DRDC | RDDC
technologysciencetechnologie

Identifying Requirements for a Cyber Common Operating Picture (CyCOP): Information Collection

Henry Doucette
DBHS Security Consulting Inc

Prepared by:
DBHS Security Consulting Inc
RPO Rideau Centre PO Box 53292
Ottawa, Ontario K1N 1C5
Contractor Document Number: C20-0224-03427
Contract Number: W6369-19-X024
Technical Authority: Abderrahmane Sokri, Defence Scientist
Contractor's date of publication: February 2020

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2020-C054
March 2020

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

DBHS
SECURITY CONSULTING INC
- Intelligent use of Security -

24 February 2020

C20-0224-03427_Document.docx

Henry Doucette

DBHS Security Consulting Inc

RPO Rideau Centre PO Box 53292
Ottawa, Ontario K1N 1C5

Contract Number: W6369-19-X024

Contract Technical Authority: Dr. Abderrahmane Sokri, DGSTCO, DRDC CORA

Abstract

The cyber domain is a unique, but complex battlefield, presenting commanders with an equally complex situational awareness (SA) problem. Cyber SA, which provides the commander with an understanding of the battlefield, can be improved through an informed cyber common operating picture (CyCOP). Such a CyCOP requires a knowledgebase, which is the underlying Cyberspace data that provides details about cyber adversaries, targets, and friendly defence capabilities. Collection of such data can be effectively achieved through a systematic collection plan, similar to the military information collection plan (ICP). This work employed the ICP approach to collect, from all layers of Cyberspace, all useful cyber information that could be used to understand friendly and adversary security postures in Cyberspace. In an effort to determine the requirements of establishing a CyCOP, the work systematically populates a generic ICP covering various possible scenarios. The resulting spreadsheet can be used as a starting point in generating mission specific ICPs and developing data models for a CyCOP. In the short term, this ICP will be used to develop data models for a few CyPOC use cases for demonstration.

Résumé

Le domaine cybernétique est à la fois unique et complexe et représente un véritable défi aux commandants opérationnels. La situation cybernétique, qui fournit aux commandants opérationnels et à leur personnel une compréhension du champ de bataille, peut être améliorée par une bonne situation opérationnelle commune dans le domaine cybernétique (CySOC). Un tel outil exige une base de connaissances sur les cyber-adversaires, les cibles, et les capacités de défense amies. Ceci pourrait s'effectuer à travers un plan de collecte systématique similaire au plan de collecte de données (PCD) militaire. Ce travail utilise l'approche du PCD au niveau des trois paliers du cyberespace pour comprendre la position sécuritaire des amis et des adversaires. Dans l'objectif d'identifier les exigences pour l'établissement d'une CySOC, le travail a systématiquement complété un PCD générique couvrant différents scénarios. Le tableur résultant peut servir comme un point de départ pour développer des PCD plus spécifiques et d'autres modèles de données pour la CySOC. Le PCD générique sera utilisé à court terme dans des études de cas illustratives.

Table of Contents

1. Introduction

This document addresses the Statement of Work (W6369-19-X024) from Defence Research and Development Canada (DRDC). It should be accompanied by an Excel spreadsheet of the same name that will be available from the technical authority (TA). The work was conducted for the Non-Munitions Targeting Sciences (NMTS) project of the DRDC Centre for Operational Research and Analysis (CORA) Science and Technology (S&T) program. The work's objective is to provide scientific support to the Canadian Forces Warfare Centre (CFWC) in establishing requirements of a cyber common operating picture (CyCOP).

The work provides a functional, high-level plan to identify the information required to address the requirements for establishing a Cyber Common Operating Picture (CyCOP). Unlike kinetic warfare where operations and strategic commanders and their staffs (OSC&S) have a good understanding of their common operating picture (COP), such a level of understanding does not currently exist in the cyber domain. The Joint Doctrine Note on Cyber Operations (JDNCO) has identified the need for a CyCOP to support situational awareness (SA), information sharing and collaboration [1]. This project aims to establish the requirements for such a COP for cyber operations.

Based on earlier analyses [2], the best way to establish these CyCOP requirements is to begin by determining all the information sources that would be required. Those information sources are expected to address specific CyCop questions in the cyber domain as defined by its three layers (i.e., physical, logical and persona). A good way to collect all the relevant information for a CyCop is to use an information collection plan (ICP) similar to the one used by military intelligence experts [2]. DRDC established that, by using this approach, only the information relevant to the CyCOP is collected and

analyzed, avoiding the possibility of collecting irrelevant information. This report documents the research conducted to develop a comprehensive CyCOP ICP for each Cyberspace layer and provides all the detail necessary for collecting such information in the cyber domain.

