove any evidence that an offensive cyber activities occurred at all.
- (2) **Offensive.** Offensive cyber capabilities also face complex challenges in that they require considerable time, effort, and expertise to identify the terrain, vulnerabilities, and mission dependencies. As noted above, a change in cyberspace can adversely impact offensive cyber capabilities. For instance, **targeted systems with identifiable vulnerabilities are often transient, and the system could be patched or replaced prior to offensive cyber activities, rendering it ineffective. Commanders and planning staff must appreciate the long lead time required for offensive cyber activities.**
- h. **Terrain.** Cyberspace is the only domain in which the terrain is man-made. Like the other domains, it too is vast and complex. While changes can occur over time in the other domains, the rate of change in cyberspace is exponentially greater where terrain can be created, modified, replicated, or destroyed with relative ease. While software developers create cyber terrain to perform functions that have value in the physical world, the value of those functions is easy to manipulate, disable, or commandeer to perform unexpected functions, leading to unexpected effects and mission failures. As military weapons, systems, and equipment become more reliant on cyberspace, the cyber terrain and the corresponding manoeuver space are increasing in size and complexity. Thus, **as cyberspace grows, so does the likelihood of vulnerabilities, therefore increasing the potential number of targets for cyber operations. This rate of change, to include fixes to vulnerabilities, can render cyber capabilities ineffective or marginalized.**
- i. **Persistence.** Once initiated, software-driven processes can function autonomously on a 24/7 basis without human intervention, causing great damage with minimal efforts.
- j. **Cost.**
- (1) **For non-State adversaries.** While “military-grade” cyber capabilities remain too expensive for most malign actors, they can still have a low cost for entry where:
- (a) Malicious code (such as viruses) and training are readily available over the Internet at no cost.
- (b) Adversaries can develop, edit, and reuse previously created tools.
- (c) Inexpensive tools and training allow an adversary to compete with States without costly ships, tanks, aircraft, or missiles. Thus, adversaries can impose significant

JDN 2017-02
(PROMULGATION DRAFT)

financial burdens on nations that rely heavily on cyberspace by forcing them to invest in cyberspace defence.

(d) Relatively inexpensive services can be provided by professional hackers.

(2) **For States.** Compared to traditional weapon systems, developing new cyber tools can be just as costly to deliver, however, production and deployment costs for cyber weapons are minimal, as are the operations and maintenance costs.³³ Note that the weapon is only effective while vulnerabilities exist, after which time the weapon may become partially or fully useless. Thus, intelligence is pivotal to the development of cyber weapons, and the speed of development is of the essence. Additionally, our cost of development can be leveraged by an adversary to reuse a cyber operations tool for their own purposes once that tool is employed. However, the knowledge gain and lessons learned may still be of value where the knowledge gain may reduce the development costs by a significant margin for the next vulnerability. Beyond cyber tools and weapons, there are significant costs to develop, implement, and maintain relevant and effective cyber operations programs and capabilities.

k. **Distance.** In contrast to the maritime, land, air, and space domains, physical distance means very little in cyberspace where actions can be initiated anywhere in the world with near instantaneous effects anywhere within the cyber domain. The ability to copy information allows for information-based capabilities to be quickly shared and employed across the globe. This allows forces to quickly replicate and reuse software capabilities; tactics; techniques and procedures (TTP); and tradecraft anywhere across the globe. As an example, a signature identified by one State can enable other partners to protect their own systems through detection and mitigation measures for that signature.

l. **Unintentional cascading effects.** While cyberspace capabilities are developed and evaluated in computer labs

STUXNET

“a highly sophisticated worm with a very specific strategic goal”

In 2010, a computer worm called STUXNET was responsible for the destruction of a significant number of Iranian nuclear centrifuges. The worm was introduced by a USB flash drive which targeted industrial programmable logic controllers (PLC) using Microsoft Windows operating systems and networks. The worm propagated across target networks, looking for specific software and specific PLC. Once identified, the worm modified the code of the software and the PLC, leading to the destruction of the centrifuges. The modified code gave unexpected commands to the PLC while providing a returning loop of normal operating system values to the users, thus it took Iranian officials months to figure out why the centrifuges were failing. This worm is still active across the Internet and its effects are reshaping the security industry.

³³ Mauren Leed. “Offensive Cyber Capabilities at the Operational Level: The Way Ahead.” (Ref. BU).

JDN 2017-02
(PROMULGATION DRAFT)

- and cyberspace ranges, there can never be complete assurances as to how a capability will behave or where it might spread when introduced in the Internet. As an example, the STUXNET virus was intended for a single target; however, the virus is still resident in the global cyber domain and available for users to reverse engineer for the development of other weapons. Reusability and perishability of capabilities will influence the operational decision making of the offensive force. It is emphasized that cyber activities can have a lasting impact and can echo throughout the entire Internet.
- m. **Projection of power.** The integration of cyber operations into joint operations enables the projection of power around the world with unmatched precision, speed, and agility.
 - n. **Governance and legal challenges.** The cyber domain, associated legislation, roles, and responsibilities of government departments and agencies remain a key challenge for the GC.

JDN 2017-02
(PROMULGATION DRAFT)

Taxonomy of Cyber Actions in a Military Context

Neutral though it may be, “attack” is operatively a key threshold concept in international humanitarian law because many of its core prohibitions and restrictions apply only to acts qualifying as such.

— Michael N. Schmitt³⁴

0308. [MATURE] Recognizing that offensive cyber activities are increasing exponentially across the globe, the international community is struggling to keep up with policy and with clarifying the application of existing international law to cyber operations. Internationally, *cyber attack* has been used for any cyber action that has adverse effects on cyberspace. While the term *cyber attack* has proven adequate for non-legal use, it is proving difficult in the legal context, given that the term *attack* has a very specific meaning in the context of international law that govern State behaviour. The term *attack*, therefore has direct consequences on the legality of particular cyber action and the follow-on responses. This confusion and debate was most clearly illustrated

North Korea v SONY

In 2014, a cyber-attack was executed against Sony Pictures. The attack included the release of confidential data from Sony Pictures to include personal information, emails, and salaries amongst other confidential data in addition of the destruction of thousands of computers, forcing Sony to take their entire network off line. The United States attributed the attack to North Korea, noting that the hacker Group called “Guardians of the Peace” were the group responsible for leaking the information, demanding the retraction of the film *The Interview*. In January 2015, the Obama administration enacted additional sanctions against the North Korean government, citing the cyber-attack and ongoing North Korean policies. North Korea has officially denied involvement in the attack, though acknowledge that it may have been the work of supporters of their regime.

³⁴ Michael N. Schmitt. “*Attack as a Term of Art in International Law: The Cyber Operations Context.*” (Ref. CA).

JDN 2017-02
 (PROMULGATION DRAFT)

in the North Korean cyber actions against Sony³⁵ and again with the Russian actions in the Ukraine.³⁶ These two specific incidents drove the international community into action to better define what constitutes a *cyber attack* in the context of an armed attack in accordance with Article 51 of the UN Charter (Ref. BJ). **In a Canadian context, the term *cyber attack* can create legal and operational issues.³⁷ While the issue had been discussed previously, it became clear that *cyber attack* is not an appropriate overarching military term for any actor that conducts cyber actions that have or have the potential to create adverse effects on cyberspace.**

0309. [CONCEPT] From a legal perspective, the law of armed conflict (LOAC) defines *attack* broadly as an act of violence against the adversary, whether in offence or defence.³⁸ Attack refers to a particular type of military operation during an armed conflict to which international humanitarian law apply. However, it is important to note that these military actions follow from an armed attack that is the action that gives States the right to respond with use of force. This leads to the question of what is the cyber equivalent to armed attack. One paper proposes that an “armed attack in the cyber context can be interpreted as encompassing any acts [*sic*] that result in consequences analogous to those caused by the kinetic [*sic*][munition-based] actions originally envisaged by the term armed attack.”³⁹

0310. [CONCEPT] These legal and doctrinal issues clearly indicate the term *cyber attack* is not appropriate for the short or long term, particularly in a military context. There is, however, an urgent need for clarity and understanding of terminology in the execution of cyber operations. This terminology must consider the defence mandate; while at the same time reflect the terminology used by government partners and allies. As a starting point, **this JDN will provide interim terminology until such time as legal definitions and interpretations allow for the evolution of this terminology.** Thus, aligned with Public Safety Canada definitions for cyber incident and cyber event, the following levels should be used to classify or describe the level of cyber actions taken against DND/CAF by an adversary or threat actor.

- a. **Level 1, Cyber security event.** Cyber vulnerabilities and potential actions and/or effects that are a matter of security rather than defence.

³⁵ In late 2014, Sony was subject to a hack in which more than 100 TB of data, including personal data, was exploited, followed by the destruction of many computers due to installed malware. (Ref. BZ). The US Government treated the situation as a serious national security matter that was attributed to North Korea, which the North Koreans have denied. Within the US, as across the globe, there was much debate as to whether this action was considered an attack against a state that could merit a response in accordance with the LOAC.

³⁶ Russia’s effective use of cyber operations (ISR, OPE, exploitation) leading up to and during the conflict in Ukraine established an advantage that enabled Russian military activities to progress faster than the NATO OODA loop. These cyber activities included espionage, DDoS attacks against Ukrainian media and governmental organizations, defacements of several NATO websites, the jamming of Ukrainian policy-makers communications, manipulation of information and videos, the leaking of confidential emails and documents, and various disruptions in networks and information systems. These cyber activities remained below the threshold that would merit international action in accordance with the LOAC. (Ref. AY)

³⁷ During the annual Cyber Guard and Cyber Flag exercises, the TF HQ had significant issues with the term cyber attack, which made it clear the CAF must define its lexicon.

³⁸ Article 49(1) of the 1977 Additional Protocol I to the 1949 Geneva Conventions (Ref. BI).

³⁹ Michael N. Schmitt. “*Attack as a Term of Art in International Law : The Cyber Operations Context.*” (Ref. CA).

JDN 2017-02
 (PROMULGATION DRAFT)

- b. **Level 2, Cyber security incident.** Cyber events that result in the compromise of GC IT systems that are a matter of security rather than defence.
- c. **Level 3, Significant cyber incident.**⁴⁰ Cyber events or incidents that can impact or have the potential to impact military operations, therefore making them a defence matter.
- d. **Level 4, Cyber attack.** Cyber actions and/or effects that are a matter of national defence and are within the parameters of the LOAC.

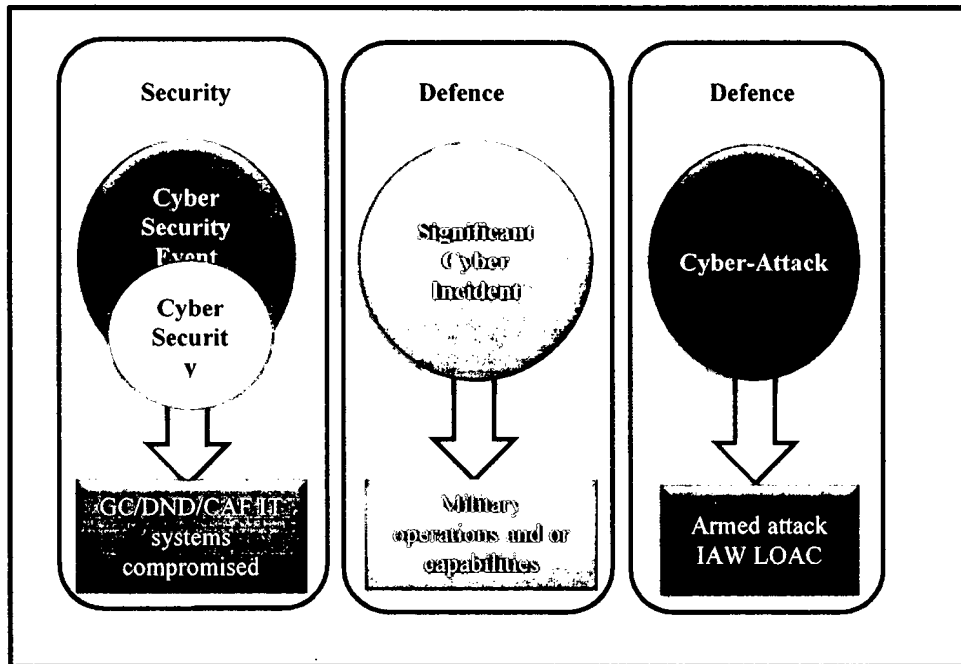


Figure 3-1. Taxonomy of Cyber Actions Taken Against DND/CAF.

