Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Cyber Capability Development Centre (CCDC) Science & Technology (S&T) Requirements, Logical Architecture & Reference Design

Alan Magar

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Defence R&D Canada – Ottawa

Contract Report
DRDC Ottawa CR 2013-057
July 2013

Canada

Cyber Capability Development Centre (CCDC) Science & Technology (S&T) Requirements, Logical Architecture & Reference Design

Alan Magar
IBISKA Telecom, Inc.

Prepared By:
IBISKA Telecom, Inc.
130 Albert Street
Ottawa, ON K1P 5G4

Contract Project Manager: Jonathan Risto, 613-990-6015
PWGSC Contract Number: W7714-135711
Contract Scientific Authority: Kathryn Perrett, 613-993-5132

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Defence R&D Canada – Ottawa

Contract Report
DRDC Ottawa CR 2013-057
July 2013

Contract Scientific Authority

Original signed by Kathryn Perrett

Kathryn Perrett

Defence Scientist, Cyber Operations and Signals Warfare Section

Approved by

Original signed by Peter Mason

Peter Mason

Acting Head, Cyber Operations and Signals Warfare Section

Approved for release by

Original signed by Chris McMillan

Chris McMillan

Head, Document Review Panel

Abstract

In order to support short- and long-term cyber science and technology (S&T) delivery, Defence Research and Development Canada (DRDC) requires an agile and effective infrastructure for cyber research, experimentation, testing and evaluation, demonstration, and training. This capability is referred to as the Cyber Capability Development Centre (CCDC). This report provides a detailed overview of the CCDC, including formalized requirements, conceptual architecture, design considerations, logical architecture, and reference architecture. Specifically, it proposes a phased implementation of the CCDC that culminates in a private Infrastructure-as-a-Service (IaaS) cloud that will enable DRDC research centres to collaborate on research activities and share computing resources as needed.

Résumé

Afin d'appuyer la prestation de services à court et à long terme en matière de cyberscience et technologie, Recherche et développement pour la défense Canada (RDDC) a besoin d'une infrastructure souple et efficace pour effectuer des recherches, des expérimentations, des essais, des évaluations, des démonstrations et de la formation en ce qui a trait au cyberespace. Cette capacité portera le nom de Centre de développement des cybercapacités (CDCC). Ce rapport présente un aperçu détaillé du CDCC, y compris les exigences, l'architecture conceptuelle, les considérations liées à la conception, l'architecture logique et l'architecture de référence qui ont été adoptées officiellement. Plus précisément, il propose une mise en œuvre par étape du CDCC qui se termine par la mise en place d'un nuage informatique privé à titre d'Infrastructure comme service (IaaS), ce qui permettra aux centres de recherche de RDDC de collaborer dans les activités de recherche et de partager les ressources informatiques au besoin.

This page intentionally left blank.

Executive summary

Cyber Capability Development Centre (CCDC) Science & Technology (S&T) Requirements, Logical Architecture & Reference Design:

Alan Magar; DRDC Ottawa CR 2013-057; Defence R&D Canada – Ottawa; July 2013.

Background: In order to support short- and long-term cyber science and technology (S&T) delivery, Defence Research and Development Canada (DRDC) requires an agile and effective infrastructure for cyber research, experimentation, testing and evaluation, demonstration, and training. This capability is referred to as the Cyber Capability Development Centre (CCDC).

Results: This report provides a detailed overview of the CCDC, including formalized requirements, conceptual architecture, design considerations, logical architecture, and reference architecture. The formalized requirements are a collection of approximately 120 S&T-related CCDC requirements that were derived from questionnaires and subsequent interviews with Cyber R&D staff. These formalized requirements were used to develop first a conceptualized architecture, and then a logical architecture, for the CCDC.

The vision for the CCDC is to facilitate collaboration within the Cyber Operations and Signals Warfare Section of DRDC Ottawa, between DRDC research centres (including DRDC Valcartier and DRDC CORA), and with external partners (including academia, industry and government). This will be accomplished by providing a centralized cyber lab capability that will allow Cyber Operations staff to easily conduct, share, and demonstrate their research experiments. The CCDC architecture consists of two primary domains (the Unclassified Domain and the Classified Domain), supplemented with research enclaves containing specialized research equipment or with specific containment/isolation requirements.

The CCDC will be implemented in three phases. Phase I is concerned primarily with providing the basic infrastructure comprising the S&T Lab so that it is fully usable for approximately twenty users. Phase II will expand upon the capabilities built in Phase I by transitioning to an interactive lab complete with training/demonstration environments and usable by approximately fifty users. Phase III will transition the interactive lab to a collaborative lab in order to facilitate collaborative research with other DRDC research centres and external partners. Specifically, this phase will transition the interactive lab into a private cloud offering Infrastructure-as-a-Service (IaaS) capabilities. It is envisioned that ultimately the collaborative labs in the various DRDC research centres would be interconnected using encrypted leased lines or Virtual Private Networks (VPNs), thereby allowing the research centres to collaborate on research activities and share computing resources as needed. The reference architecture details how the CCDC can be built using virtualization/cloud software from a leading vendor.

Significance: Not only will the CCDC provide a lab capability that will enable Cyber R&D staff to conduct their research both efficiently and effectively, but it will provide a means by which staff can interact and collaborate with Cyber R&D staff located at other DRDC campuses and

with external partners. It is envisioned that this capability will significantly improve research activities within the Cyber Program.

Future plans: The phased implementation of the CCDC should be implemented as outlined in this report.

Sommaire

Cyber Capability Development Centre (CCDC) Science & Technology (S&T) Requirements, Logical Architecture & Reference Design:

Alan Magar ; DRDC Ottawa CR 2013-057 ; R & D pour la défense Canada – Ottawa; juillet 2013.

Contexte : Afin d'appuyer la prestation de services à court et à long terme en matière de cyberscience et technologie, Recherche et développement pour la défense Canada (RDDC) a besoin d'une infrastructure souple et efficace pour effectuer des recherches, des expérimentations, des essais, des évaluations, des démonstrations et de la formation en ce qui a trait au cyberespace. Cette capacité portera le nom de Centre de développement des cybercapacités (CDCC).

Résultats : Ce rapport présente un aperçu détaillé du CDCC, y compris les exigences, l'architecture conceptuelle, les considérations liées à la conception, l'architecture logique et l'architecture de référence qui ont été adoptées officiellement. Les exigences officielles représentent un ensemble d'environ 120 exigences du CDCC liées à la science et à la technologie qui ont été dégagées de questionnaires et d'entrevues subséquentes avec le personnel de la recherche et du développement du domaine du cyberespace. Ces exigences ont d'abord servi à établir une architecture conceptualisée puis une architecture logique pour le CDCC.