2. The Information Collection Plan (ICP) Format

This section outlines the format of the ICP used in the spreadsheet. The ICP is laid out in a typical table format with several columns that are intended to provide as much information to the Commander as is required. Table 1 shows the basic structure of the ICP.

Table 1: The structure of an ICP – (continued on page 5)

CCIR	PIR	IR	Indicators
1: What does the Commander need to know? …	1. Does PAX have a motive to attack the CAF? 2. … …	1.1 Has PAX shown interest in attacking CAF?	1.1.1
			1.1.2
			1.1.3. … ….
		1.2 Has PAX collected CAF information in the Cyber Domain, previously? …	1.2.1
			1.2.2 …

The first column of Table 1 identifies the questions most critical to a mission, which are referred to as the Commander's Critical Information Requirements (CCIRs). This overarching term addresses the primordial concerns about which a decision-maker will need to know in order to make the correct decisions.[1] The table shows one such high level question, which is generically stated as: What does the Commander need to know? To provide answers to this very high-level question requires more finer-grained questions that concern the adversary, threat, or hostile actor, which we collectively refer to as Potential Adversary X (PAX). These more detailed questions are known as Priority Intelligence Requirements (PIRs), which are shown in column 2 of Table 1.

PIRs are the high-level questions that address the Commander's intelligence requirements.[2] These requirements provide a full understanding of the PAX and friendly cyber security postures. Although the decision-maker approves and is ultimately responsible for the information collected or gaps not addressed, it is the cyber information collection staff's (or in more general terms, intelligence officer) principal responsibility to create these, regardless of the level at which the headquarters sits.[3]

[1] Canadian Forces Joint Publication 2.0, "Intelligence", Government of Canada, 2017.
[2] The ICP created herein is compliant with CFINTCOM production standards, as well as NATO / Allied Intelligence STANAGs.
[3] These staff principals are also commonly known as: G2, N2, J2, or S2.

To make the PIRs more actionable and allow for a more detailed understanding of what the Commander needs to know, they are broken down into several sub-questions, known as Information Requirements (IRs). The IRs, which are shown in the third column of Table 1, focus on capability, intent and opportunity. IRs also allow the collectors, sources, or agencies to collect against the problem by defining what to look for.

Lastly, IRs are broken down into even smaller bits of information that are sometimes referred to as the Essential Elements of Information (EEIs) or indicators, which are shown in the last column of Table 1. The indicators tell the collector (source or agency) what the information will look like, what to specifically look for, and/or what they might see. The presence of these indicators (whole or in part), provides an initial level of confirmation that the IR has been answered. Multiple IRs answered, from more than one source/collector, ensures that the decision maker has not been deceived, and that the information collected is likely accurate.

One of the key benefits of an ICP is that it will also allow the analyst to detect new adversary events or attempts and previously unseen tactics techniques and practices (TTPs). This is made possible by the way the ICP uses high-level and purposely broadens questions to orient analyses, without becoming too specific or allowing assumptions/bias to inadvertently narrow the scope of the collection. Thus, the decision maker must remain agnostic to the how but instead focus on what all or any type of attack might look like across the unit's boundaries in cyberspace.

Because the ICP is at the starting point of the information collection cycle, its vast scope means that the Commander (or decision-maker) must endorse the prioritization of collection by their assets, as well as the authority to use this plan to task other sources and agencies. That brings us to the second part of the ICP that deals with the sources and formats of the information collected. This is shown in Table 1 below.

The first column in the table identifies the different sources of information to identify the indicators mentioned in column 4 of Table 1. Examples of such sources are shown in the table and include all sources, open sources, human intelligence (HUMINT), Technical Intelligence (TECHINT), Signals Intelligence (SIGINT), and Imagery Intelligence (IMINT). In this document, the source types suited to collecting specific information have an "**X**" indicating that the analyst should source information from such groups to get this information and report it. The best-suited or more authoritative source has "**XX**" to indicate its importance. Every unit or mission may have its own sources, so the table can be tailored to suit different situations.