0311. [CONCEPT] When classifying cyber vulnerabilities, actions or effects, it is important that a rapid analysis be conducted to determine the intent and scale of effects where both intent and scale can influence the outcome. For example, **an action that impacted military operations that resulted from accident (no intent to compromise military operations or capabilities) may be classified as a *cyber incident* rather than a *significant cyber incident*.** However, the scale of the effect may make that situation a significant cyber incident.

⁴⁰ *United States Cyber Incident Coordination* (Ref. AT) indicates that the US has also acknowledged a gap between *cyber attack* and *cyber incident*. The directive introduces a new term, *significant cyber incident*, defined as a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the US or to the public confidence, civil liberties, or public health and safety of the American People.

Page 36

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

0315. [MATURE] Today's military operations are faced with persistent and daily challenges that threaten friendly force freedom of action within and through cyberspace. These threats are increasing and evolving quickly and expose new vulnerabilities in both new and existing systems. Recalling the core attributes of the cyber domain, it is virtually impossible to defend and/or protect every aspect of the DND/CAF footprint in the cyber domain; thus, to focus security and/or defensive efforts, commanders can help determine the level of threat by determining:

- a. **Intent.** Understanding the potential intent and rationale for a threat actor is the most critical factor in determining the level of threat. Intent provides in-depth intelligence or context as to why an adversary may act. An adversary's intent can be either declared, demonstrated, or both. While an actor may have the capability and opportunity, if there is no intent, the threat is likely low or non-existent. Intent can be known or deduced.
- b. **Capability.**⁴³ Intelligence analyses focus primarily on understanding an adversary's strengths and the ability to generate and sustain them. In the cyber domain, this includes force structure, technical superiority, readiness, and sustainability. Sophistication levels will drive resources and the capabilities required to defend and secure friendly cyberspace. While a capability may exist, there may be no intent or opportunity to use it.
- c. **Opportunity.** Opportunities may arise at any time and can be created by friendly forces and/or shaped/influenced by threat actors. Opportunity is the key variable in assessing threat as the opportunity to act can present itself in many guises and at any time. Adversaries may actively seek to generate their own opportunity to act, through a variety of influencing or shaping activities. Opportunities will be available through changes or variances in the environment, providing potential advantage to the adversary. An adversary could also drive

⁴³ "The ability to carry out a military operation to create an effect." DTB record 36730.

JDN 2017-02
(PROMULGATION DRAFT)

friendly forces along a specific operational path resulting in potentially higher, repeatable risk. There may also be opportunities provided by friendly force activity more widely where their vulnerabilities provide avenues that threat actors can exploit to achieve their aims.

JDN 2017-02
(PROMULGATION DRAFT)

cyberspace. International doctrine and terminology make reference to effects that take place in or through cyberspace or the cyber domain. While most people understand the concept of effects in cyberspace or the cyber domain, there is still confusion with the concept of effects that are achieved through cyberspace. To illustrate this nuance, the following examples are provided:

- a. **“Within” or “in” cyberspace or the cyber domain.** These are cyber operations or activities that are conducted in cyberspace to create targeted effects in cyberspace. Examples of effects within cyberspace include:
 - (1) **Industrial and State espionage.**

Through cyber intrusions, intruders search for intelligence, intellectual property, prototypes, and company trade secrets to gain a strategic or operational advantage in military operations. The threat actors can be State, criminal, or industrial (to gain industrial advantage). Theft of Canadian technologies can drastically shorten capability development timelines and reduce the adversary’s economic investments to achieve intelligence and capabilities. Theft of operational plans can allow adversaries to gain the element of surprise within the operational environment. Successful espionage can prompt adversaries to develop counter-measures to our capabilities before they are even fielded.
 - (2) **Disruption or denial of access.** Disruption or denial of service can affect the availability of networks, information, or cyber-enabled resources. Denial of access can have catastrophic effects in operations; for example, if area air defence is disabled for a period of time, an adversary creates an open window for attack.
 - (3) **Destructive action.** Destructive action includes corruption, manipulation, or direct activity that threatens to destroy or degrade networks.
- b. **“Through” cyberspace or the cyber domain.** These are cyber operations that are conducted in cyberspace, but where the intended effect is in another domain. A theoretical example is the commandeering of an unmanned aircraft to redirect its flight path and/or fire one of its weapons. Another example of a cyber operation that had destructive effects in another domain was the STUXNET virus that destroyed Iranian nuclear centrifuges.

Page 40

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

CAF Approach to Cyber Solutions: Comprehensive, Integrated, Adaptive, and Networked

0323. [MATURE] In accounting for the complexities and challenges of cyberspace, DND/CAF solutions should be:

JDN 2017-02
(PROMULGATION DRAFT)

a. **Comprehensive:**

- (1) an in-depth understanding of the strategic environment;
- (2) an accurate definition of the problem and appropriate goal setting; and
- (3) an ability to apply a multidisciplinary approach.

b. **Integrated:**

- (1) a coordinated effort between DND and the CAF for force development, force generation, and force employment; and
- (2) the ability for two or more distinct organizations such as OGDAs and allies to work together in joint, integrated, or multinational operations.

c. **Adaptive:**

- (1) intelligent, through context-appropriate behaviour and decisions;
- (2) resilient, able to recover or adjust from shock, surprise, damage, or misfortune;
- (3) robust, by remaining effective across a range of conditions;
- (4) flexible, able to reconfigure;
- (5) agile, able to redirect swiftly;
- (6) creative, by generating novel and useful concepts, solutions, or products;
- (7) responsive, through speed of recognition and action; and
- (8) enduring, by withstanding prolonged strain.

- d. **Networked.** Both social networks (within the persona and cyber-persona layers) and technical networks (within the logical and physical layers) must be exploited by the CAF across the strategic environment and within all domains in response to adversaries' increased technical- and social-enabled capabilities.⁴⁶ Solutions must consider both human- (social) and

Crimea

In 2014, the Russians executed numerous low-level cyber-attacks against Ukrainian media and governmental organizations that encompassed digital propaganda, denial-of-service (DoS) campaigns, website defacements, information leaks by hacktivist groups, and cutting-edge cyber espionage malware. Advancing their information superiority further, Russia also used kinetic forces to sever communication and Internet connectivity between Crimea and Ukraine. These events illustrated the effective integration of cyber operations with traditional military operations to achieve military objectives that resulted in the annexation of Crimea from the Ukraine. These actions also demonstrate Russia's effective use of cyber operations in their broader strategy of information warfare.

⁴⁶ *Integrated Capstone Concept* (Ref. H), p. 17.

JDN 2017-02
(PROMULGATION DRAFT)

technology-enabled networks, where they are both equally important and interdependent.⁴⁷ When considering cyber operations, the need to consider technological networks is fairly obvious, whereas the requirement to consider the human network (e.g. political, military, economic, and cultural) may not be as evident. The Russian annexation of Crimea in 2014, described in the paper “Cyber War in Perspective: Russian Aggression against Ukraine” (Ref. AY)⁴⁸ illustrates how the Russians leveraged both the technological and social networks to exploit the hierarchical decision structures that were too slow to adapt and respond to the evolving situation. North Korea’s attack on Sony⁴⁹ is another example of an adversary’s ability to leverage both human and technological networks for strategic effects. The complex security environment, exemplified by these examples, indicates that both the human and technological networks will continue to play a pivotal role in the global security environment, thus solutions must address both networks.

⁴⁷ As an example, technological networks have created virtual social networks where distance is not a factor and where the boundary between a social network and a technical network is in some respects irrelevant.

⁴⁸ Kenneth Geers. “Cyber War in Perspective: Russian Aggression against Ukraine” (Ref. AY).

⁴⁹ Pete Williams, Robert Windrem, and Andrea Mitchell; NBC News: “North Korea Behind Sony Hack: U.S. Officials” (Ref. CL).

JDN 2017-02
(PROMULGATION DRAFT)

This page was intentionally left blank

JDN 2017-02
(PROMULGATION DRAFT)

Chapter 4

Defining Cyber Operations

Introduction

0401. [MATURE] A growing number of nations, both allied and adversary, have established, or are in the process of integrating cyber operations into military doctrine and planning. Increasingly sophisticated and effective cyber capabilities are being developed to exploit traditional and non-traditional⁵⁰ vulnerabilities. These more sophisticated cyber operations have the potential to undermine or impede our ability to operate across all domains. The last ten years have demonstrated how they can be used effectively to shape the information environment in support of political, economic, and military objectives. For example, Russia⁵¹ and China⁵² have integrated cyber operations into their military doctrine and planning. This was particularly evident during the Russian annexation of Crimea, in which a Russian whole-of-government approach was taken prior to traditional military action during phase 0 of the conflict.⁵³

0402. [MATURE] Within the operational environment, military actions in or through the cyber domain can be realized through interconnected physical and virtual networks or by exploiting individuals with network and system access. Military actions within the cyber domain can range from intelligence collection, to information operations, to sabotage and destruction. For example:

- a. Espionage can now draw from a dramatically larger medium through which to gain information that can subsequently be used to influence or jeopardize operations.
- b. Disruption or denial of access can affect network-enabled technologies that can jeopardize systems such as C2, weapon, and platform systems.
- c. **Cyber activities can destroy data, software, and components within cyberspace itself, or they can be physical within other domains as exemplified by taking control of an adversary unmanned aircraft (UA) and firing its weapon system.**

⁵⁰ The focus of traditional cyber vulnerabilities were on computer and ITS. An expanded focus is required to account for the non-traditional vulnerabilities represented in platform systems, weapon systems, soldier systems, and embedded systems that can have a detrimental effect on operations within and external to the cyber domain.

⁵¹ TRUNews; *Putin Updates Russian Cyber Doctrine* (Ref. CG).

⁵² Shannon Tiezzi; "China (Finally) Admits to Hacking: An updated military document for the first time admits that the Chinese government sponsors offensive cyber units" (Ref. CE)

⁵³ Kenneth Geers. "Cyber War in Perspective: Russian Aggression against Ukraine" (Ref. AY).

JDN 2017-02
(PROMULGATION DRAFT)

0404. This chapter will provide an overview of the operational art definitions for cyber operations to include:

- a. the principles of cyber operations;
- b. the types of cyber operations:
 - (1) defensive cyber operations;
 - (2) offensive cyber operations; and
 - (3) support cyber operations; and
- c. cyber operations in the joint battlespace.

Key Terminology

0405. The following key terminology is introduced in this chapter:

- a. **Cyber operational preparation of the environment (cyber OPE).** Cyber activities conducted to prepare and enable cyber intelligence, surveillance, and reconnaissance in support of cyber operations.⁵⁴

⁵⁴ Conceptual definition that requires development.

JDN 2017-02
 (PROMULGATION DRAFT)

- b. **Defensive cyber operation (DCO).** “A defensive operation conducted in or through cyberspace to detect, defeat and/or mitigate offensive and exploitive actions to maintain freedom of action. A DCO may include internal defensive measures and response action.”⁵⁵
- c. **Defensive cyber operation - Internal defensive measures (DCO-IDM).** “In DCOs, measures and activities conducted within one’s own cyberspace to ensure freedom of action.”⁵⁶
- d. **Defensive cyber operation - response action (DCO-RA).** “In DCOs, measures and activities conducted in or through cyberspace, outside of one’s own cyberspace, against ongoing or imminent threats to preserve freedom of action.”⁵⁷
- e. **Key terrain.** Key terrain in the cyber context still needs to be defined. It is currently defined as “Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant.”⁵⁸
- f. **Offensive cyber operation (OCO).** “An offensive operation intended to project power in or through cyberspace to achieve effects in support of military objectives.”⁵⁹
- g. **Support cyber operation (SCO).** “A network operation tasked by, or under direct control of, a commander to support offensive and defensive cyber operations.”⁶⁰

Cyber Operations

Many actors remain undeterred from conducting reconnaissance, espionage, and even attacks in cyberspace because of the relatively low costs of entry, the perceived payoff, and the lack of significant consequences. Moscow and Beijing, among others, view offensive cyber capabilities as an important geostrategic tool and will almost certainly continue developing them while simultaneously discussing normative frameworks to restrict such use. Diplomatic efforts [beginning in the 2010] have created the foundation for establishing limits on cyber operations, and the norms articulated in a 2015 report of the UN Group of Governmental Experts suggest that countries are more likely to commit to limitations on what cyber operations can target than to support bans on the development of offensive capabilities or on specific means of cyber intervention.