La vision pour le CDCC est de faciliter la collaboration entre la section des cyberopérations et de la guerre des transmissions de RDDC Ottawa, les centres de recherche de RDDC (y compris RDDC Valcartier et RDDC CARO) et les partenaires externes (y compris le milieu universitaire, l'industrie et le gouvernement). Pour ce faire, on fournira un laboratoire centralisé de cybercapacité qui permettra au personnel des cyberopérations de mener les expériences de recherches, d'en faire la démonstration et de les communiquer facilement. L'architecture du CDCC consiste en deux principaux domaines (le domaine sans classification et le domaine classifié), auxquels s'ajoutent des enclaves de recherches qui contiennent de l'équipement de recherche spécialisé assorties d'exigences précises d'isolement ou de confinement.

Le CDCC sera mis en œuvre en trois étapes. La première étape vise principalement à fournir l'infrastructure de base, ce qui comprend le laboratoire de science et technologie, de manière à ce qu'environ 20 utilisateurs puissent s'en servir. La deuxième étape consistera à élargir les capacités qui ont été mises en place à la première étape, au moyen d'une transition vers un laboratoire interactif, doté d'environnements de formation et de démonstration, et qui pourra servir à environ 50 utilisateurs. À la troisième étape, le laboratoire interactif deviendra un laboratoire collaboratif afin de faciliter la collaboration en matière de recherche avec les autres centres de recherche de RDDC et les partenaires externes. Plus particulièrement, dans cette étape, on transformera le laboratoire interactif en nuage informatique privé qui offrira des capacités d'Infrastructures comme service (IaaS). À terme, on prévoit que les laboratoires dans les divers centres de recherche de RDDC qui collaborent seront reliés au moyen de lignes louées chiffrées ou de réseaux privés virtuels (RPV), ce qui permettra aux centres de recherche de collaborer dans les activités de recherche et de partager les ressources informatiques au besoin. L'architecture de

référence décrit de quelle manière le CDCC peut être constitué à l’aide d’un logiciel d’infonuagique ou de virtualisation offert par un fournisseur de premier plan.

Importance : Non seulement le CDCC fournira-t-il une capacité de laboratoire qui permettra au personnel de la recherche et du développement du domaine du cyberespace de mener des recherches de manière optimale, mais il fournira aussi un moyen par lequel les employés peuvent interagir et collaborer avec le personnel du même domaine dans les autres centres de recherche de RDDC et chez les partenaires externes. On prévoit que cette capacité améliorera grandement les activités de recherche au sein du programme lié au cyberespace.

Plans futurs : La mise en œuvre par étape du CDCC devrait être réalisée conformément au plan prévu dans le rapport.

Table of contents

List of figures

List of tables

1 Introduction

1.1 Background

In order to support short- and long-term cyber science and technology (S&T) delivery, Defence Research and Development Canada (DRDC) requires an agile and effective infrastructure for cyber research, experimentation, testing and evaluation, demonstration, and training. This capability is referred to as the Cyber Capability Development Centre (CCDC) throughout this report.

1.2 Purpose

The purpose of this report is to formalize S&T-related requirements for the CCDC, and to develop conceptual, logical, and reference architectures – including a network architecture.

1.3 Approach

The approach used within this report is as follows:

1) Formalize the Requirements – gather and analyze S&T-related CCDC requirements from both DRDC Ottawa and DRDC Valcartier;

2) Develop a Conceptual Architecture – develop a conceptual architecture for the CCDC based on the formalized requirements;

3) Evaluate Design Considerations – decide on a number of key design considerations that will have a significant impact on the logical and reference architectures;

4) Develop a Logical Architecture – develop a logical architecture for the CCDC based on the conceptual architecture and the design considerations; and

5) Provide a Reference Architecture – design a reference architecture for the CCDC that can be implemented by DRDC researchers for performing tests and conducting experiments within a secure environment.

2 Requirements

2.1 Overview

The requirements gathering process was a two stage process consisting of a questionnaire and an interview. The questionnaire, which can be found in Annex A, was circulated to approximately twenty individuals within the Cyber Operations & Signals Warfare Section of DRDC Ottawa. A more focussed questionnaire, which can be found in Annex B, was also circulated to approximately ten individuals within the Mission Critical Cyber Security (MCCS) Section of DRDC Valcartier. This was followed by an interview process, which was conducted based on research groups within the Cyber Program of DRDC.[1]

Approximately 120 requirements were derived from questionnaires and subsequent interviews with Cyber R&D staff. These requirements were divided into the following groups:

- Access – these requirements capture how, when and the frequency with which Cyber Operations personnel intend to access the CCDC;

- Collaboration – these requirements capture with whom and the manner in which Cyber Operations personnel intend to use the CCDC for collaboration;

- Interaction – these requirements capture the manner in which Cyber Operations personnel intend to interact with the CCDC;

- Research – these requirements capture how Cyber Operations personnel intend to conduct their research activities in the CCDC; and

- DRDC Valcartier – these requirements, which were collected separately using the targeted questionnaire in Annex B, capture how DRDC Valcartier's Cyber R&D staff within the MCCS Section intend to use the CCDC for both malware analysis and penetration testing research.

Note – A "U" preceding the requirement designation is used to denote a requirement that is applicable to an unclassified portion of the CCDC, whereas a "C" denotes a requirement for the classified portion. A "U/C" preceding the requirement designation indicates a requirement that is applicable to both the Unclassified and the Classified Domains.

2.2 Access Requirements

CCDC access requirements consist of the following:

[1] The Cyber Program within DRDC will be used throughout this report to refer to the Cyber Operations & Signals Warfare Section within DRDC Ottawa, the Mission Critical Cyber Security Section within DRDC Valcartier, and the Cyber component of DRDC CORA.

- A-1 (U/C) – Cyber Operations staff must be able to access the CCDC from within the CCDC lab environment(s);

- A-2 (U) – Cyber Operations staff must be able to access the CCDC remotely from their respective offices;

- A-3 (U) – Cyber Operations staff must be able to access the CCDC remotely from outside the DRDC campus;

- A-4 (U/C) – Cyber Operations staff require access to the CCDC on average 8.6 hours per week[2];

- A-5 (U/C) – Cyber Operations staff expect to require access to the CCDC on average 11.3 hours per week in approximately four years' time[3];

- A-6 (U/C) – Cyber Operations staff must be able to access the CCDC outside of normal working hours;

- A-7 (U/C) – The CCDC should be available for use most of the time with relatively limited downtime;[4]

- A-8 (C) – The CCDC must support classified research and testing;

- A-9 (C) – Cyber Operations staff require access to classified lab facilities for 22% of their work[5];

- A-10 (C) – Cyber Operations staff envision requiring access to classified lab facilities for 34% of their work in approximately four years' time[6];

- A-11 (U/C) – The CCDC must provide a mechanism to transfer data between the unclassified and the classified lab environments;

- A-12 (U/C) – The CCDC must accommodate a phased implementation consisting of the following three phases:

    - S&T Lab – basic S&T lab with approximately twenty users;

    - Interactive Lab – S&T lab with a demonstration and training environment, and in excess of fifty users; and

[2] This figure is the average time based on the completed questionnaires.
[3] This figure is the average time based on the completed questionnaires. It represents a 31.4% increase.
[4] Most respondents were of the opinion that there would be little negative effect if the CCDC were to be unavailable for a relatively short period of time (i.e., hours) and there would be some effect if it were to be unavailable for a longer period of time (i.e., days).
[5] This figure is the average based on the completed questionnaires.
[6] This figure is the average based on the completed questionnaires. It represents a 59.5% increase.