Table 1 Continued from page 3: The structure of an ICP

Sources						Information Specifications		
All Source	Open	HUMINT	TECHINT	SIGINT	IMINT	Standards	Language	T & T
X		X	X	X	X	1.1.1.1 Unstructured	E	RSS feeds
…	…	…	…	…	…	…	…	…

Finally, the ICP lists the format of the information that can be collected using this plan. For example, intelligence information could be unstructured data, or it could have been obtained through web logs that are in an Internet Information Services (IIS) format for example. All this information is useful in creating data models for the CyCOP.

The rest of the document provides more detail on the ICP. Note that this report must be used with the electronic spreadsheet that contains the details of the ICP. The spreadsheet is available from the Contract Technical Authority.[4]

3. Order of Priority

The PIRs, IRs, and indicators in this document are listed in order of priority. This allows for the prioritization of PIRs of a higher priority to be actioned ahead of lower priority ones in the event that timing or resource availability or conflicting orders. Thus PIR 1.2 has a higher priority than PIR 3.4. Such information would be reflected in the CyCOP and it would be up to the commander on how such information should be exploited to improve their SA. For this work, the contractor (author) used his knowledge and experience in cyber security and intelligence information collection to qualitatively rank the PIRs, IRs, and indicators where necessary.

The decision makers must review this prioritization (and the completeness of each question) on a regular basis. Based on the author's knowledge and experience, it is recommended that this review be conducted not less than quarterly to ensure relevance, need, and accuracy of collection. In addition, the review can be used when there is a need for change (i.e. the development of new IRs or even PIRs), especially as the situation changes.

[4] maxwell.dondo@drdc-rddc.gc.ca; Abderrahmane.Sokri@forces.gc.ca

4. Examples of Information at Various Cyber Layers

As shown in Figure 1, the cyber domain is made up of the physical, logical and the cyber persona layers.

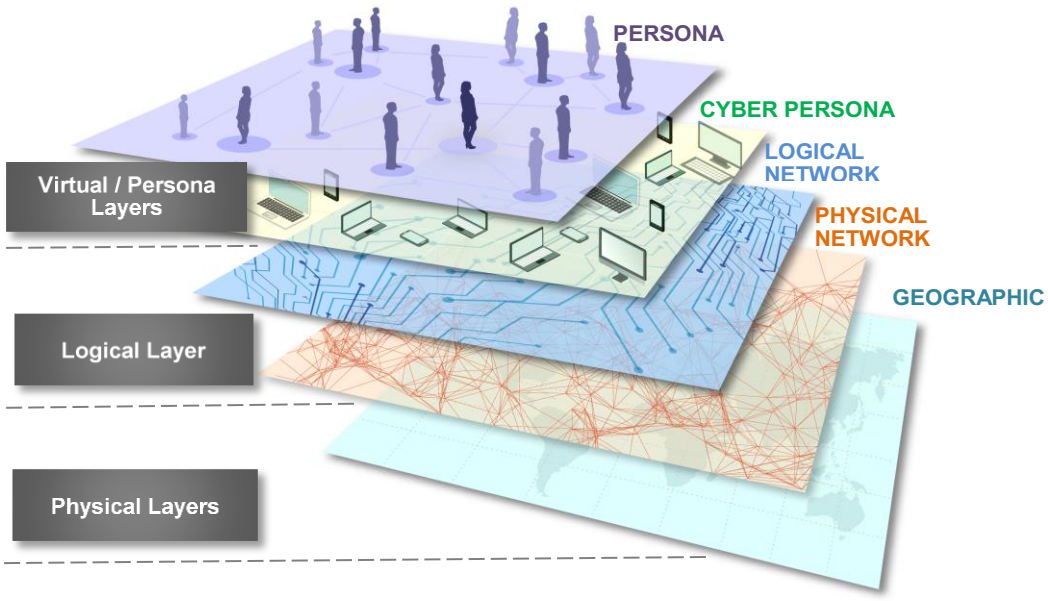

Figure 1 Cyber domain layer

An ICP is the first step in the intelligence collection process by providing direction. In order to collect the information, the intelligence staff will then develop an Intelligence, Surveillance and Reconnaissance (ISR) plan, which outlines where, and when to collect and on which layer of cyberspace the information is applicable. That information will then be incorporated into the CyCOP. Information must be collected to cover all the layers. Examples of such information collection is provided in Tables 2-4. While the tables complement the ICP information, they also provide the tools that are needed to collect such information. While our tables are not exhaustive, it is expected that a complete ICP for the CyCOP would provide more technical information that would be useful for commanders in achieving mission objectives.