— James R. Clapper, Director of National Intelligence⁶¹

0406. [MATURE] *The CDS Initiating Directive for Defensive Cyber Operations* (Ref. I) defined cyberspace as a new domain for DND/CAF, complementary to the traditional domains. The cyber domain

⁵⁵ DTB record 693742.

⁵⁶ DTB record 694340.

⁵⁷ DTB record 694341.

⁵⁸ DTB record 4612.

⁵⁹ DTB record 693752.

⁶⁰ DTB record 694337.

⁶¹ James R. Clapper. “Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee” (Ref. AO), p.7.

JDN 2017-02
(PROMULGATION DRAFT)

requires that the same functions of C2 be exercised to prepare, deploy, employ, and redeploy forces and capabilities in support of CAF objectives. A flexible, efficient, and responsive C2 of cyber capabilities must permit the delivery of comprehensive, operationally responsive, and decisive effects at the place and time of the commander's choosing. Operations within cyberspace must be integrated, planned, and executed coherently within the DND/CAF, across OGDA, and with military allies and partners.

0407. [CONCEPT] Many States, both allied and adversary, have publicly declared their capability and/or their intentions to develop full-spectrum cyber operations capabilities. Thus, the CAF must be prepared to operate in a contested operational environment that could include OCO. It is essential that commanders and their staff not only understand OCOs, but that they are equipped and trained to defend against those actions. This new complexity in the operational environment will pose serious challenges to commanders as they operate within the cyber domain, as they must understand what activities can take place internal to or external to friendly force networks and to seek the appropriate rules of engagement (ROE) and authorities for those cyber operations that take place external to friendly force networks. CAF cyber operations that remain within DND/CAF networks include DCO-IDM and SCO. Cyber operations external to friendly force networks would be considered OCO and DCO-RA and consistent with allies, would have to be governed under use of force, requiring ROE and appropriate authorities. At this time, the CAF are not authorized to conduct OCO or DCO-RA operations, but many of our allies are. As such, commanders and their staff must be aware of how these operations are integrated into the planning and targeting processes of joint and combined operations.

0408. [MATURE] Cyber operations are military operations conducted in or through cyberspace to ensure the freedom of action and deliver effects on behalf of a strategic, operational, or tactical commander. As such, there is a need for a C2 link between the relevant commander and the organizations conducting cyber operations. Cyber operations deliver effects for a military commander, against an adversary. At the operational level, commanders will need a staff capable of identifying requirements for effects and integrating cyber operations into joint operations.

**Pages 49 to / à 54
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)



Support Cyber Operations

0435. [MATURE] Operations, including cyber operations, are a CAF responsibility under the authority of the CDS. In the execution of military operations, under the defence mandate of the CAF, there may be

JDN 2017-02
 (PROMULGATION DRAFT)

some activities that will cross both network operations⁶⁸ and cyber operations. These two operational lines have differing purposes. Network operations can occur throughout the spectrum of conflict, but are focused on the optimised routine performance of ITSs to meet a wide range of operating conditions while cyber operations focus on a specific adversary and the achievement of a military effect. For ITSs, there is little distinction between some of the activities of these two lines of operations in terms of functions and capabilities. For network operations and cyber operations, frequently the same personnel or organisations are engaged to perform both roles. Despite the observable overlap in functions as illustrated in Figure 4-2, there is a distinct delineation based on the intent, skills, and authorities required:

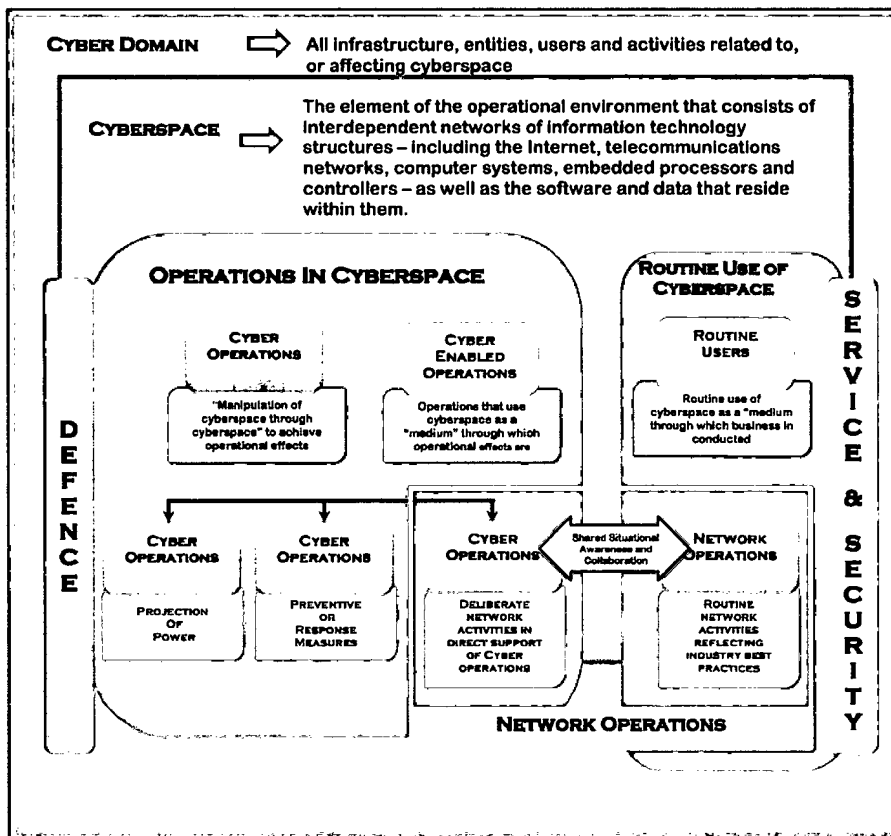


Figure 4-2. Functional Overview of Cyber Domain.

⁶⁸ Network operations are focused on the security and protection of ITS in accordance with industry best practices. Network operations are those routine day to day activities undertaken to build, operate, maintain, and protect the cyber domain. Network operations constitute activities for the provision and operation of a secure DND/CAF cyber domain to support operations and routine use of cyberspace. They include the following types of activities: developing secure network architecture, the monitoring of the health of networks, and the investigation and addressing of security infractions. They also include the practices, policies, procedural controls, and guidelines that describe the necessary operating conditions for the cyber domain. Network operations require enormous effort and resources to provide and operate the DND/CAF cyber domain, and to ensure the confidentiality, integrity, and availability of the critical information required to conduct military operations.

JDN 2017-02
(PROMULGATION DRAFT)

- a. **Intent.** Network operations usually include routine and normalized tasks that are threat agnostic. Cyber operations involve manoeuvres against a specific threat or adversary.
- b. **Skills.** Both network and cyber operations require extensive technical capabilities for ITS delivery and management, however cyber operations require a broad and deep understanding of cyberspace, cyber operations, tradecraft, and TTP focused not only a friendly systems, but also on the diversity of systems across cyberspace.
- c. **Authorities.** ADM(IM) is the responsible delegated authority for network operations, whereas the CDS is the responsible authority for cyber operations.

0436. [MATURE] SCOs are a critical operations support function and, in concert with network operations, they set the conditions for defence and help ensure mission assurance. Focused on the adversary and informed by intelligence, SCOs will drive such factors as bolstering defence and the sequencing and prioritizing of cyber operations and network operations in accordance with the campaign plan. They will contribute to the development of threat assessments and enhance CAF knowledge of the adversary.

0437. [DEVELOPING] To ensure mission assurance when confronted with an adversary within the operational environment, it is imperative that the CAF have the authority to plan and conduct those network operations that are in direct support of cyber operations. Recognizing that the majority of network operations are under the authority of ADM(IM), there is a need to differentiate routine network operations from those that are in support of cyber operations. This differentiation is captured in the term SCO, which fall under CAF authority and constitute an element of cyber operations. This delineation in authorities, from routine force generation of ITS network operations to a force employer, will ensure that operational needs will take precedence and actioned in accordance with military requirements for cyber operations. The table in Table 4-1 illustrates some functions that differentiate network operations from cyber operations:

JDN 2017-02
 (PROMULGATION DRAFT)

Network Operations (Security)	Cyber Operations ⁶⁹ (Defence)
Mission- and terrain-focused: fulfill normalized, routine tasks to assure missions; <u>threat agnostic</u>	Enemy-focused: address exceptional conditions or events <u>triggered by an adversary</u>
Operations occur only on and within friendly terrain	Operates across the entire battlespace to engage the adversary
Operationally prepare defended terrain for defensibility, reliability, and resilience	Conduct deliberate and crisis operations
Restore services caused by outages	Anticipate and/or respond to adversary activities (ISR, OPE, and effects)
Develop and maintain “mission maps” (results of mission-terrain analysis that identify mission dependencies on cyberspace; performed along with operations staff)	Maintain understanding of mission-terrain dependencies (“mission maps”) and mission threat analysis to inform refinements
Routine operation and maintenance	Mission-focused: sense, detect, orient, and engage enemy to assure the commander’s mission and outmanoeuvre the adversary
Assemble, configure, deploy, and secure systems, including sensors, to shape the environment for optimal mission performance in diverse conditions	Reposition and prioritize systems and sensors to execute the mission and address adversarial capabilities
Develop and maintain baseline profiles of system operation; understand normal v anomalous performance	

Table 4-1. Network Operations v Cyber Operations.

0438. [MATURE] Since DCO activities lead to a new defensible baseline or precondition for CAF networks, there is a requirement to ensure SCO and DCO activities are integrated and that appropriate liaison is maintained within cyber security organizations, particularly when new defence and/or security measures are to be addressed and/or implemented. The interdependencies and overlaps of SCO and DCO-IDM are enormous and require clear authorities, responsibilities, and accountabilities (ARA) and a centralized coordination function. The effectiveness of DCO-IDM depends intimately on a detailed understanding of the technical environment that is provided by SCO activities, which provide technically focused situational awareness. The reverse interdependency is also true, where ISR conducted under DCO-IDM can influence and/or direct SCOs such that the future cyber security posture of the networks can evolve to ensure effective response to general and specific threats. While DCO-IDM and SCOs are different activities, they are used complimentary to each other to achieve effects.

Network Operations

0439. [DEVELOPING] While not cyber operations, network operations create, shape, configure, operationalize, secure, and maintain DND/CAF cyberspace to support missions in the cyber *battlespace*. This activity is critical for assuring supported missions and providing the best advantage to the defender in future engagements. Network operators define the topology of the network; develop and maintain maps of the terrain; analyze the baseline behaviour of applications, protocols, missions, and users; maintain mission maps in partnership with the supported mission owner; and deploy the primary sensor network for joint operations. As part of maintaining DND/CAF cyberspace, network operations also focus on the

⁶⁹ Includes SCO, DCO, and OCO activities.

JDN 2017-02
(PROMULGATION DRAFT)

availability of services, optimization of resources, and configuration and management of the terrain. Network operations often provide the first line of defence and are the first to respond to events or crises, particularly when the means, cause, or effects are still unclear. Network operations are the priority when events are not the result of adversary action. When an event or crisis appears to have been exploited by an adversary, network operations are then subordinate to DCO-IDM activities.