    - Collaborative Lab – S&T lab that facilitates collaboration by providing connectivity with external users.

- A-13 (U) – The CCDC must provide Internet connectivity in order to facilitate firmware and software updates.

2.3 Collaboration Requirements

It is important to note that the word connectivity is used for a number of collaboration requirements. It is intended to be a general term denoting one-way network connectivity in order to facilitate the transfer of data from the DND network to the CCDC. However, there may be a requirement for enhanced connectivity at a later point in time.

CCDC collaboration requirements consist of the following:

- C-1 (U/C) – The CCDC must facilitate collaboration with Cyber R&D staff within the same DRDC campus;

- C-2 (U/C) – The CCDC must facilitate collaboration among Cyber R&D staff at different DRDC campuses;

- C-3 (U/C) – The CCDC must facilitate collaboration with DRDC Centre for Operational Research and Analysis (CORA) colleagues;

- C-4 (U/C) – The CCDC must facilitate collaboration with colleagues in other Government of Canada (GC) departments and agencies;

- C-5 (U/C) – The CCDC must facilitate collaboration with external partners (e.g., university collaborations, industry partners)[7];

- C-6 (U/C) – The CCDC must facilitate capability demonstrations[8];

- C-7 (U/C) – The CCDC must facilitate data exchange with collaborating partners;

- C-8 (U/C) – The CCDC must allow partner access to projects;

- C-9 (U/C) – The CCDC must facilitate training, including the provisioning and de-provisioning of systems for training[9];

[7] During the interview process there was specific mention of the Modeling and Simulation Group in NATO and red-teaming challenges/war-gaming with the Royal Military College (RMC).

[8] Capability demonstrations are extremely important for Cyber Operations staff in order to promote and enhance their research activities. E.g., one Cyber Operations project specifically mentioned a requirement for at least two independent large displays (e.g., Smart TVs) for the demonstration of experiments.

[9] E.g., one Cyber Operations employee has a requirement to train eight analysts at a time.

- C-10 (C) – The CCDC must provide access/connectivity to the CFWC Battle Lab for exercises such as Coalition Warfare Interoperability Demonstration (CWID), Joint Exercise (JOINTEX) and Coalition Attack Guidance Experiment (CAGE);

- C-11 (U/C) – The CCDC must provide access to previous/current/upcoming Technology Demonstrator Projects (TDPs) (e.g., Secure Access Management for Secret Operational Networks (SAMSON), Joint Network Defence and Management System (JNDMS), Automated Computer Network Defence (ARMOUR), Tactical Edge Cyber Command and Control (TEC3))[10];

- C-12 (C) – The CCDC must provide connectivity to the Testing Development Center (TDC) and Classified Testing Development Center (CTDC) at Tunney's Pasture in order to facilitate project migration;

- C-13 (C) – The CCDC must provide connectivity to the Canadian Forces National Operations Centre (CFNOC);

- C-14 (U) – The CCDC must provide connectivity to the Defence Research Establishment Network (DREnet); and

- C-15 (U) – The CCDC must provide connectivity to the Defence Wide Area Network (DWAN).

2.4 Interaction Requirements

CCDC interaction requirements consist of the following:

- I-1 (U/C) – The CCDC must allow Cyber Operations staff to install applications on existing operating systems within the CCDC;

- I-2 (U/C) – The CCDC must allow Cyber Operations staff to install specific operating systems on systems within the CCDC;

- I-3 (U/C) – The CCDC must allow Cyber Operations staff to make limited physical changes (e.g., memory, processors) to systems within the CCDC;

- I-4 (U/C) – The CCDC must allow Cyber Operations staff to install network components (e.g., routers, switches, firewalls) within the CCDC;

- I-5 (U/C) – Cyber Operations staff must have administrative access to their own lab systems; and

[10] It is recommended that DRDC contracts include project support in the CCDC for a period of two years in order to ensure that TDP use can be maximized.

- I-6 (U/C) – The CCDC must be staffed so as to provide some assistance to DRDC researchers in terms of installing, configuring and maintaining lab hardware and software[11].

2.5 Research Requirements

Due to their extensive and diverse nature, the research requirements were sub-divided as follows:

- General requirements;
- Network requirements;
- Hardware requirements;
- Software requirements; and
- Data requirements.

Note – It was assumed that the CCDC will ultimately encompass the ARMOUR Technology Demonstrator (TD) laboratory. Consequently, some requirements were taken from the ARMOUR TD Lab.[12]

2.5.1 General Requirements

General requirements for the CCDC consist of the following:

- RG-1 (U/C) – The CCDC must facilitate Cyber Operations research to the greatest extent possible. Specifically, the CCDC must support a variety of Cyber Operations research capabilities. These capabilities, which are listed in no particular order, include the following:
  - Traffic and data analysis;
  - Testing and measurement of networks, systems, and technologies;
  - Red-teaming and blue-teaming experiments;
  - Network and host behaviour classification;
  - Course-of-action cost analysis experiments;

[11] Defence scientists within the Cyber Operations & Signals Warfare section of DRDC Ottawa were largely unanimous in their requirement for a lab administrator to provide some assistance in terms of installing, configuring and maintaining lab hardware and software. However, they were equally vocal in their requirement for a computer scientist/technologist to support lab experiments and field trials.

[12] *ARMOUR TD Laboratory Proposed Requirements*, Draft 0.3, February 2011.

  - Electronic warfare/cyber convergence experiments;
  - Vulnerabilities of wireless interfaces and systems;
  - Simulation for wireless mobile ad-hoc network (MANET) security such as access control, routing security, attack detection, and traffic analysis;
  - Development of Digital Signal Processing (DSP) algorithms and implementation on Software Defined Radio (SDR);
  - Network, system and application modeling and simulation experiments;
  - Intrusion Detection System (IDS) alert correlation;
  - Defensive posture evaluation;
  - Operating system vulnerability assessments;
  - Malware analysis;
  - Network data recovery and analysis;
  - Attack detection and validation;
  - Testing prototype cyber defence tools;

- RG-2 (U/C) – The CCDC must be partitionable into multiple independent experimental testbeds that can be used simultaneously;
- RG-3 (U/C) – The CCDC must be capable of supporting multiple simultaneous environments including development and demonstration environments;
- RG-4 (U/C) – The CCDC must support the archiving of completed or dormant projects for at least two years;
- RG-5 (U/C) – The CCDC must be capable of hosting an instantiation of whatever cyber operations products are in use by the Department of National Defence (DND) and/or Canadian Forces (CF);
- RG-6 (U/C) – The CCDC must support scalable hardware and software performance;
- RG-7 (U/C) – The CCDC must support ease of management and require minimal administrative expertise;
- RG-8 (U/C) – The CCDC must support system image archival;

2.5.2 Network Requirements

Network requirements for the CCDC consist of the following:

- RN-1 (U) – The CCDC must be capable of providing a reasonable facsimile of the DREnet;
- RN-2 (U) – The CCDC must be capable of providing a reasonable facsimile of the DWAN;
- RN-3 (U/C) – The CCDC must be capable of simulating wireless networks[13];
- RN-4 (U/C) – The CCDC must facilitate the research and development of MANETs;
- RN-5 (U/C) – The CCDC must support flexible and easy network configuration to allow for the isolation of research environments;
- RN-6 (U/C) – The CCDC must provide isolated network segmentation and configuration from other staging and production environments;
- RN-7 (U/C) – The CCDC must be capable of duplicating Canadian Forces (CF) environments (e.g., deployed networks);
- RN-8 (U/C) – The CCDC must be capable of simulating/emulating very large networks;
- RN-9 (C) – The CCDC must support integration with the EW enclave;
- RN-10 (U) – The CCDC must include a cyber-Defence Technology Experimental Research (DETER) testbed; and
- RN-11 (C) – The CCDC must include a Canadian Forces Network Operations Centre (CFNOC) environment for the testing and evaluation of R&D outputs.