4.1 Physical layer

Table 2: Examples of information at the physical layer

What I need to know	Reason	Formats, standards, language	Tools
Location	Where my cyber assets are physically located?	GPS, maps, proprietary images	GIS, ESPI, Mobac atlas, Openstreet maps, Maxmind (IP geolocation)
Environment	How cyber assets/operations could be affected by extreme weather patterns such as flooding?	RSS feeds, unstructured (from public safety, environment Canada, etc), CAF WAS	Proprietary
Threats	Is prone to disruptive activities such as restive population, treaty violations, etc	Unstructured, proprietary	Law enforcement, crime map
Asset type	What type of assets (e.g. routers, switches, badge scanners)?	Asset Inventory (e.g. human managed spreadsheet), proprietary, schematics	Tag scanners, CAD drawings, proprietary
Communication mode	How cyber assets communicate?	Physical wiring, schematics, proprietary	CAD drawings, proprietary
Vulnerabilities	What are the known vulnerabilities?	CVE, proprietary vendor information, unstructured reports.	Proprietary, Locksmith tools
Safeguards	What are the safeguards protecting cyber assets?	Physical security records, badge access records, locks/keys	Proprietary
Physical security measures	Can the cyber asset be vandalized, stolen, cloned, etc?	Location, floor plans, wiring diagrams	Solana SmartHawk, CAD drawings

4.2 Logical Layer

Table 3: Examples of information at the logical layer

What I need to know	Reason	Data collection methods, formats, standards, language	Tools
Asset connectivity	Which asset talks to who, and how?	Scan and interpret topology, or collect from infrastructure directly: deep packet inspection (DPI) classification (voip, data/type, video, etc…) of communication, DNS-SD, mDNS, NetFlow, NetJSON (for data interchange for networks), proprietary firewall configuration management	Discovery and Network Management Tools (SolarWinds, Solana SmartHawk, nmap), Firewall rules, ReadSeal, MaxMind (for IP geolocation)
Communication mode	How cyber assets communicate?	Same as asset connectivity	Same as above
Vulnerabilities	What are the known vulnerabilities?	Scan assets. OVAL (vul assessment), CVE, NVD, CVSS, CWE, CPE, proprietary	Nessus, IP360, etc
Safeguards	What are the safeguards protecting cyber assets?	Patches, Security advisory, bulletins	Redhat security advisory, MS security bulletin
Assets type	The type of asset and revisions	OVAL (system inventory), proprietary	Asset Inventory Management (Microsoft System Center Config Manager, Spiceworks)
Threat information	Sources and types of threats to organisation and missions	STIX/TAXII	Security advisory

4.3 Persona/Virtual layer

Table 4: Examples of information at the persona/virtual layer

What I need to know	Reason	Data collection methods, formats, standards, language	Tools
Role (type of user)	What is the role of person?	Unstructured, domain specification language (DSL), Global address system (GAS)	STUCCO, GAS, Proprietary
Privilege level	Types of activities user can perform	Proprietary, unstructured	STUCCO, MulVal, ARMOUR
Cyber competency	Person has been provided sufficient training to access cyber resources. Is user susceptible to social information gathering, target influencing, …	Proprietary, unstructured.	STUCCO, ARMOUR
Vulnerabilities	Person's vulnerabilities that may impact cyber	Unstructured, CWE, NVD, CVSS	Proprietary, Nessus, IP360
Contact information	How can the user be reached at all times	Unstructured, GAS	GAS

An example of a Cy ISR plan would therefore use a pictorial or graphical representation of each layer of cyberspace, while layering over those items known as "Named Areas of Interest" (NAIs). NAIs combine the source type(s) best suited for collection, the exact location and timing an adversarial activity is expected, and the associated EEIs and PIRs from the ICP. Such technical information would be incorporated into the CyCOP that would be useful for informing commanders and improve their cyber SA. Experts, such as DBHS (the author) security can assist in putting all this information together.

DBHS recommends that this document and associated data are stored on the system of the highest classification in use. This ensures that the decision maker has the complete picture based on all available data, while also preventing transmission security violations. If the decision maker intends to share the document with others who might also adjust and change the document, a shared solution such as a web page or application works best. Alternatively, where the collectors do not need to adjust the document, the decision maker would keep the master copy saved on a shared drive, but disseminate the document to shareholders (read only) for their action or collection. The normal means to induce action is that the decision maker attaches this plan to the Operations Order (or Fragmentary Order) the Commander signs, so that it carries his/her weight as an order. This ensures that the plan receives proper attention and prioritization from collectors, while also telling them that this has been officially authorized and is a legitimate order.