0440. [MATURE] Network operations are focused on the security and protection of ITS in accordance with industry best practices. Network operations are those routine day to day activities undertaken to build, operate, maintain, and protect the cyber domain. Network operations constitute activities for the provision and operation of a secure DND/CAF cyber domain to support operations and routine use of cyberspace. They include the following types of activities: developing secure network architecture, monitoring of the health of networks, investigating and addressing security infractions. They also include the practices, policies, procedural controls, and guidelines that describe the necessary operating conditions for the cyber domain. Network operations require enormous effort and resources to provide and operate the DND/CAF cyber domain, and to ensure the confidentiality, integrity, and availability of the critical information required to conduct military operations.

Page 60

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

Situational Awareness

0450. [MATURE] To build and maintain situational awareness within the cyber domain and the greater operational environment, one must consider the core attributes of cyberspace, which include the vastness of information, convergence, and the continual changes that occur across the layers of cyberspace. These core attributes demand that solutions be comprehensive, integrated, adaptive, and networked across the CAF and developed in collaboration with our government partners and our allies. This approach will directly contribute to the development of situational awareness that will enable timely and adaptive decision making. As examples, this approach will enhance the:

- a. effectiveness of attribution, through collaboration, multiple sources can contribute to positive identification;
- b. identification of linkages between what may have otherwise appeared to be unconnected events;
- c. identification of potential hostile intentions; and
- d. identification of evolving hybrid campaigns.

Page 62

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)


**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

Partnerships

0455. [MATURE] The most critical principle for cyber operations is partnerships, as reflected in Canadian, Five Eyes, and NATO strategic policies. Commanders and their staff must be prepared to ensure that partnerships are well defined to ensure the coordination and deconfliction of cyber activities across the cyber domain while balancing information confidentiality and integrity with accessibility and security. These partnerships will help identify collective and individual vulnerabilities, which when corrected, can strengthen individual and collective resilience. Further, commanders and their staff must ensure that their partnerships support the key principles of attribution, security, resilience, and situational awareness to both enable and enhance effective cyber operations within the operational environment.

0456. [MATURE] Cyber engagement with our partners and allies is realized through several key collaboration programs, which include:

- 
- b. **NATO Cooperative Cyber Defence Centre of Operational Excellence (CCDCOE).** Although not under unified NATO command, the Centre's mission is to enhance capability, cooperation, and information sharing among NATO, its member nations and partners in cyber defence by virtue of education, research and development, lessons learned, and consultation.
 - c. **Combined Communications Electronics Board (CCEB).** The CCEB conducts IT-related investigations on behalf of the Five Eyes, producing recommended IT standards solutions influencing the evolving cyber domain at large and SCOs specifically.
 - d. **International Computer Network Defence Coordination Working Group (ICCWG).** The ICCWG influences DCCG activities in its role to facilitate the conduct of multilateral information assurance, DCOs, and information sharing to achieve mutually assured national defence information networks. Areas of collaboration with the DCCG include the development of cyber concepts, protocols risk management, and multinational training initiatives.
 - e. **Technical Cooperation Program (TCP).** Cyber research and development (R&D) is limited to the TCP, specifically the Cyber Strategic Challenge Group, which facilitates agreement and establishment of cyber R&D joint projects, including the assignment of resources, with a current focus on DCO.

**Pages 64 to / à 66
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

Chapter 5

Cyber in the Operational Environment

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

—Sun Tzu, *The Art of War*

Introduction

0501. [MATURE] While it is possible that some military objectives can be achieved by cyber operations alone, commanders at the operational level must plan and execute cyber operations just as they would for maritime, land, and air operations. To do this, commanders must understand how cyber operations and actions fit into the context of joint operations such that they are synchronized with other operations during execution. In this larger context of joint operations, commanders must recognize their dependency on cyberspace for virtually all of their C2 to include:

Key Terminology

0503. [MATURE] The following key terminology is introduced in this chapter.

- a. **Act.** “The operational function that integrates manoeuvre, firepower and information operations to achieve the desired effects.”⁷⁶

⁷⁶ DTB record 26165.

JDN 2017-02
(PROMULGATION DRAFT)

- b. **Area of operation (AO).** “A geographical area, within an AOR, assigned to a subordinate commander within which that commander has the authority to plan and conduct tactical operations.”⁷⁷
- c. **Area of responsibility (AOR).** “The geographical area assigned to an operational-level commander within which that commander has the authority to plan and conduct military operations.”⁷⁸
- d. **Battle damage assessment (BDA).** “The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective.”⁷⁹
- e. **Command.** “The operational function that integrates all the operational functions into a single comprehensive strategic, operational or tactical level concept.”⁸⁰
- f. **Cyber intelligence.** Information of value collected and processed through cyber operations.⁸¹
- g. **Operational environment.** “The set of conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander.”⁸²
- h. **Sense.** “The operational function that provides the commander with knowledge. This function incorporates all capabilities that collect and process data.”⁸³
- i. **Shield.** “The operational function that protects a force, its capabilities and its freedom of action.”⁸⁴
- j. **Sustain** “The operational function that regenerates and maintains capabilities in support of operations.”⁸⁵
- k. **Vital ground.** “Ground of such importance that it must be retained or controlled for the success of the mission.”⁸⁶
- l. **Vulnerability.** In the context of cyber operations, the characteristics of a system that render it open to exploitation or susceptible to a given hazard or threat, possibly resulting in an impaired capability to perform a designated task.

⁷⁷ DTB record 3528.

⁷⁸ DTB record 34612.

⁷⁹ DTB record 26988.

⁸⁰ DTB record 26166.

⁸¹ The MITRE corporation. MCDC for MCDO definition for cyber intelligence. This is a conceptual definition until a cyber intelligence definition is ratified through the Defence Terminology Standardization Board.

⁸² DTB record 43606.

⁸³ DTB record 26167.

⁸⁴ DTB record 26169.

⁸⁵ DTB record 26170.

⁸⁶ DTB record 1529.

**Pages 69 to / à 71
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

The Cyber Area of Operations

0516. [MATURE] Commanders traditionally exercise military authority by establishing an AOR that is defined geographically. However, given the global nature of cyberspace, commanders must understand their freedoms and constraints when operating in the cyber domain. Their plans must consider internal and external networks that exist within and external to their AOR. Commanders may require authorities and delegations to conduct cyber operations beyond the geographical boundaries of their AOR.

Control and Coordination of Resources

0517. [DEVELOPING] Cyber forces can realize both tangible and intangible operational objectives across the full spectrum of operations. It is critical that the control of cyber resources and effects, with corresponding accountability responsibilities, be held at the level that ensures their most effective utilization. For example, a cyber operation can be used in support of an information operation objective, however this effect may jeopardize cyber operations or intelligence capabilities that can be employed for greater effect at the operational or strategic levels.

JDN 2017-02
(PROMULGATION DRAFT)

0518. [DEVELOPING] Given the cyber domain is global, control and coordination is extremely complex and will require collaboration with OGDAs, allies, partners, and/or host nations. For example, **diplomatic activity may be necessary to allow the commander to have use of host-nation resources such as services, infrastructure, and material that need to be coordinated in support of cyber operations.**

Risk Assessment

0519. [MATURE] Developing an assessment of cyber domain risk is critical to mission assurance. Associating key terrain with specific threats allows for an initial risk assessment. The application of mitigation strategies will result in a residual risk rating that should be part of the activities in the mission analysis of OPP and eventually in the initial staff estimate. Identifying the key terrain is the first step in the generic cyber operations information-collection process. Key terrain is mission-specific, and with a focused intelligence effort, is instrumental in developing a risk assessment approach to support the risk assessment activities in the mission analysis activities as part of operations planning.

⁸⁷ CFJP 3-0, *Operations* (Ref. R), p. 1-3.

**Pages 74 to / à 77
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

Freedom of Action

0539. [CONCEPT] DCO and SCO are critical enablers to ensuring the CAF's freedom of action within the operational environment, both within the cyber domain itself, as well as within the physical domains. Extending beyond the traditional ITSs, commanders and staff must be aware of the vulnerabilities of their weapon and platform systems that are dependent on cyberspace, whether they are stand-alone or interconnected. A compromise within the cyberspace of a weapon or platform system (e.g. engine controller) may directly or indirectly impact on the freedom of action of that weapon or platform system in one or more of the physical domains.

0540. [CONCEPT] To ensure freedom of action, DCO and SCO forces need to coordinate activities and evolve over time based on best practices. The key is for SCO forces to fix identified vulnerabilities and for DCO forces to focus on unresolved and unknown vulnerabilities on an ongoing cycle. The DCO forces

JDN 2017-02
(PROMULGATION DRAFT)

should not be burdened with continuing to monitor against fixed vulnerabilities and exploits against them as a priority, as it wastes limited and valuable resources.

0541. [CONCEPT] OCO can also support freedom of action by overwhelming adversary OCO and DCO forces with secondary OCO activities (as a distraction), while the main OCO activities manoeuvre on primary targets.

Concentration of Force

0542. [CONCEPT] The identification of key terrain, combined with the threat and vulnerability analysis will help drive force composition, structure, and concentration of resources such that they can achieve their greatest effect.

Page 80

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

Operations Planning Process (OPP)

0552. [MATURE] Military cyber operations must be coordinated, synchronized, and integrated with all other military capabilities across the strategic, operational, and tactical levels of operations. These activities are best considered as part of the full-spectrum targeting processes. It recognizes that other nations or actors, both friendly and adversary, may use cyber capabilities to enhance their own ability to achieve a degree of local, regional, and/or international influence, which may otherwise be limited through other means. The OPP is where everything comes together and it is emphasized that cyber operations planning is done in conjunction with many other planning processes such as network operations, joint fires, ISR, intelligence, electronic warfare, and information operations.

0553. [MATURE] Cyber operation planners are presented the same considerations and challenges that are present in planning for other joint capabilities and functions, as well as some unique considerations. **The challenge in cyber operations rests with the second- and higher-order effects in and through cyberspace, which can be more difficult to predict, therefore necessitating more branches and sequels in plans. While cyber effects can be non-lethal, their effects can be significant in terms of scope and scale, where second and third-order effects can potentially echo throughout global cyberspace and have many unintended consequences.**

0554. [MATURE] One significant characteristic of cyber operations already discussed is time. Cyber preparations often take years to develop. Knowledge of specific capabilities will be tightly controlled and held at the highest classification levels. While this preparatory phase can take years, the execution phase may only take seconds. Similarly, in defensive terms, it may take far more people, time, and resources to successfully protect and defend our own networks than for an adversary to launch a credible attack against them.

Cyber Operations – Effects in the Operational Environment

0555. [MATURE] Integration of cyber operations with the physical domains takes place through the OPP. In accordance with CFJP 5.0, *Canadian Forces Operational Planning Process* (Ref. V), the OPP is applicable in all CAF operations and consists of five consecutive stages: initiation, orientation, course of action (COA) development, plan development, and plan review. The OPP process adapts well to cyber operations and it is imperative that cyber operations be considered at each stage of the process so that effects through or within the cyber domain are properly considered, evaluated and, if required, programmed to meet operational objectives. These effects can be achieved at any of the strategic, operational, or tactical levels.

Page 82

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)**Authorities**

0556. [MATURE] Regardless of the operational phase underway, it is always important to determine what authorities are required to execute cyber operations. **Cyber operations planners must account for the lead time to acquire the authorities needed to achieve the desired effect, recognizing that cyber operations require national approval in coordination with OGDA and/or allies.** This does not change operational commanders' planning fundamentals, but does emphasize the importance of coordination with interagency partners, who may have authorities that are different from those of DND/CAF.

0557. [CONCEPT] Commanders have the authority⁹⁵ to operate, monitor, posture, reconfigure, and defend (SCO and DCO-IDM) DND/CAF cyberspace within their designated operating area. These activities include monitoring and detection of threats. Cyber forces in support of commanders conduct cyber operations under their authority. The escalation of incidents or events may quickly supersede the local commander's authority and shift the supporting/supported relationships for cyber operations. **Commanders may delegate authority to forces (both organic and supporting) for data collection, data management, monitoring, and analysis of DND/CAF cyberspace. As authorized by the supported commander, these forces may employ active defensive features in coordination with higher headquarters.**

0558. [CONCEPT] Commanders can approve actions taken in response to anomalies or adversary presence detected within DND/CAF cyberspace. **Commanders may authorize pre-approved responses, partially or wholly automated, for defined conditions and events.** Expert cyber operators support the commander's risk assessment associated with these automated responses. **While automated responses will mitigate some risks, they might present new ones.**

0559. [CONCEPT] Due to the potential impact on the commander's mission, authority to apply cyber operations capabilities that change the normal function of DND/CAF mission systems are not generally delegated; appropriate command authority will specifically direct these. It is necessary for commanders

⁹⁵ Authorities are defined in operations orders.