2.5.3 Hardware Requirements

Hardware requirements for the CCDC consist of the following:

- RH-1 (C) – The CCDC must have cryptographic components such as KG84C, Tactical Local Area Network Encryption (TACLANEs), etc.;
- RH-2 (C) – The CCDC must support removable storage units in order to support chain-of-custody rules required for investigations;
- RH-3 (U/C) – The CCDC must facilitate the use of military tactical radios;

[13] Wireless, and wired, networks are currently simulated within Cyber Operations using the EXata cyber simulation tool.

- RH-4 (U/C) – The CCDC must provide system access in order to support research into cross-layer information exchange;

- RH-5 (U/C) – The CCDC must have an extremely large storage capacity (i.e., >10TB) in order to support large datasets. Furthermore, the storage capacity must be able to be easily expanded to accommodate future requirements;

- RH-6 (U/C) – The CCDC must support very fast access to disk in order to support large number of simultaneous disk reads;

- RH-7 (U/C) – The CCDC must be capable of supporting port mirrors and network taps;

- RH-8 (U/C) – The CCDC must be capable of distributing processing workload across multiple systems;

- RH-9 (U/C) – The CCDC must be capable of supporting highly process-intensive applications;

- RH-10 (U/C) – The CCDC must be capable of supporting Trusted Platform Modules (TPMs);

- RH-11 (U/C) – The CCDC must be capable of supporting pico and micro base stations supporting a variety of wireless interfaces including Long-Term Evolution (LTE), WiMAX, Iridium, Inmarsat Broadband Global Area Network (BGAN), Thuraya, and Bluetooth;

- RH-12 (U/C) – The CCDC must be capable of supporting mobile devices, such as smart phones and tablets, with wireless interfaces for testing;

- RH-13 (U/C) – The CCDC must be capable of supporting hardware-based traffic generators;

- RH-14 (U/C) – The CCDC must be capable of supporting wireless routers;

- RH-15 (U/C) – The CCDC must be capable of supporting both traditional and wireless traffic monitors;

- RH-16 (U/C) – The CCDC must be capable of supporting web filtering and firewall appliances; and

- RH-17 (U/C) – CCDC personnel must be capable of dedicating specific hardware resources to experiments.

2.5.4 Software Requirements

Software requirements for the CCDC consist of the following:

- RS-1 (U/C) – The CCDC must be capable of managing version control for development projects;
- RS-2 (U/C) – The CCDC must be capable of supporting virtual channel emulators;
- RS-3 (U/C) – The CCDC must be capable of supporting virtual mobile devices;
- RS-4 (U/C) – The CCDC must be capable of supporting multiple operating systems simultaneously;
- RS-5 (U/C) – The CCDC must provide a standard library of images for vendor software and operating systems;
- RS-6 (U/C) – The CCDC must provide access to a variety of Operating Systems (OS) for vulnerability assessment work;
- RS-7 (U/C) – The CCDC must support malware analysis tools[14];
- RS-8 (U/C) – The CCDC must support traffic generator software (network layer and application layer);
- RS-9 (U/C) – The CCDC must support simulation/emulation software[15];
- RS-10 (U/C) – The CCDC must support network Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) sensors and Security Information/Event Management (SIEM) software[16];
- RS-11 (U/C) – The CCDC must support statistical computing languages and environments[17];
- RS-12 (U/C) – The CCDC must support open source machine learning software[18];
- RS-13 (U/C) – The CCDC must support Software Defined Radio Platforms (SDRP)[19];

[14] During the interview process there was specific mention of the Automated Experiment System (AES).

[15] During the interview process there was specific mention of MatLab (http://www.mathworks.com/products/matlab/), including the Steepest Ascent algorithm, and SystemVue (http://www.home.agilent.com/en/pc-1297131/systemvue-electronic-system-level-esl-design-software?&cc=CA&lc=eng).

[16] During the interview process there was specific mention of HP Arcsight (http://www.hpenterprisesecurity.com/products) and Netwitness (http://www.netwitness.com).

[17] During the interview process there was specific mention of R (http://www.r-project.org).

[18] During the interview process there was specific mention of RapidMiner (http://rapid-i.com/content/view/181/190/), Weka (http://www.cs.waikato.ac.nz/ml/weka/) and ELKI (http://elki.dbs.ifi.lmu.de).

- RS-14 (U/C) – The CCDC must support Computer Aided Design (CAD) tools;

- RS-15 (U/C) – The CCDC must be capable of supporting network protocol analyzers[20];

- RS-16 (U/C) – The CCDC must be capable of supporting cloud computing software; and

- RS-17 (U/C) – The CCDC must be capable of supporting endpoint protection software including virus scanners[21].

2.5.5 Data Requirements

Data requirements for the CCDC consist of the following:

- RD-1 (U/C) – The CCDC must support the use of internally generated data;

- RD-2 (U/C) – The CCDC must support the use of client capture relay data;

- RD-3 (U/C) – The CCDC must support the use of live data feeds;

- RD-4 (U) – The CCDC must support live capture of DREnet data;

- RD-5 (U) – The CCDC must support live capture of DWAN data;

- RD-6 (U/C) – The CCDC must support the use of Protected Repository for the Defence of Infrastructure against Cyber Threats (PREDICT) datasets;

- RD-7 (U/C) – The CCDC must be capable of supporting blended datasets;

- RD-8 (U/C) – The CCDC must have access to, and support the use of, CF data sources and joint exercise/experiment data;

- RD-9 (U/C) – The CCDC must have access to, and support the use of, Unmanned Aerial Vehicle (UAV) or Link 16 capture data;

- RD-10 (U/C) – The CCDC must have access to, and support the use of, military SATCOM data; and

- RD-11 (U/C) – The CCDC must support JNDMS and ARMOUR feeds.

[19] During the interview process there was specific mention of Universal Software Radio Peripheral (USRP), FatBoy, LYRtech and PS3.

[20] During the interview process there was specific mention of Wireshark (http://www.wireshark.org).

[21] During the interview process there was specific mention of Symantec Endpoint Protection (http://www.symantec.com/endpoint-protection).