5. References

[1] Canadian Armed Forces (2017). Joint Doctrine Note: Cyber Operations JDN 2017-02, Ottawa, Canada.

[2] Dondo, M., Sokri, A., Ghanmi, A., & Legge, A. (2018) On developing requirements for a Common Operating Picture for cyber operations. Defence Research and Development Canada Scientific Letter, DRDC-RDDC-2018-L148.

[3] DND (2018). Strong, Secure, Engaged (SSE), Defence plan 2018-2023, Ottawa, Canada.

[4] NATO (2016), Allied joint doctrine for joint intelligence, surveillance and reconnaissance, (Technical Report AJP-2.7) NATO.

[5] DND (200), Intelligence Field Manual, B-GL-357-001/FP-001, Ottawa, Canada.

[6] Canadian Forces Joint Planning (CFJP) Manual 2.0 – Intelligence.

[7] Canadian Forces Intelligence Command (CFINTCOM) Production Standards Manual (2017).

ANNEX A - Definitions [5]

C20-0224-03427_Document.docx

Definitions

In this section, we present some key terns for this report. We also define the used acronyms.

Sources and agencies – The sources and agencies are those organizations, individual units, tools, and or capabilities that provide answers to the Intelligence Problem. These can include domestic, allied, military, civilian, NGO, academic, classified and unclassified. The intent is to have the widest range of possible sources of information across as many source types as possible (these could include Human and Counter-Intelligence, Interrogation reports, Imagery, Measurements and Signatures (of metal objects), Signals Intelligence (including emitters, communications and telemetry), Open source (including the Internet, academics, and commercial premium online websites), Acoustic Intelligence, and Technical Intelligence etc. The names of the Allies, other government departments and specific source types / agencies are omitted here for classification reasons but would be included in non-public facing versions.

Common Operating Picture – The data collected by this plan supports the development of a common operating picture by allowing for the collectors (**sources and agencies**) to specifically look for and identify the items of interest that the Commander will want to know about. Thus, it seeks to collect the information that provides a commander and staff the current disposition of a threat **actor** (on any layer of cyberspace), as well as insights into what that **actor** might do in the future. It does this by collecting information on intentions which the analyst determines using structured analytical techniques, basic intelligence and current intelligence reporting. The information from this plan also allows the analyst to identify the adversary's Key Terrain (and Vital Ground). These are nodes/networks/ controllers/files (etc.) that would afford a decided advantage, with the distinction being that the most important of these is referred to as the Vital Ground, which the adversary would defend to a greater degree than the rest.

Actors – Actors can be individuals, non-state, or state actors.

Individuals – include hacktivists, insiders and lone wolf actors. A hacker is a person who secretly gets access to a computer system to get information or cause damage. A hacktivist therefore a person who conducts cyber activities to advance a political agenda. Insider threats may be developed at the behest of foreign governments, groups, or individuals who act on their own initiative (e.g. for revenge). They could also be accidental actions or inactions.

[5] All definitions are taken from the CAF Cyber Joint Doctrine Note (Final), Government of Canada, 2017.

State actors – These will have (or actively working to develop) cyber warfare doctrine, and programs with a social, political, ideological, or religious agenda by causing disruption, inducing fear, or undermining confidence. Targets are often selected on the basis of impact and opportunity. These can include State-sponsored proxies.

Non-state actors – include organizations with the ability to hire or develop hacker skill sets. They may seek to create disruptive or destructive acts normally perpetrated against noncombatant targets. Their attacks are intended to intimidate or coerce a government or population in furtherance of a social, political, or ideological agenda.

ANNEX B – List of Abbreviations/Acronyms

C20-0224-03427_Document.docx

List of Abbreviations/Acronyms

Abbreviation/ Acronym	Definition
ARMOUR	
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CA	Canadian Army
CAD	Computer Aided Design
CANSOFCOM	Canadian Special Operations Forces Command
CCIRs	Commander's Critical Information Requirements
CDS	Chief of the Defence Staff
CFINTCOM	Canadian Forces Intelligence Command
CFWC	Canadian Forces Warfare Centre
CJOC	Canadian Joint Operations Command
CJWC	Canadian Joint Warfare Centre
Comd	Commander
COP	Common Operating Picture
CORA	Centre for Operational Research and Analysis
CPE	Customer-provided equipment
CSE	Communications Security Establishment
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CyCop	Cyber Common Operating Picture
DM	Deputy Minister of National Defence
DNS	Domain Name System
DNS-SD	Domain Name System – Service Discovery
DPI	Deep Packet Inspection
DRDC	Defence Research and Development Canada
DSL	Domain Specification Language
EEIs	Essential Elements of Information
ESPI	Enhanced Serial Peripheral Interface
GAS	Global Address System
GC	Government of Canada
GPS	Global Positioning System
GIS	Geographic Information System
HUMINT	Human Intelligence
ICP	Information collection plan
IP	Internet Protocol
IIS	Internet Information Services