JDN 2017-02
(PROMULGATION DRAFT)

and their staff to ascertain whether and under which circumstances specific cyber operations are authorized.

Intelligence Requirements

0561. [DEVELOPING] The recognition of the cyber domain as a warfighting domain gives impetus to the broad application of military intelligence practices that have not previously been applied to the cyber domain. In particular, cyber operations focus intently on the enemy threats to DND/CAF missions, and

JDN 2017-02
(PROMULGATION DRAFT)

they rely heavily on ISR from across the entire operational environment for planning and operational decision making. Regardless of the source or activity that generated the information, **cyber intelligence includes all information regarding the enemy in relation to cyberspace.**

0562. [MATURE] Commanders should consider cyberspace as an area of intelligence collection and analysis in its own right. Intelligence support to operations within cyberspace is essential to provide knowledge, reduce risk, and support effective operational decision making. Trying to simultaneously defend key terrain, let alone all of cyberspace is impractical. Timely intelligence produces an understanding of the most likely areas of attack, thereby informing decision makers as to where cyber operations need to be focused. **Linked to intelligence is risk analysis and risk management where risk management is about reviewing identified risks to decide what can be mitigated, transferred, or accepted. Some risks are unacceptable, and it is necessary to mitigate the risks by using cyber operations capabilities. These capabilities are usually a limited resource, and therefore need to be prioritized to enable mission assurance.**

0563. [DEVELOPING] A comprehensive view of the adversary includes all the traditional elements of military intelligence applied to cyberspace: intent, risk profile, organization, composition, disposition, strength, capabilities (operational and technical), limitations, tradecraft, tactics, likely COAs, etc. The disposition, strength, and capabilities support an analysis of adversary potential COA. Capabilities, tradecraft, intent, and disposition are difficult to assess with confidence, given the current level of maturity of cyber operations. Consequently, the range of possible COAs is much broader in cyberspace, increasing the need for rigorous and creative intelligence collection and analysis. To achieve a comprehensive understanding of the adversary, DND/CAF must collect, fuse, and analyze data across the entire operational environment, then make the analysis results available to military planners, operators, and commanders. This involves complex intelligence needs that depend on data collection across a significantly broader array of sources and locations.

0564. [MATURE]

Information requirements are general or specific subjects on which there is a need for the collection of information or the production of intelligence. **Information requirements related to cyberspace may include: network infrastructures, personnel status, readiness of adversary's equipment, unique cyberspace signature identifiers such as software/firmware versions, configuration of files, etc.** Cyberspace planners can submit RFIs to generate intelligence collection efforts in support of cyber operations support to the OPP. RFIs respond to customer requirements, ranging from dissemination of existing products through the integration or tailoring of on hand information to scheduling original production. The information must be timely, accurate, and in a usable format.

0565. [MATURE] Given the complex and interconnected nature of DND/CAF cyberspace, broad and rapid sharing of cyber threat intelligence is needed to counter the speed, scale, and operational reach of adversary ISR and OCO. **Since adversaries within the cyber domain apply common capabilities and tradecraft against multiple targets across the globe, broad sharing and multi-echelon analysis are needed to understand and counter those adversaries. The aggregated intelligence supports analysis and correlation to increase detection, mitigation, attribution, and response effectiveness globally, and it is more likely to reveal the adversary's higher-level objectives and overall campaign.**

JDN 2017-02
 (PROMULGATION DRAFT)

0566. [MATURE] The cyber threat knowledge base comprises known or suspected enemy activity across the area of interest, but specifically focuses on adversary activities in friendly or partner networks, and any known or suspected attempts to breach those networks. The data contains adversary observables, indicators of compromise, events and incidents, capabilities, TTP, tradecraft, friendly and enemy campaigns, disposition, C2 infrastructure, threat actors, victims, etc. The cyber threat knowledge base enables automated analytics and reporting as well as manual analysis, query, and discovery.

Intelligence Support to Cyber Operations

0567. [DEVELOPING] Intelligence involves the collection and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer COAs to enhance decision making. The intelligence activities must span all five layers of the cyber domain, to include the geographical and persona layers. Intelligence is a complex, multifaceted approach to framing and reacting to cyber adversarial activity. To better understand and anticipate adversarial actions and intent, the need for timely intelligence is important. Intelligence requires an integrated approach to the environment taking into account the human factor and all the constraints that are the cause of every cyber activity. Analysis will need to develop the understanding of the human element (including their intent, how they plan, coordinate and execute, and what motivates them toward action or inaction), rather than just simply network functionality.

0568. [MATURE] Intelligence on nation-State threats should include all-source analysis to factor in traditional political/military indications and warnings. Adversary cyberspace actions will often occur outside, and often well in advance of, traditional adversary military activities. Additionally, cyber intelligence and warnings may recognize adversary cyber operation triggers with only a relatively short time available to respond. These factors make the inclusion of all-source intelligence analysis very important for the effective analysis of an adversary's intentions in cyberspace.

Intelligence Gain/Loss (IGL)

0569. [MATURE] The intelligence and operational gain/loss decision space within cyber operations is subtle and complex. Knowledge of tactics effective at exploiting vulnerabilities is valuable to both offence and defence. The gain/loss decision for the attacker must account for the risk of exposing offensive capabilities and tradecraft. First, an exposure educates the defender on the existence of the attack capability or tradecraft. This loses the element of surprise and degrades the effectiveness of the capability or tradecraft. Second, the software capability and techniques can enable the adversary to employ that attack back on the attacker. Third, a single exposure can lead to global exposure and subsequent mitigation, significantly amplifying the first two risks. Attacks might tolerate the exposure of a single point of data, believing that they maintain plausible deniability. However, global exposure can provide significant evidence of intent and complicate plausible deniability.

0570. [MATURE] The defender also makes gain/loss decisions. By striking an enemy every time they are observed, the defender reveals to the attacker where they have observed and not observed; the action serves an immediate objective, but has a strategic cost of improving the adversary's situational awareness. The defender is educating the attacker about defensive sensing capabilities and the weaknesses in their attack. This enables the attacker to operate in locations where the defence does not observe.

Page 87

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

0574. [MATURE] The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn Manual) (Ref. BF) is a comprehensive, academic, non-binding analysis of how international law applies to cyberspace. It provides various rules reflecting consensus among a group of international experts as to the application of the law currently governing cyber conflict. Although the *Tallinn Manual* serves as a guide, this is an emerging area of law with little directed consideration by courts in terms of cyber warfare at this time. The *Tallinn Manual* is not an authoritative statement of the law and reference to it in targeting should be on the basis of legal advice to ensure the correct application of applicable laws.

0575. [MATURE] The *Tallinn Manual* (Rule 30) (Ref. BF) establishes that a cyber attack is a cyber operation, whether offensive or defensive, if it is reasonably expected to cause injury or death to persons, or damage or destruction of objects. The notion of attack may extend to serious injury and severe mental suffering that are tantamount to injury. Operations that do not cause violent consequences do not qualify as attacks. However, it is important to note that it is the consequence of the cyber operation, not its nature, that characterizes it as violent or not. With respect to attacks on objects, the majority of *Tallinn Manual* experts were of the view that cyber interference with the functionality of an object may represent damage, thereby constituting a cyber attack, if the restoration of such objects requires the replacement of a physical component. A cyber attack that is successfully intercepted and does not result in actual harm could still be considered an attack in accordance with the LOAC. If a cyber operation is an important part of a larger operation, such as disabling defences, that also include the use of munitions-based means, the LOAC rules with respect to attacks would apply to the cyber operations.

Page 89

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**



JDN 2017-02
(PROMULGATION DRAFT)

Areas of operations (AOs)

0583. [DEVELOPING] AOs should be large enough for subordinate commanders to accomplish their goals, achieve their objectives, and succeed in their missions. AOs in cyberspace should normally be aligned with the geographic operating area. However, when recognizing the multiple layers of cyberspace, there

JDN 2017-02
 (PROMULGATION DRAFT)

are distinct dependencies on other cyberspace AOs. A general goal is to minimize confusion due to overlapping AOs.

0584. [DEVELOPING] Commanders must understand operating area boundaries and coordinate operations at the seams or within overlapping areas. Joint and component commanders must collaborate to reduce the complexity and number of interfaces to provide the best possible control to the supported commander. Operations normally have critical external dependencies and interfaces. These dependencies and interfaces should be made explicit between the associated commands. A commander's cyberspace area of interest extends beyond the command's operating area to include portions of the associated service environment, portions of the DND/CAF wide area backbone, the Internet, and adversary terrain. The overlap in areas of interest for all commanders justifies the need for holistic intelligence operations and collaborative analysis.

0585. [DEVELOPING] The speed and operational reach¹⁰² of OCO is such that conditions can rapidly expand across cyberspace, or may already exist there unbeknownst. A natural tension exists regarding where to direct the engagement. Ideally, the engagement is directed and forces are allocated at the lowest level possible within their mission context (of the supported commander). The potential for rapid and broad impact of adversary OCO often induces a desire to escalate and centralize control of situations even for tactical engagements at lower echelons. The challenge with that approach is that higher echelons lack the full operational context of the supported commander. In general, escalation of operational control occurs only when both:

- a. the risk to a larger AO outweighs the operational risk at the lower echelon; and
- b. lower echelons are not likely to succeed in managing this risk.

0586. [DEVELOPING] Commanders at all echelons and allocated/supporting forces must continuously assess the potential for conditions to escalate beyond the commander's operating area, presenting risk to other commanders and their missions. They proactively communicate on conditions where there is a reasonable belief that adversary or friendly activities or their effects might extend beyond the local operating area.

Legal Considerations

0587. [MATURE] There is a fundamental difference between the laws governing cyber operations in peacetime and those applicable to cyber operations during an armed conflict. Hence the authority and scope to act will vary legally; as will the language used to characterize the numerous, complex operational parameters and descriptors.

0588. [MATURE] International law generally prohibits the threat or use of force but allows for exceptions when there is a legal basis to resort to force. These include, consent of the State, enforcement action taken by the UN Security Council and the right to self-defence under Article 51 of the UN Charter (Ref. BJ) and in customary international law.

¹⁰² Operational reach: The extent to which military capability can effectively be employed, expressed in distance and duration. [DTB record 32315]

JDN 2017-02
(PROMULGATION DRAFT)

0589. [MATURE] The international body of law that would apply to cyber operations during an armed conflict is the LOAC, also referred to as “international humanitarian law” (IHL). LOAC is a specialized body of international law that governs the conduct of hostilities of parties to an armed conflict for the duration of the armed conflict.

0590. [MATURE] For cyber operations that take place outside of an armed conflict, the applicable legal framework is peacetime international law. Some general principles of peacetime international law that may apply are State sovereignty, jurisdiction, and responsibility. The ability to use force in peacetime will be limited and LOAC does not apply to peacetime cyber operations.

0591. [MATURE] An important principle that will come into play during peacetime cyber operations is the principle of *State responsibility*. States bear responsibility for their internationally wrongful acts in accordance with the law of State responsibility. An internationally wrongful act is an act or omission that constitutes a breach of an international legal obligation applicable to that State and is attributable to the State under international law. One State may be entitled to take a countermeasure in response to a breach of an international obligation that is owed by another State. Countermeasures are used by an injured State to compel or convince the responsible State to desist in its internationally wrongful acts or omissions. Countermeasures must comply with a number of requirements that include limiting countermeasures to the time of non-compliance by the responsible State and being proportional to the injury suffered. Countermeasures are not available in response to a cyber operation by a non-State actor unless the operation is attributable to a State.