2.6 DRDC Valcartier

The DRDC Valcartier requirements have been sub-divided as follows:

- Common Requirements;
- Malware Analysis; and
- Penetration Testing.

2.6.1 Common Requirements

DRDC Valcartier common requirements for the CCDC consist of the following:

- VC-1 (U) – The CCDC must support monitoring tools to facilitate malware analysis and penetration testing;[22]
- VC-2 (U) – The CCDC must support a variety of operating systems to facilitate malware analysis and penetration testing research;[23]
- VC-3 (U) – The CCDC must support a variety of hardware platforms, both conventional and unconventional, to facilitate malware analysis and penetration testing research;[24]
- VC-4 (U) – The CCDC must provide an appropriate level of separation for malware analysis and penetration testing research activities;[25]
- VC-5 (U) – The CCDC must facilitate collaboration between Cyber R&D staff in DRDC Ottawa and DRDC Valcartier by providing connectivity between their respective lab networks;
- VC-6 (U) – The CCDC must provide Cyber R&D staff in DRDC Valcartier with complete control and setup of their own network;
- VC-7 (U) – The CCDC must support a direct (unfiltered and anonymized) connection to the Internet in order to allow malware to call home or to download additional components; and
- VC-8 (U) – The CCDC must support a Graphics Processing Unit (GPU) cluster in order to facilitate password cracking research.

[22] There was specific mention of monitoring tools such as Process Monitor (ProcMon - http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx), Wireshark (http://www.wireshark.org) and EtherApe (http://etherape.sourceforge.net).

[23] There was specific mention of operating systems such as Linux, Solaris, Mac OS X, Microsoft Windows.

[24] In terms of unconventional hardware, there was specific mention of Arduino (http://www.arduino.cc) and Raspberry Pi (http://www.raspberrypi.org).

[25] In terms of isolation, virtualization is sufficient for the majority of malware and penetration testing research. However, occasionally full physical isolation will be required.

2.6.2 Malware Analysis Requirements

DRDC Valcartier malware analysis requirements for the CCDC consist of the following:

- VM-1 (U) – The CCDC must support malware analysis systems;[26]
- VM-2 (U) – The CCDC must support anti-virus/malware scanners;
- VM-3 (U) – The CCDC must support emulators to facilitate malware analysis research;[27]
- VM-4 (U) – The CCDC must support kernel debuggers to facilitate malware analysis research;[28]
- VM-5 (U) – The CCDC must support code analysis tools to facilitate malware analysis research;[29]
- VM-6 (U) – The CCDC must support task automation frameworks to facilitate malware analysis research;[30]
- VM-7 (U) – The CCDC must support forensics analysis tools to facilitate malware analysis research;[31]
- VM-8 (U) – The CCDC must provide a large body of malware with which to conduct malware analysis research; and
- VM-9 (U) – The CCDC must provide a repository for the safe storage and retrieval of malware.[32]

[26] There was specific mention of malware analysis systems such as ValidEdge (http://www.validedge.com) and FireEye (http://www.fireeye.com).

[27] There was specific mention of emulators such as Bochs (http://bochs.sourceforge.net) and QEMU (http://wiki.qemu.org/Main_Page).

[28] There was specific mention of kernel debuggers such as WinDbg (http://msdn.microsoft.com/en-us/windows/hardware/gg463009.aspx) and Syser (http://www.sysersoft.com).

[29] There was specific mention of code analysis tools such as BinDiff (http://www.zynamics.com/software.html), BinNavi (http://www.zynamics.com/software.html), 010 Editor (http://www.sweetscape.com/010editor/), HexDump (http://www.fileformat.info/tool/hexdump.htm) and Interactive DisAssembler (IDA – https://www.hex-rays.com).

[30] There was specific mention of task automation frameworks such as PowerShell (http://technet.microsoft.com/en-ca/scriptcenter/powershell.aspx).

[31] There was specific mention of forensic/analysis tools such as Volatility Framework (https://www.volatilesystems.com/default/volatility) and HBGary Responder (http://www.hbgary.com/responder-pro).

[32] Malware is typically stored encrypted in a repository (either LDAP or a file server) and protected with discretionary access controls. The malware files are zipped with encryption using a common password (“infected” or “malware”).

2.6.3 Penetration Testing Requirements

DRDC Valcartier penetration testing requirements for the CCDC consist of the following:

- VP-1 (U) – The CCDC must support vulnerability scanners and penetration testing software to facilitate penetration testing research;[33]

- VP-2 (U) – The CCDC must support packet manipulation tools to facilitate penetration testing research;[34]

- VP-3 (U) – The CCDC must support Intrusion Detection and Prevention Systems (IDS/IPS) to facilitate penetration testing research;[35]

- VP-4 (U) – The CCDC must support penetration testing-specific operating system distributions to facilitate penetration testing research; and [36]

- VP-5 (U) – The CCDC must support target environments specifically developed for penetration testing.

[33] There was specific mention of vulnerability scanners and penetration testing software such as Nessus (http://www.tenable.com/products/nessus), Nikto (http://www.cirt.net/nikto2), Nmap (http://nmap.org), Metasploit (http://www.metasploit.com), CORE Impact (http://www.coresecurity.com/content/core-impact-overview) and Social-Engineer Toolkit (SET – https://www.trustedsec.com/downloads/social-engineer-toolkit/).

[34] There was specific mention of packet manipulation tools such as Scapy (http://www.secdev.org/projects/scapy/).

[35] There was specific mention of IDS/IPS such as Snort (http://www.snort.org).

[36] There was specific mention of operating system distributions such as BackTrack (http://www.backtrack-linux.org) and Backbox (http://www.backbox.org).

3 Conceptual Architecture

3.1 Overview

This section of the report will detail a logical architecture for the CCDC derived from the requirements that were formalized in the preceding section of the report. The mapping of formalized requirements to the logical architecture can be seen in Appendix C. The CCDC logical architecture is illustrated in Figure 1.

It is envisioned that there will be two main domains, the Unclassified Domain and the Classified Domain, at each DRDC campus. These two primary domains will be supplemented with research enclaves containing specialized research equipment or with specific containment/isolation requirements. Furthermore, it is anticipated that network connectivity will exist initially between the respective Unclassified Domains, and eventually the Classified Domains.

Specifically, this section will examine the following aspects of the CCDC logical architecture:

- DRDC Ottawa Domains;
- Research Centres;
- Research Enclaves;
- Connectivity;
- Demonstration Environment; and
- Training Environment.