IMINT	Imagery Intelligence
IP360	Commercial Vulnerability Software
IRs	Information Requirements
ISR	Intelligence, Surveillance, and Reconnaissance
JDNCO	Joint Doctrine Note on Cyber Operations
mDNS	Computer protocol that resolves hostnames to IP addresses
MulVal	Multi-host, Multi-Stage Vulnerability Analysis Language
NAIs	Named Areas of Interest
Nessus	Commercial open-source network vulnerability scanner
NetFlow	Commercial (Cisco) networking protocol
NetJSON	Data interchange format for networks
NMTS	Non-Munitions Targeting Sciences (NMTS) project
NORAD	North American Aerospace Defence Command
NVD	National Vulnerability Database
OSC&S	Operations and strategic commanders and their staffs
OSINT	Open Source Intelligence
OVAL	Vulnerability Assessment
PAX	Potential Adversaries
PIRs	Priority Intelligence Requirements
RCAF	Royal Canadian Air Force
RCN	Royal Canadian Navy
S&T	Science and Technolgy
SIGINT	Signals intelligence
SmartHawk	Network monitoring tool
STIX	Structured Threat Information eXxpression
TAXII	Trusted Automated eXchange of Indicator Information
TECHINT	Technical Intelligence
VA	Vulnerability Assessment
VoIP	Voice over Internet Protocol

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

DBHS Security Consulting Inc
RPO Rideau Centre PO Box 53292
Ottawa, Ontario K1N 1C5

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Identifying Requirements for a Cyber Common Operating Picture (CyCOP): Information Collection: Example of a subtitle

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

Doucette, H.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
February 2020	16	7

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

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

DRDC – Centre for Operational Research and Analysis
Defence Research and Development Canada
Carling Campus, 60 Moodie Drive, Building 7S.2
Ottawa, Ontario K1A 0K2
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
06ae - Non-Munitions Targeting Sciences	W6369-19-X024

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2020-C054	C20-0224-03427

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Cyber Common Operating Picture; Cyber Space; Cyber Layers; Infromation Collection Plan

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

The cyber domain is a unique, but complex battlefield, presenting commanders with an equally complex situational awareness (SA) problem. Cyber SA, which provides the commander with an understanding of the battlefield, can be improved through an informed cyber common operating picture (CyCOP). Such a CyCOP requires a knowledgebase, which is the underlying Cyberspace data that provides details about cyber adversaries, targets, and friendly defence capabilities. Collection of such data can be effectively achieved through a systematic collection plan, similar to the military information collection plan (ICP). This work employed the ICP approach to collect, from all layers of Cyberspace, all useful cyber information that could be used to understand friendly and adversary security postures in Cyberspace. In an effort to determine the requirements of establishing a CyCOP, the work systematically populates a generic ICP covering various possible scenarios. The resulting spreadsheet can be used as a starting point in generating mission specific ICPs and developing data models for a CyCOP. In the short term, this ICP will be used to develop data models for a few CyPOC use cases for demonstration.

Le domaine cybernétique est à la fois unique et complexe et représente un véritable défi aux commandants opérationnels. La situation cybernétique, qui fournit aux commandants opérationnels et à leur personnel une compréhension du champ de bataille, peut être améliorée par une bonne situation opérationnelle commune dans le domaine cybernétique (CySOC). Un tel outil exige une base de connaissances sur les cyber-adversaires, les cibles, et les capacités de défense amies. Ceci pourrait s'effectuer à travers un plan de collecte systématique similaire au plan de collecte de données (PCD) militaire. Ce travail utilise l'approche du PCD au niveau des trois paliers du cyberespace pour comprendre la position sécuritaire des amis et des adversaires. Dans l'objectif d'identifier les exigences pour l'établissement d'une CySOC, le travail a systématiquement complété un PCD générique couvrant différents scénarios. Le tableur résultant peut servir comme un point de départ pour développer des PCD plus spécifiques et d'autres modèles de données pour la CySOC. Le PCD générique sera utilisé à court terme dans des études de cas illustratives.