Page 93

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

This page was intentionally left blank

JDN 2017-02
(PROMULGATION DRAFT)

Chapter 6

Command and Control of Cyber Operations

Introduction

0601. [MATURE] To ensure that the CAF can unfailingly react to GC direction to respond and deploy in support of domestic and global events, the CAF must invest in a combat-capable force that is properly equipped and trained to operate in a contested cyber environment. This force must be agile enough to respond to continuously evolving threats.

**Pages 96 to / à 97
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

This page was intentionally left blank

JDN 2017-02
(PROMULGATION DRAFT)

Chapter 7
Challenges and Next Steps

Introduction

0701. [DEVELOPING] Operational and organizational needs required doctrine for cyber operations be published immediately, recognizing that it would be impossible to capture the entire scope of cyber operations within the first iteration of this JDN. The intent of this last chapter is to attempt to capture some of the significant gaps and challenges that currently exist. Given that many of the concepts, terminology, and definitions will continue to evolve for many years, the content of this iteration ranges in maturity from conceptual through to mature. This designation should help commanders and staffs to understand cyber operations, to include the gaps or content that has not yet been covered as well as some of the significant challenges that have yet to be resolved within the cyber domain. This information should influence commanders and staffs to:

- a. seek additional advice from the respective functional, occupational, technical, and operational authorities;
- b. seek legal and political advice;
- c. establish liaison with appropriate stakeholders within the CAF, and among OGDAs and allied partners; and
- d. inform the development of their own doctrine and TTP.

Policy and Doctrine

JDN 2017-02
(PROMULGATION DRAFT)

Characteristics of the Cyber Domain

0704. Much more work is required to develop, refine, and validate the characteristics of the cyber domain. For example, the following concept has merit for consideration, but requires more work: *time, space, force, and energy*. The relationship between time, space, force, and energy in cyberspace differs from the traditional domains. These differences can offer significant opportunities for innovations in the science and art of war.

**Pages 101 to / à 103
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

JDN 2017-02
(PROMULGATION DRAFT)

This page was intentionally left blank

JDN 2017-02
 (PROMULGATION DRAFT)

Glossary

One of the challenges in defining strategy, policy, and doctrine for cyber operations is the lack of consistent terminology within the international community. Canada and the UK use NATO terminology a priority. Canada will have its own terminology when it is required because of Canadian law or because the NATO definition does not reflect the Canadian reality. When Canada's definition is different from the NATO one, the latter is also given. We have also given those of our closest allies when there are differences.

The following references are cited:

AJP-3.20	(NATO) <i>Allied Joint Doctrine for Cyberspace Operations</i> (Ref. AU)
DTB	<i>Defence Terminology Bank</i> (Ref. E)
GC SEMP	<i>Government of Canada Cyber Security Event Management Plan</i> (Ref. C)
JDP 0-50	(UK) <i>Cyber Doctrine</i> (Ref. AL)
JP3-12	(US) <i>Cyber Operations</i> (Ref. AR)
Tallinn Manual 2.0	<i>Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare</i> (Ref. BF)
Termium	<i>TermiumPlus</i> (Ref. AI)

area of operations (AO)

A geographical area, within an AOR, assigned to a subordinate commander within which that commander has the authority to plan and conduct tactical operations. [DTB Record 3528]

NATO► An area defined by the joint force commander within a joint operations area for the conduct of specific military activities.

area of operations management

The prioritization, coordination and deconfliction of activity across all dimensions within an assigned AO. [DTB Record 32222]

attack

In military operations, to take offensive action against a specified objective. [DTB Record 693774]

computer network attack (CNA)

Term is obsolete [DTB Record 26982]

NATO► Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself.

computer network defence (CND)

Term is obsolete [DTB Record 26985]

JDN 2017-02
(PROMULGATION DRAFT)

computer network exploitation (CNE)

An intelligence collection activity intended to access, gather data from or control an ITS of an adversary, potential adversary or other Government of Canada approved party.

NATO ► Action taken to make use of a computer or computer network, as well as the information hosted therein, to gain advantage.

computer network operation (CNO)

Term is obsolete [DTB Record 47917]

cyber attack

A cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. [Rule 92, Tallinn Manual 2.0]

NATO ► An attempt by hackers to damage or destroy a computer network system. [AJP-3.20]

cyber domain

All infrastructure, entities, users and activities related to, or affecting, cyberspace. [DTB Record 694360]

NATO ► The virtual global domain consisting of all interconnected networks which are separated or independent [AJP-3.20]

UK, US ► Used interchangeably with cyberspace.

cyber event

Any significant loss or serious threat of loss of networks or data that threaten DND/CAF or its interests. [proposed by CJOC and adapted from US Emergency Action Procedures Volume VI – dated 14 Sep 2012]

cyber incident

NATO ► The appearance of any undesired behaviour in or a restriction of own freedom of maneuver. [AJP-3.20]

cyber key terrain (CKT)

NATO ► Those elements of cyberspace that enable mission essential activities, operations or functions. It comprises any area (physical, logical, and social) whose seizure, retention or disruption affords a marked advantage to either combatant. [AJP-3.20]

US ► The network links and nodes that are essential to a particular friendly or adversary capability. [JP 3-12]

JDN 2017-02
(PROMULGATION DRAFT)

cyber operation

An operation whose primary purpose is to achieve an objective in or through the cyber domain.

Note: Cyber operations consist of offensive cyber operations, DCOs and SCOs.

[DTB Record 69442]

NATO ► The employment of capabilities where the primary purpose is to create effects in support of the commander's intent in or through cyberspace.

UK ► The planning and synchronization of activities in and through cyberspace to enable freedom of manoeuvre and to achieve military objectives. [JDP 0-50]

US ► The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. [JP3-12]

cyber security (CS)

The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability. [TermiumPlus]

NATO ► All measures required to ensure absolute protection of own cyber networks as well as all measures to disguise own cyber activities to deny traceability of own forces action.

cyber security event

The indication that a cyber vulnerability may exist, that a cyber threat may be planned or that a cyber security incident may have occurred, requiring analysis and a risk management decision to determine an appropriate COA [GC CSEMP]

cyber security incident

any cyber security event (or collection of security events) or omission that results in the compromise for a GC IT system [GC CSEMP]

NATO ► The appearance of any undesired behaviour in or a restriction of own freedom of maneuver. [AJP-3.20]

JDN 2017-02
(PROMULGATION DRAFT)

cyberspace

The element of the operational environment that consists of interdependent networks of information technology structures-including the Internet, telecommunications networks, computer systems, embedded processors and controllers-as well as the software and data that reside within them. [DTB Record 694338]

NATO► Cyber - Of, relating to, or involving (the culture of) computers, virtual reality, or the Internet, futuristic. [AJP-3.20]

UK► An operating environment consisting of the interdependent network of digital technology, infrastructures (including platforms, the Internet, communications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical, virtual and cognitive domains. [JDP 0-50]

US► A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [JP 3-12]

cyber threat

NATO► The possibility of a malicious attempt to damage or disrupt a computer network system. [AJP-3.20]

cyber tool

NATO► Cyber means of warfare that are by design, use, or intended use not considered as a cyberweapon. [AJP-3.20]

cyberwarfare

NATO► The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic military purposes. [AJP-3.20]

cyber weapon

NATO► A piece of computer software or hardware used to commit cyberwarfare. [AJP-3.20]

defensive cyber operation (DCO)

A defensive operation conducted in or through cyberspace to detect, defeat and/or mitigate offensive and exploitive actions to maintain freedom of action.

Note: A DCO may include internal defensive measures and response action.

[DTB Record 694340]

NATO► Active and passive measures to preserve the ability to use cyberspace. [AJP-3.20]

US► Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and other designated systems [JP3-12]

JDN 2017-02
(PROMULGATION DRAFT)

defensive cyber operation - internal defensive measures (DCO-IDM)

In defensive cyber operations, measures and activities conducted within one's own cyberspace to ensure freedom of action. [DTB Record 694340]

- US▶** 1. Those defensive cyber operations that are conducted within the DoD information network. [JP 3-12]
2. Internal defensive measures conducted within defended terrain, to include actively hunting for advanced internal threats [also known as "ISR"] as well as the internal responses to these threats. Respond to unauthorized activity or alerts/threat information within the DODIN and leverage intelligence, counter-intelligence (CI), law enforcement (LE), and other military capabilities as required.

defensive cyber operation - response action (DCO-RA)

In defensive cyber operations, measures and activities conducted in or through cyberspace, outside of one's own cyberspace, against ongoing or imminent threats to preserve freedom of action. [DTB Record 694341]

US▶ Deliberate, authorized defensive measures or activities taken outside the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. [JP3-12]

deliberate operation

An operation characterized by detailed planning and coordination.

Note: A deliberate operation is conducted at the time of a commander's choosing. [DTB Record 41406]

domain

A sphere of activity, influence or knowledge related to a specific physical or conceptual property.

Note: In joint doctrine, the domains are physical, moral and informational. [DTB Record 34947]

NATO▶ The sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent to achieve desired effects. [AJP-3.20]

honeynet

A virtual environment consisting of multiple honeypots, designed to deceive an intruder into assuming that he or she has located a network of computing devices of targeting value. [Tallinn Manual 2.0]

JDN 2017-02
(PROMULGATION DRAFT)

honeypot

A deception technique in which a person seeking to defend computer systems against malicious cyber operations uses a physical or virtual environment designed to lure the attention of intruders with the aim of: deceiving the intruders about the nature of the environment; having the intruders waste resources on the decoy environment; and gathering counter-intelligence about the intruder's intent, identity, and means and methods of cyber operations. Typically, the honeypot is co-resident with the actual systems the intruder wishes to target. [Tallinn Manual 2.0]

information technology system (ITS)

Computers, networks, and networked devices, including all associated hardware, firmware and software used to transmit, process or store data and/or control mechanical devices.

key terrain

LAND CONTEXT► Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant. [DTB Record 4612]

CYBER CONTEXT► See cyber key terrain

offensive cyber operation (OCO)

An offensive operation intended to project power in or through cyberspace to achieve effects in support of military objectives. [DTB Record 693752]

NATO► Activities that project power to achieve military objectives, in or through, cyberspace. [AJP-3.20]

US► Cyberspace operations intended to project power by the application of force in or through cyberspace. [JP 3-12]

network

A number of interconnected computers, machines, or operations. [*Oxford Dictionary of Computing*]

phishing

[The use of] “falsified” e-mails to lead consumers to counterfeit Web sites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. [TermiumPlus]

spear phishing

A phishing attack that focuses on a single user or department within an organization, addressed [apparently] from someone within the company in a position of trust and requesting information such as login IDs and passwords. [TermiumPlus]

JDN 2017-02
(PROMULGATION DRAFT)

support cyber operation (SCO)

A network operation tasked by, or under direct control of, a commander to support offensive and defensive cyber operations. [DTB Record 694337]

vital ground

Ground of such importance that it must be retained or controlled for the success of the mission.
[DTB Record 1529]

JDN 2017-02
(PROMULGATION DRAFT)

This page was intentionally left blank

JDN 2017-02
(PROMULGATION DRAFT)

List of Abbreviations

AOR	area of responsibility
ARA	authority, responsibility, accountability
C2	command and control
CAF	Canadian Armed Forces
CCEB	Combined Communications Electronics Board
CCIR	commander's critical information requirement
CD IRT	cyber defence immediate reaction team
CDS	Chief of the Defence Staff
CFDS	<i>Canada First Defence Strategy</i>
CIRT	computer incident response team
CIS	communication and information systems
CJOC	Canadian Joint Operations Command
COA	course of action
CONOP	concept of operation
CSE	Communications Security Establishment
DCO	defensive cyber operation
DCO-IDM	defensive cyber operation (internal defensive measures)
DCO-RA	defensive cyber operation (response action)
D Cyber FD	Director Cyber Force Development
FD	force development
FE	force employment
FG	force generation
GC	Government of Canada
ICCWG	International Computer Network Defence Coordination Working Group
IP	Internet Protocol
IPE	intelligence preparation of the environment
IT	information technology
ITS	information technology system
I&W	Indications and Warnings
J2	Joint Staff, Intelligence
J3	Joint Staff, Operations
J5	Joint Staff, Plans
J6	Joint Staff, Communication Information Systems
LOAC	law of armed conflict