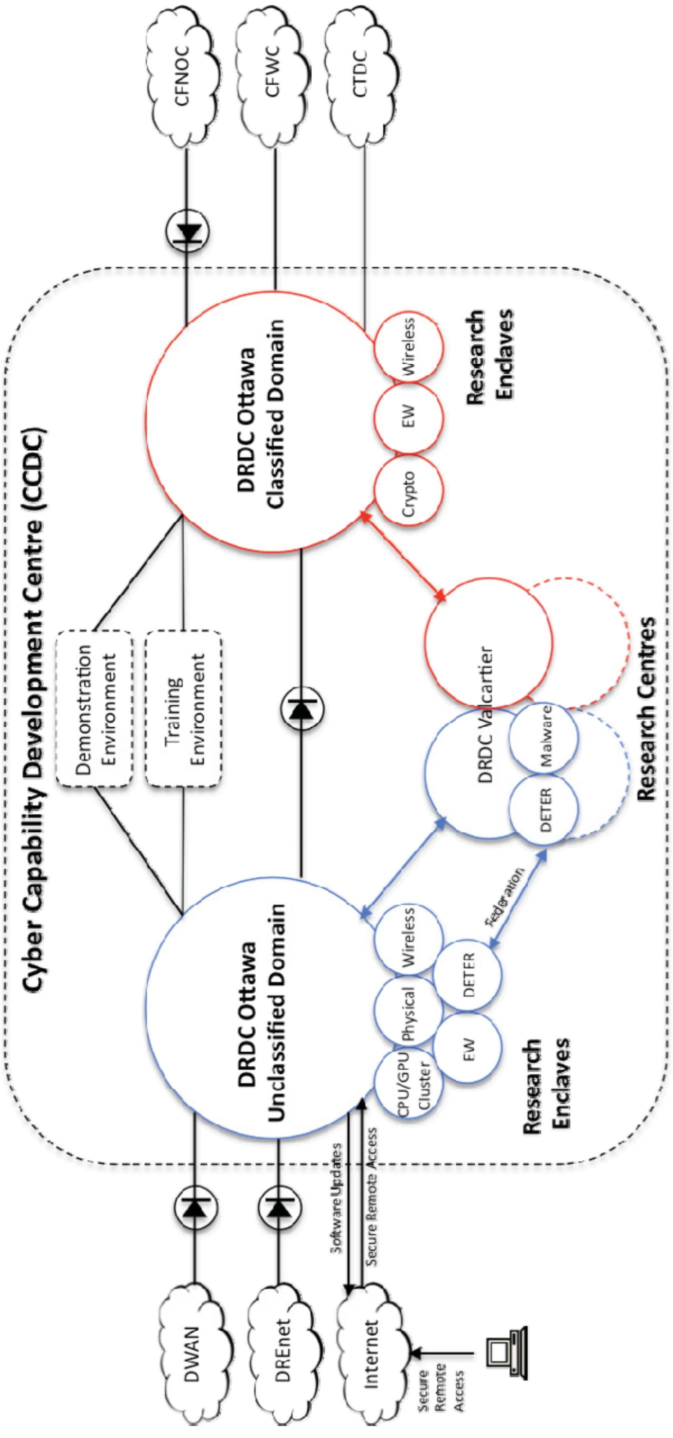

Figure 1 – CCDC Logical Architecture

3.2 DRDC Ottawa Domains

There are two DRDC Ottawa Domains: the Unclassified Domain and the Classified Domain. The DRDC Ottawa Unclassified Domain is intended for Cyber Operations research activities at the unclassified level. The DRDC Ottawa Classified Domain is intended for Cyber Operations research activities up to and including Secret. It was determined that there is limited immediate requirement for a Cyber Operations domain at the Top Secret level. However, nothing in the logical architecture precludes its later addition to the CCDC. The DRDC Ottawa Domains are illustrated in Figure 2.

This section will describe the DRDC Ottawa Domains in terms of the following:

- Access;
- Collaboration;
- Interaction; and
- Research.

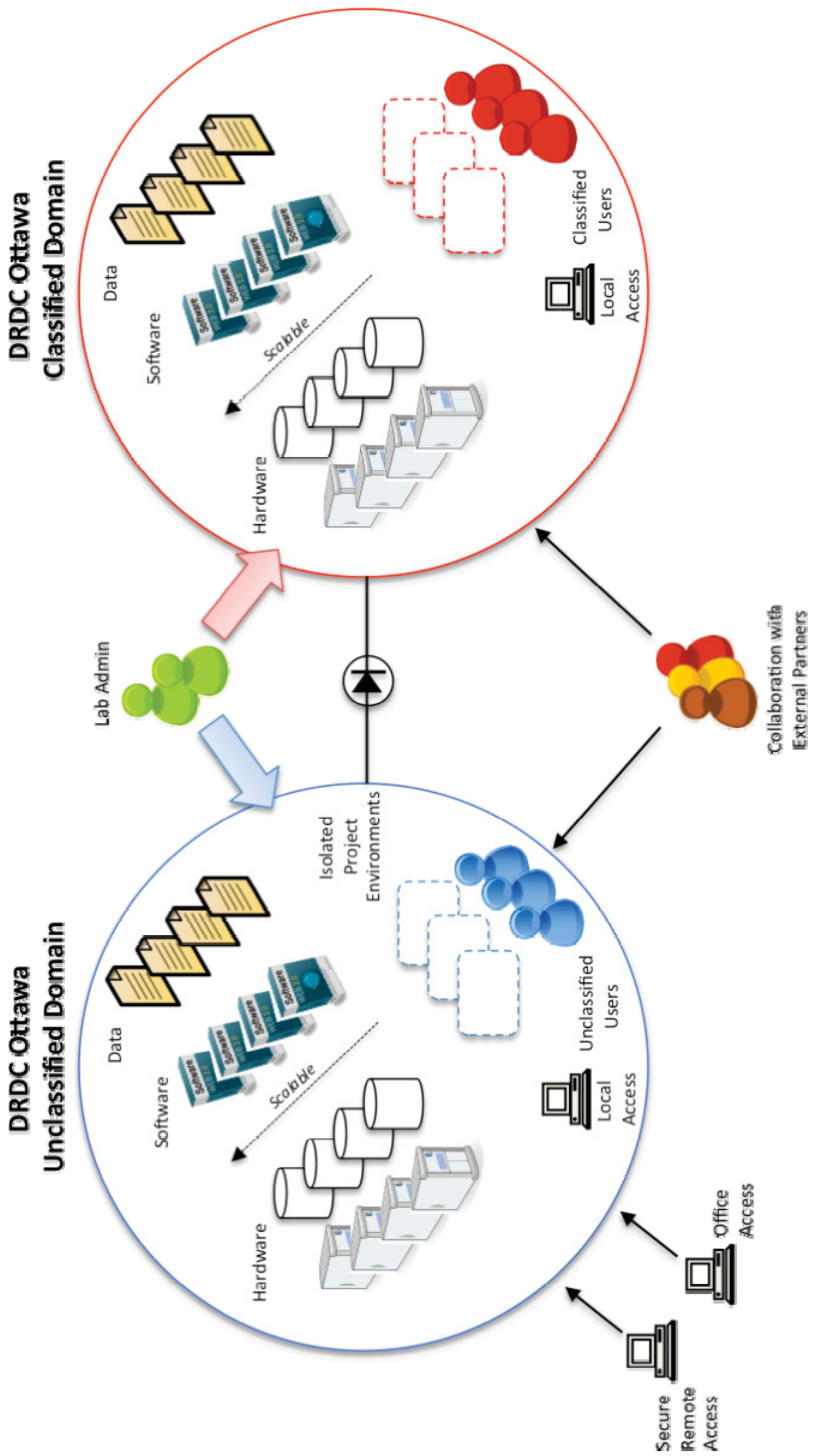

Figure 2 – DRDC Ottawa Domains

3.2.1 Access

In order to maximize its utility the DRDC Ottawa Unclassified Domain will be accessible 24/7 from within the lab itself, from the offices of Cyber Operations staff, and eventually remotely over the Internet. The Secret Domain, which will be located in a separate physical environment, will only be accessible from within the lab itself. It is envisioned that the CCDC will have a number of workstations, consisting of a keyboard, video and mouse, from which to access both the Unclassified and Classified Domains. Secure access over the Internet to the Unclassified Domain is discussed in further detail in Section 3.5.3.