JDN 2017-02
(PROMULGATION DRAFT)

NCIRC	NATO Cyber Incident Response
OCO	offensive cyber operation
OPCON	operational control
OPE	operational preparation of the environment
OPORD	operation order
OPP	operations planning process
PIR	priority intelligence requirements
PSC	Public Safety Canada
R&D	Research and Development
RFI	request for information
ROE	rules of engagement
SCO	support cyber operation
SSC	Shared Services Canada
TTP	tactics, techniques and procedures

JDN 2017-02
(PROMULGATION DRAFT)

List of References

Government of Canada

- A. *Canada's Cyber Security Strategy* (2010)
- B. Policy on Government Security (1 July 2009)
- C. *Government of Canada Cyber Security Event Management Plan* (GC SEMP), 2015.
<http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/sim-gsi/msi-gis/csemp-pgec-eng.asp#toc1-5> [accessed 2016-09-15]

Department of National Defence

- D. *Canada First Defence Strategy*.
- E. *Defence Terminology Bank*.
- F. DND/CAF Policy on CAF Computer Network Operations (Interim, December 2012)
- G. DM and CDS Initiating Directive for Cyber Mission Assurance Program Development (17 January 2017)
- H. Integrated Capstone Concept [for Cyber Operations] (2010)

Canadian Armed Forces

- I. Perron, LCol J.P.M. "Decision on Command and Control for Cyber." Briefing Note for the CDS. (6 October 2016)
- J. CDS Guidance to the CAF (June 2013)
- K. CDS Initiating Directive for Defensive Cyber Operations (February 2015)
- L. CAF Cyber Operations Primer (February 2014)
- M. Canadian Forces Network Operations Centre Concept of Operations (16 Jan 2011)
- N. CFJP 01, *Canadian Military Doctrine* (B-GJ-005-000/FP-001) (September 2011)
- O. CFJP 2-0, *Intelligence* ((B-GJ-005-200/FP-001) (October 2011)
- P. CFJP 2-1.1, *Intelligence Preparation of the Operational Environment*
- Q. CFJP 2-7, *Joint Intelligence, Surveillance, and Reconnaissance*
- R. CFJP 3-0, *Operations* (B-GJ-005-300/FP-001) (September 2011)

JDN 2017-02
 (PROMULGATION DRAFT)

- S. CFJP 3-0.1, *The Law of Armed Conflict at the Operational and Tactical Levels* (B-GJ-005-104/FP-001)
- T. CFJP 3-9, *Targeting* (B-GJ-005-309/FP-001) (December 2014)
- U. CFJP 3.10 *Information Operations* (B-GJ-005-310/FP-001) (April 1988)
- V. CFJP 5-0, *The Canadian Forces Operational Planning Process* (B-GJ-005-500/FP-001) (April 2008)
- W. CFJP 5-1, *Use of Force for CF Operations*,
- X. CJOC Website, “Op IMPACT,” <http://cjoc-coic.mil.ca/sites/intranet-eng.aspx?page=17919> [accessed 2016-12-07]
- Y. Defensive Cyber Operations: Functional Concept (Draft, 28 February 2013)
- Z. Not allocated
- AA. Future Security Environment 2013-2014 (2014)
- AB. JDN 03-2014, *Operations Security*
- AC. Maillé, Julie and Louise Baillargeon. “A Doctrine for Individual Training and Education,” <http://www.journal.forces.gc.ca/vol16/no4/page68-eng.asp> [accessed 2017-02-16]
- AD. Strategic Review of NORAD Cyberspace Warning and Defence
- AE. Yarker, D.R. LCol. “A Concept for CAF Cyber Operations.” Service paper. (16 Apr 2015)

Other Government of Canada Departments and Agencies

- AF. Bernier, Melanie and Joanne Treurniet, “CF Cyber Operations in the Future Cyber Environment Concept”, Ottawa: DRDC CORA TM2009-058 (December 2009)
- AG. Bernier, Melanie and Kathryn Perrett, “Mission-Function-Task (MFT) Analysis for Cyber Defence”, DRDC STO-MP-IST-999
- AH. *CSIS 2018 Security Outlook: Potential Risks and Threats*. June 2016.
- AI. *TermiumPlus* <http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-fra.html?lang=fra&srchtxt=&i=1&index=alt> [accessed 2016-09-15]

United Kingdom

- AJ. *Cyber Primer*, 2nd Ed. (July 2016)
- AK. JDN 3/12, *Cyber Operations: The Defence Contribution*
- AL. JDP 0-50, *Cyber Doctrine* (December 2015)

JDN 2017-02
 (PROMULGATION DRAFT)

- AM. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a digital World* (November 2011)
- AN. “Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review” (October 2010)

United States

- AO. Clapper, James R. “Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee” (9 February 2016)
- AP. DoD Strategy for Operating in Cyberspace (July 2011).
<http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>
 [accessed 2017-02-16]
- AQ. JP 3-0, *Joint Operations* (11 August 2011)
- AR. JP 3-12, *Cyber Operations* (5 February 2013)
- AS. US Cyber Command. “Operational Concept for Defensive Cyberspace Operations” (23 May 2016)
- AT. PPD-41, US Presidential Policy Directive , *United States Cyber Incident Coordination*, 26 July 2016. <http://assets.documentcloud.org/documents/2998812/Read-the-official-White-House-directive-on-cyber.pdf> [2017-05-15]

NATO

- AU. AJP-3.20. *Allied Joint Doctrine for Cyberspace Operations* (Draft, version 1)
- AV. Applegate, Scott D. “The Principle of maneuver in Cyber Operations,” *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012.
- AW. Concept on NATO’s Cyber Defence (March 2011)
- AX. Cyber Defence Committee. “Initial Comprehensive Assessment of the Utility and Possible Implications for the Alliance of Recognizing Cyberspace as a Domain ” (23 March 2016)
- AY. Geers, Kenneth , ed. “Cyber War in Perspective: Russian Aggression against Ukraine”; Tallinn, NATO CCD COE Publications, 2015.
- AZ. “Multinational Defensive Cyber Operations: A Planning Guide to Producing an Initial Staff Estimate for Multinational Defensive Cyber Operations” (18 July 2016)
- BA. NATO Cyber Defence Concept for Military Operations (June 2012)
- BB. NATO Cooperative Cyber Defence Centre of Excellence, “Cyber War in Perspective: Russian Aggression Against Ukraine”; accessible at: <https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html> [accessed 2016-02-26]
- BC. NATO Fact Sheet – NATO Cyber Defence (July 2016)
- BD. NATO. Press Conference, 14 June 2015.
http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en [accessed 2016-11-29]

JDN 2017-02
 (PROMULGATION DRAFT)

- BE. NATO Warsaw Summit Communiqué, para 70&71, 9 July 2016;
<https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommuniqué.pdf>
 [accessed 2017-02-16]
- BF. Schmitt, Michael N., ed. (NATO Cooperative Cyber Defence Centre of Excellence). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2017.
- BG. “Strategy on NATO’s Role in Countering Hybrid Warfare” (November 2015)

France

- BH. Cyberdéfense. Doctrine interarmée. 2014

United Nations

- BI. 1977 Additional Protocol I to the 1949 Geneva Conventions
- BJ. United Nations Charter

Other

- BK. Ackerman, Spencer. “US Central Command Twitter account hacked to read ‘I love you ISIS’”. *The Guardian*. <http://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack> [accessed 2016-09-14]
- BL. Bender, Jason M. “The Cyber Planner: Challenges to Education and understanding of Offensive Cyberspace Operations.” 2013.
- BM. Brantly, Aaran F. “Strategic Maneuver”. *Small Wars Journal*, 17 October 2015
- BN. Clark, David. “Characterizing Cyberspace: Past, Present and Future”. MIT CSAIL (v. 1.2, March 2010)
- BO. Colarik PhD, Andrew M. and Iech Janczewski DEng. “Establishing Cyber Warfare Doctrine”. *Journal of Strategic Security, Volume 5 Number 1* Spring 2012, Article 7.
- BP. Gioe, Dr David. “Can the Warfare Concept of maneuver be Usefully Applied in Cyber Operations?” *The Cyber Defence Review*. Accessed from <http://www.cyberdefensereview.org/2016/01/14warfare-concept/> [accessed 2016-06-15]
- BQ. Hillier, Paul, ed. *Papers from the 15th Annual Graduate Student Symposium -Looking Beyond*. CDA Institute, Canadian Security Interests, 2013.
- BR. Houghton, General Sir Nicholas. “Building a British military fit for future challenges rather than past conflicts,” speech delivered at the Chatham House international affairs think tank on 16 September 2015. <https://www.gov.uk/government/speeches/building-a-british-military-fit-for-future-challenges-rather-than-past-conflicts> [accessed 2016-12-21]
- BS. Kelley, Colonel Olen L. “Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative”. 2008

JDN 2017-02
 (PROMULGATION DRAFT)

- BT. Korns, Stephen W and Joshua E. Kastenberg, “Georgia’s Cyber Left Hook”, 2009. <http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/08winter/korns.pdf> [accessed 2017-02-16]
- BU. Leed, Mauren. “Offensive Cyber Capabilities at the Operational Level: The Way Ahead”. *Center for Strategic & International Studies*, Washington, DC. 2013. http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf [accessed 2016-11-02]
- BV. McGuffin, Chris and Paul Mitchell. “On Domains: Cyber and the Practice of Warfare.” *International Journal: Canada’s Journal of Global Policy Analysis*. 16 July 2014 <http://ijx.sagepub.com/content/early/2014/07/16/0020702014540618> [accessed 2016-04-05]
- BW. MITRE. *MITRE Systems Engineering Guide*. <https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/cyber-mission-assurance> [accessed 2016-11-02]
- BX. Soanes, Catherine and Angus Stevenson, ed. *Concise Oxford English Dictionary, 11th ed.* New York: Oxford University Press, 2004.
- BY. Pope, Billy. “Cyber Power: A Personal Theory of Power”. *Center for International Maritime Security*. May 28, 2014. <http://cimsec.org/cyber-power-personal-theory-power/11436> [accessed 2016-06-08]
- BZ. Sanger, David E and Martin Fackler. “NSA Breached North Korean Networks Before Sony Attack, Official Say”, *New York Times*. Jan 18 2015. http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0; [accessed 2017-02-16]
- CA. Schmitt, Michael N. “Attack as a Term of Art in International Law: The Cyber Operations Context” http://ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf [accessed 2015-09-15]
- CB. Schmitt; “International Law and Cyber Attacks: Sony v. North Korea,” 17 December 2014. <https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea> [accessed 2016-03-22]
- CC. Schmitt, Michael N. “Tallinn Manual on the International Law Applicable to Cyber Warfare” Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence. <https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf> [accessed 201702-16]
- CD. Sindrey, Maj G.G. “International Law Applied to Cyberwarfare and the Attribution Challenge”. Canadian Forces College. JCSP 40. Solo Flight Paper.

JDN 2017-02
(PROMULGATION DRAFT)

- CE. Tiezzi, Shannon; “China (Finally) Admits to Hacking: An updated military document for the first time admits that the Chinese government sponsors offensive cyber units; *The Diplomat*, 18 March 2015. <http://thediplomat.com/2015/03/china-finally-admits-to-hacking/> [accessed 2016-12-06]
- CF. Tikk, Eneken, Kadri Kaska, Liis Vihul. “International Cyber Incidents: Legal Considerations.” Cooperative Cyber Defence Centre of Excellence. 2010.
- CG. TRUNews; *Putin Updates Russian Cyber Doctrine*, 6 December 2016. <http://www.trunews.com/article/putin-updates-russian-cyber-doctrine> [accessed 2016-12-06]
- CH. Waters, Gary, Desmond Ball and Ian Dudgeon. “Australia and Cyber-Warfare”. Canberra: Australian National University E Press, 2008.
- CI. Weeden, Jen. “Beyond ‘Cyber War’: Russia’s Use of Strategic Cyber Espionage and Information Operations in Ukraine”. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Weedon_08.pdf [accessed 2016-11-03]
- CJ. Williams, Brett. “Cyberspace: What is it, where is it and who cares?” *Armed Forces Journal*. March 13, 2014. <http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/> [accessed 2016-01-18]
- CK. Williams, Brett. “The Joint Force Commander’s Guide to Cyberspace Operations” *JFQ 2nd Quarter* 2014. <http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations/> [accessed 2017-02-16]
- CL. Williams, Pete, Robert Windrem and Andrea Mitchell; *NBC News*: “North Korea Behind Sony Hack: U.S. Officials.” NBC News. <http://www.nbcnews.com/news/world/north-korea-behind-sony-hack-u-s-officials-n270451> [accessed 2016-08-12]
- CM. Winterfeld, Steve and Jason Andress. “The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice”. Waltham, MA, Elsevier, 2013.