Based on the survey conducted Cyber Operations staff envision spending an average of 6.8 hours a week now, and 7.4 hours a week in approximately four years, working directly on systems in the Unclassified Domain. Similarly, Cyber Operations staff members envision spending an average of 1.8 hours a week now, and 3.9 hours a week in approximately four years, working directly on systems in the Classified Domain. It should be noted that the time estimation responses from Cyber R&D staff are very rough estimates only. When one factors in the phased implementation schedule, the CCDC must support the levels of access included in Table 1.

Table 1 – Anticipated Usage

Phase	# of Users	Anticipated Usage (weekly)	
		Unclassified Enclave	Classified Enclave
1 – S&T Lab	20	136-148 hours	36-78 hours
2 – Interactive Lab	50	340-370 hours	90-195 hours
3 – Collaborative Lab	100	680-740 hours	180-390 hours

Furthermore, based on the questionnaires submitted and subsequent interviews with Cyber Operations staff, it was determined that the target availability should be 99%, 24 hours per day, 7 days per week. This equates to 1.7 hours of downtime per week, 7.2 hours per month and 3-4 days per year.

3.2.2 Collaboration

The vision for the CCDC is to facilitate collaboration within the Cyber Operations and Signals Warfare Section of DRDC Ottawa, between DRDC research centres (including DRDC Valcartier and DRDC CORA), and with external partners (including academia, industry and government).

This will be accomplished by providing a centralized cyber lab capability that will allow Cyber Operations staff to easily conduct, share, and demonstrate their research experiments. This includes providing access to both current and completed TDPs (e.g., SAMSON, JNDMS/Net C2 ISAC, ARMOUR, and TEC3). Collaboration will include the ability to exchange data with partners, provide access to research experiments to partners, and demonstrate research experiments to stakeholders.

3.2.3 Interaction

In order to perform research experiments in the CCDC, some Cyber R&D staff members require limited administrative access to systems in order to install operating systems and applications on systems. Cyber Operations staff may even need to make limited physical changes (e.g., memory, processors) to systems and install network components (e.g., routers, switches, firewalls). However, due to their primary focus being on research, defence scientists and engineers expect the CCDC to be staffed so as to provide some assistance with the installation, configuration and maintenance of lab hardware and software. Consequently, the CCDC will need to be easy to manage and must require minimal administrative expertise.

3.2.4 Research

This section will examine the DRDC Ottawa Domains in terms of the following:

- General;
- Network;
- Hardware;
- Software; and
- Data.

3.2.4.1 General

The CCDC must be able to support a wide range of research activities encompassing the entire gamut of Cyber S&T. In order to facilitate these diverse research activities, the CCDC must be partitionable into multiple independent environments – including development and demonstration environments – that can be used simultaneously for different research activities. The environments must be capable of being isolated from one another in order to prevent one research activity from inadvertently affecting another. Furthermore, given its support for DND operations, the CCDC must be capable of hosting an instantiation of products in use by DND/CF in order to facilitate development and testing. Finally, the CCDC must be capable of archiving dormant projects, including system image archival, for a period of two years.

3.2.4.2 Network

In order to be able to test research experiments in as realistic an environment as possible, the CCDC must be able to simulate very large networks. This would include wireless networks to facilitate the research and development of MANETs. It would also include DRDC and CF environments such as DREnet and DWAN, and data from one or more of the CFNOC networks. In terms of the lab network itself, it must support the partitioning of isolated network segments for the purpose of supporting a variety of environments. This must be accomplished in a flexible and easy-to-configure manner.

3.2.4.3 Hardware

The hardware in use in the CCDC must be scalable in order to support ever increasing workloads as a result of additional users and increasingly process-intensive applications. Supporting these process-intensive experiments requires that the CCDC be capable of dedicating specific hardware resources to experiments and distributing the processing workload across multiple systems. In terms of storage, the CCDC must have a large (e.g., 10+ terabytes) storage capacity to support large datasets. This storage must be extensible to support future requirements. Furthermore, it must support very rapid storage access and a large number of simultaneous disk reads.

In addition to standard system resources, the CCDC must also support a number of additional hardware resources in order to facilitate specific research. These hardware requirements are not extensive enough to warrant a separate enclave, so they need to be addressed within the DRDC Ottawa Domains themselves. They include the following:

- Removable storage units to support chain of custody rules required for investigations;
- Physical system access to support research into cross-layer information exchange;
- TPMs for platform integrity;
- Hardware-based traffic generators;
- Port mirrors and network taps; and
- Web filtering and firewall appliances.

3.2.4.4 Software

Within the Cyber Operations section of DRDC Ottawa, software acquisition and use has typically been conducted in research project silos. The disadvantage of this approach is that the entire section does not have access to the software or the expertise contained in the silo. A centralized approach would ensure that all software is available for use by all Cyber Operations personnel. In addition, a centralized approach allows Cyber Operations staff to take advantage of a standard library of images of vendor software and operating systems. This will allow Cyber Operations staff to spend more time conducting research experiments, consisting of a variety of applications and operating systems, rather than setting them up. Lastly, this centralized approach will provide scalable software performance due to the fact that the software is running on a common pool of hardware.

In terms of the software required to conduct experiments, the CCDC needs to be equipped with a variety of simulation and emulation software. This software includes the following:

- Traffic generation software (network layer and application layer);
- Virtual channel emulators;
- Virtual mobile devices; and
- SDRP.

In addition, the CCDC must support a wide range of additional software including the following:

- Software to manage version control for development projects;
- Network IDS/IPS sensors and SIEM software;
- Statistical computing languages and environments;
- CAD tools;
- Open source machine learning software;
- Network protocol analyzers;
- Cloud computing software;
- Endpoint protection software including virus scanners;
- Malware analysis tools; and
- Network and system monitoring software.

3.2.4.5 Data

Realistic data is an integral component of experiment development and testing. Consequently, the CCDC should be equipped with a library of data, including CF data sources and joint exercise/experiment data, which would be available to all Cyber Operations staff for their research. These data sets would reside in the CCDC domain that is appropriate to their classification. The following types of data would be included:

- Internally generated data;
- Client capture relay data;

- Live data feeds;
- PREDICT datasets; and
- Blended datasets.[37]

More specifically, this would include the following:

- Live capture of DREnet data;
- Live capture of DWAN data;
- UAV or Link 16 capture data;
- Military SATCOM data; and
- JNDMS and ARMOUR feeds.