From:

Sent:

To:

Subject:

January 16, 2020 10:53 AM

FW: Stakeholders Review - Update of the JDN on Cyber Operations, Part 2 of 3 (ch 2)

As discussed.

From:

Sent: January 14, 2020 11:06 AM

To:

Subject: RE: Stakeholders Review - Update of the JDN on Cyber Operations, Part 2 of 3 (ch 2)

Good day reviewers,

If you are still in the process of reviewing chapter 2, please do not review section 6 -

This whole section will be have to be 'rethought'.

We're still aiming for 17 Jan. Thanks to those who provided their feedback already.

Thank you.

From:

Sent: December 13, 2019 11:54 AM

To:

Subject: RE: Stakeholders Review - Update of the JDN on Cyber Operations, Part 2 of 3 (ch 2)

Good day all,

The return date for this has been pushed back to **17 Jan 2020**.

Thank you.

From:

Sent: November 20, 2019 12:35 PM

To:

Subject: Stakeholders Review - Update of the JDN on Cyber Operations, Part 2 of 3 (ch 2)

Good day,

Following our request for comments regarding the Updated JDN on Cyber Operations, we have received great feedback from many of you along with designated points of contact. We are actively working on integrating this information and may get back to some of you on it as needed.

The **Second Section** (Chapter 2) is now available for review and comments. It can be accessed at the following link (you will have to click on *Edit Document* at the top of the screen):

As a reminder, the track changes feature has been activated and improvements may directly be proposed by making text modifications for small changes, or by inserting comments for more extensive modifications or additions (this is the preferred method and is highly encouraged).

All the recipients of this email have been given access to this file. If this is not the case, please send myself an email. I invite you to share this with other members of your group and we can provide access to the file upon request.

We aim at sending to all points of contact the **last section for review in roughly two weeks**. A meeting with the points of contact could follow to resolve any remaining items.

Note that if you have not already provided your comments on Part 1 (Chapter 1), the SharePoint link is:

Please let us know of any new comments you insert there to ensure they are taken into account.

Do not hesitate to contact
this.

should you have any questions regarding

Best Regards,

From:
Sent: January 16, 2020 2:52 PM
To:
Cc:
Subject: JDN Ch 1_Feedback
Attachments: Cyber JDN Ch 1 - STAKEHOLDERS REVIEW_ docx
Importance: High

Sir,

Please find the JDN Ch 1 with comments that I have injected.

Very respectfully,



**Pages 127 to / à 146
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1), 21(1)(b)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

From:
Sent: January 16, 2020 4:19 PM
To:
Cc:
Subject: FW: JDN Ch 1_Feedback
Attachments: Cyber JDN Ch 1 - STAKEHOLDERS REVIEW_ docx

See CFINTCOM comments on Ch 1. Feedback on Ch 2 to follow (maybe early next week).

Cheers,

From:
Sent: January 16, 2020 2:52 PM
To:
Cc:
Subject: JDN Ch 1_Feedback
Importance: High

Sir,

Please find the JDN Ch 1 with comments that I have injected.

Very respectfully,

From:
Sent: November 20, 2019 12:35 PM
To:


Subject: Stakeholders Review - Update of the JDN on Cyber Operations, Part 2 of 3 (ch 2)

Good day,

Following our request for comments regarding the Updated JDN on Cyber Operations, we have received great feedback from many of you along with designated points of contact. We are actively working on integrating this information and may get back to some of you on it as needed.

s.15(1)

s.16(2)(c)

The **Second Section** (Chapter 2) is now available for review and comments. It can be accessed at the following link (you will  to click on *Edit Document* at the top of the screen):

As a reminder, the track changes feature has been activated and improvements may directly be proposed by making text modifications for small changes, or by inserting comments for more extensive modifications or additions (this is the preferred method and is highly encouraged).

All the recipients of this email have been given access to this file. If this is not the case, please send myself an email. I invite you to share this with other members of your group and we can provide access to the file upon request.

We aim at sending to all points of contact the **last section for review in roughly two weeks**. A meeting with the points of contact could follow to resolve any remaining items.

Note that if you have not already provided your comments on Part 1 (Chapter 1), the SharePoint link is:

Please let us know of any new comments you insert there to ensure they are taken into account.

Do not hesitate to contact
this.

should you have any questions regarding

Best Regards,

**Pages 150 to / à 169
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1), 21(1)(b)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

From:
Sent: January 16, 2020 4:20 PM
To:
Cc:
Subject: RE: JDN Ch 1_Feedback

Great comments.

Thanks,

From:
Sent: January 16, 2020 2:52 PM
To:
Cc:
Subject: JDN Ch 1_Feedback
Importance: High

Sir,

Please find the JDN Ch 1 with comments that I have injected.

Very respectfully,

From:
Sent: January 17, 2020 10:01 AM
To:
Cc:
Subject: RE: JDN Ch 1_Feedback

Sir,

Thank you for your comments. And as mentioned in previous email for ch 2: Do not review section 6 -

From:
Sent: January 16, 2020 4:19 PM
To:
Cc:

Subject: FW: JDN Ch 1_Feedback

See CFINTCOM comments on Ch 1. Feedback on Ch 2 to follow (maybe early next week).

Cheers,

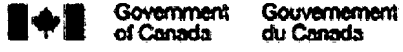
From:
Sent: January 16, 2020 2:52 PM
To:
Cc:
Subject: JDN Ch 1_Feedback
Importance: High

Sir,

Please find the JDN Ch 1 with comments that I have injected.

s.15(1)

Very respectfully,



Canada

From:
Sent: November 20, 2019 12:35 PM
To:

Subject: Stakeholders Review - Update of the JDN on Cyber Operations, Part 2 of 3 (ch 2)

Good day,

Following our request for comments regarding the Updated JDN on Cyber Operations, we have received great feedback from many of you along with designated points of contact. We are actively working on integrating this information and may get back to some of you on it as needed.

The **Second Section** (Chapter 2) is now available for review and comments. It can be accessed at the following link (you will have to click on *Edit Document* at the top of the screen):

As a reminder, the track changes feature has been activated and improvements may directly be proposed by making text modifications for small changes, or by inserting comments for more extensive modifications or additions (this is the preferred method and is highly encouraged).

All the recipients of this email have been given access to this file. If this is not the case, please send myself an email. I invite you to share this with other members of your group and we can provide access to the file upon request.

We aim at sending to all points of contact the **last section for review in roughly two weeks**. A meeting with the points of contact could follow to resolve any remaining items.

Note that if you have not already provided your comments on Part 1 (Chapter 1), the SharePoint link is:

Please let us know of any new comments you insert there to ensure they are taken into account.

Do not hesitate to contact
this.

should you have any questions regarding

Best Regards,

From:
Sent: January 17, 2020 2:49 PM
To:
Subject: RE: JDN Ch 1_Feedback

Wilco, and I'll ask them to add you to the dist list.

Cheers,

From:
Sent: January 17, 2020 8:56 AM
To:
Subject: RE: JDN Ch 1_Feedback

I heard about this JDN rewrite earlier this week at the Cyber FD Coord. But had not seen any correspondence reaching CFINTCOM before this.

Could you please signal a provisional response to Cyber. We have been working with DG Cyber FD to look at some aspects of Int support to Cyber Activities based upon the It might
be worthwhile looking at this to ensure that they are lining up.

Thanks,

From:
Sent: January-16-20 4:19 PM
To:
Cc:

Subject: FW: JDN Ch 1_Feedback

See CFINTCOM comments on Ch 1. Feedback on Ch 2 to follow (maybe early next week).

Cheers,

From:
Sent: January 16, 2020 2:52 PM
To:
Cc:
Subject: JDN Ch 1_Feedback
Importance: High

Sir,

Please find the JDN Ch 1 with comments that I have injected.

Very respectfully,



Canada

From:
Sent: November 20, 2019 12:35 PM
To:

s.15(1)

s.16(2)(c)

Subject: Stakeholders Review - Update of the JDN on Cyber Operations, Part 2 of 3 (ch 2)

Good day,

Following our request for comments regarding the Updated JDN on Cyber Operations, we have received great feedback from many of you along with designated points of contact. We are actively working on integrating this information and may get back to some of you on it as needed.

The **Second Section** (Chapter 2) is now available for review and comments. It can be accessed at the following link (you will have to click on *Edit Document* at the top of the screen):

As a reminder, the track changes feature has been activated and improvements may directly be proposed by making text modifications for small changes, or by inserting comments for more extensive modifications or additions (this is the preferred method and is highly encouraged).

All the recipients of this email have been given access to this file. If this is not the case, please send myself an email. I invite you to share this with other members of your group and we can provide access to the file upon request.

.15(1)

s.16(2)(c)

We aim at sending to all points of contact the **last section for review in roughly two weeks**. A meeting with the points of contact could follow to resolve any remaining items.

Note that if you have not already provided your comments on Part 1 (Chapter 1), the SharePoint link is:



Please let us know of any new comments you insert there to ensure they are taken into account.

Do not hesitate to contact
this.

should you have any questions regarding

Best Regards,

From: [REDACTED]
Sent: January 23, 2020 8:31 AM
To:
Subject: RE: JDN Ch 1_Feedback
Attachments: Cyber JDN Ch 2 - REVIEW e.docx

Sir,

Please see the attached review. A significant gap that I have observed is in para 4.4.1,

Very respectfully,

 of Canada du Canada



From:
Sent: January 16, 2020 4:19 PM
To:
Cc:

Subject: FW: JDN Ch 1_Feedback

See CFINTCOM comments on Ch 1. Feedback on Ch 2 to follow (maybe early next week).

Cheers,

s.15(1)

From:
Sent: January 16, 2020 2:52 PM
To:
Cc:
Subject: JDN Ch 1_Feedback
Importance: High

Sir,

Please find the JDN Ch 1 with comments that I have injected.

Very respectfully,



Canada

From:
Sent: November 20, 2019 12:35 PM
To:

Subject: Stakeholders Review - Update of the JDN on Cyber Operations, Part 2 of 3 (ch 2)

Good day,

Following our request for comments regarding the Updated JDN on Cyber Operations, we have received great feedback from many of you along with designated points of contact. We are actively working on integrating this information and may get back to some of you on it as needed.

The **Second Section** (Chapter 2) is now available for review and comments. It can be accessed at the following link (you will have to click on *Edit Document* at the top of the screen):

As a reminder, the track changes feature has been activated and improvements may directly be proposed by making text modifications for small changes, or by inserting comments for more extensive modifications or additions (this is the preferred method and is highly encouraged).

All the recipients of this email have been given access to this file. If this is not the case, please send myself an email. I invite you to share this with other members of your group and we can provide access to the file upon request.

We aim at sending to all points of contact the **last section for review in roughly two weeks**. A meeting with the points of contact could follow to resolve any remaining items.

Note that if you have not already provided your comments on Part 1 (Chapter 1), the SharePoint link is:

Please let us know of any new comments you insert there to ensure they are taken into account.

Do not hesitate to contact
this.

should you have any questions regarding

Best Regards,

Page 181

**is withheld pursuant to section
est retenue en vertu de l'article**

15(1)

**of the Access to Information Act
de la Loi sur l'accès à l'information**

**Pages 182 to / à 204
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1), 21(1)(b)

**of the Access to Information Act
de la Loi sur l'accès à l'information**