3.3 Research Centres

There are currently eight centres within DRDC. However, based on the formalized requirements, Cyber R&D staff members currently have a requirement to collaborate among three of the research centres: DRDC CORA, DRDC Ottawa and DRDC Valcartier. However, there may be a requirement in the future to more closely collaborate with the other research centres, such as the DRDC Centre for Security Science (CSS) or DRDC Toronto. In some cases, the research centres should have their own lab networks in order to facilitate administration and provide local support. However, the individual unclassified lab networks should be connected (in Phase III) in order to facilitate collaboration.

3.3.1 DRDC Valcartier

DRDC Valcartier has a requirement for an Unclassified Domain in which to conduct malware analysis and penetration testing research. It is envisioned that the DRDC Valcartier Unclassified Domain would be similar in most respects to the DRDC Ottawa Unclassified Domain. As with DRDC Ottawa, DRDC Valcartier needs to have complete control and setup of their own network. In addition, they require an anonymized Internet connection to their Unclassified Domain in order to enable software download and to facilitate malware research. They also require a variety of hardware platforms, both conventional and unconventional, to facilitate their testing.

There are a number of key differences between the two Unclassified Domains. First, the DRDC Valcartier Unclassified Domain would need to be sized to reflect the user community and envisioned use within DRDC Valcartier. Second, it would need to provide sufficient isolation between research environments for malware and penetration testing research. Third, it would

[37] A blended dataset is a combination of two or more datasets. These datasets are typically combined for research purposes.

need to be equipped with specialized malware analysis and penetration testing software, including the following:

- System emulators;
- Malware analysis systems & scanners;
- Network IDS/IPS sensors and SIEM software;
- Monitoring tools;
- Kernel debuggers;
- Code analysis tools;
- Task automation frameworks;
- Forensic/analysis tools;
- Vulnerability scanners and penetration testing software;
- Packet manipulation tools;
- Penetration testing-specific operating system distributions;
- Variety of operating systems;
- Repository of malware; and
- Target environments for penetration testing.

3.4 Research Enclaves

Due to the diverse research requirements within the Cyber Program within DRDC, it is nearly impossible to address all of them within the two primary domains. Not only do some research activities have specific isolation/containment requirements, but others require specialized equipment specific to a particular research group. Furthermore, some research activities require access to physical systems, so the use of virtualization may introduce artifacts that could adversely affect experimental results. Domains based solely on virtualized infrastructures could be unsuitable for this type of research.

Consequently, based on the formalized requirements, it was decided that the domains would be used for the majority of computer-based research. However, they would be supplemented with research enclaves for conducting research requiring specialized equipment. This proposed use case is well illustrated by the Resilient Tactical Networks group. This group envisions using the two main DRDC Ottawa domains for simulations, development and testing using virtual emulators, and even as a simulated Forward Operating Base (FOB). However, ultimately they will need to field-test actual wireless devices/MANETs. Consequently, they require a wireless research enclave to perform this specialized research.

This section will examine the following research enclaves:

- CPU/GPU Cluster Enclave;
- Crypto Enclave;
- DETER Enclave;
- Electronic Warfare (EW) Enclave;
- Malware Enclave;
- Physical Enclave; and
- Wireless Enclaves.

Note 1 – It is assumed that the ARMOUR and SAMSON lab environments would be subsumed by the CCDC.

Note 2 – Nothing in the logical design precludes the addition, or subtraction, of research enclaves.

3.4.1 CPU/GPU Cluster Enclave

A CPU and/or GPU cluster enclave would consist of a large number of clustered compute nodes capable of performing a great many calculations in order to solve complex problems. The CPU/GPU cluster enclave could be used for analyzing brute-force attacks on passwords or cryptographic keys.

3.4.2 Crypto Enclave

It is anticipated that the Crypto Enclave would be equipped with Type-1 cryptographic components needed for classified research.

3.4.3 DETER Enclave

The DETER testbed is "*a shared infrastructure designed for medium-scale repeatable experiments in computer security, especially those experiments that involve malicious code"* **[1]**. The testbed is used by academic, industry, and government researchers "*to provide an experimental infrastructure to support the development and demonstration of next-generation information security technologies*." The Cyber Program within DRDC intends to establish DETER testbeds at DRDC Ottawa and DRDC Valcartier. The DETER testbeds allow experimenters to repeat experimental conditions precisely, modifying them only in a controlled manner. Furthermore, they are partitionable into multiple independent experimental testbeds that can be used simultaneously.

Due to the nature of its research, the DETER enclave must provide containment. The Internet, the main enclave and the other research enclaves must be protected from the side effects of the security experiments that run in the testbed. Likewise, the experiments running in the DETER enclave must not be affected by these entities. The DETER testbed provides this isolation through the use of limited network connectivity (no route for packets to leave the testbed) and firewalls. Furthermore, it provides physical link isolation in order to prevent one experiment from interfering with another.

While remote access to the DETER testbed is provided, there should be limited connectivity between it and the main enclave (for all but the most dangerous experiments) in order to support experiment initiation and monitoring. However, there must be a mechanism to transfer data, including code, between the two lab environments. Furthermore, federated connectivity with the DeterLab itself may be desirable in the future in order to support collaborative research with a broader cyber S&T community. However, federated connectivity between DETER testbeds in DRDC Ottawa and DRDC Valcartier is desirable immediately. This connectivity would permit Cyber R&D staff to collaborate with each other on experiments. This can be accomplished using the DETER Federation Architecture (DFA). This is discussed in some detail in *A Federated Experiment Environment for Emulab-based Testbeds* **[2]**.

3.4.4 EW Enclave

It is envisioned that connectivity with the EW Enclave is a future capability. Consequently, it will not be addressed within this iteration of the report.

The EW Enclave would consist of a classified EW lab containing traditional laboratory equipment such as radios, spectrum analyzers, antennas, oscilloscopes, Vector Signal Analyzers (VSAs), etc. This equipment, which might typically be connected to stand-alone computer systems, is used for testing. In addition, experiments on live over-the-air signals are conducted using feeds from rooftop antennas.

During the interview process with EW personnel, the idea that the traditional lab equipment in the EW lab could be connected to the Classified Domain and then provisioned as required was explored. This approach, which would have the benefit of facilitating collaboration and data exchange while increasing the potential use of available equipment, may be desirable at some future point in time.

3.4.5 Malware Enclave

A physically isolated malware enclave may be required for research and analysis of particularly virulent code. In the event that a separate malware analysis lab is required, it should be designed as a completely isolated lab consisting of dedicated systems whose disk drives and memory chips never leave the lab and are never reused.

3.4.6 Physical Enclave

There is a requirement for physical systems in order to conduct research and development activities requiring direct interaction with physical hardware. For example, there may be a requirement to collect system metrics. These characteristics will likely differ between physical and virtualized systems. Similarly, there may be a requirement for direct system access in order to support research into cross-layer information exchange.

3.4.7 Wireless Enclaves

Wireless enclaves, likely consisting of both an unclassified and a classified enclave, would serve to provide wireless connectivity to the main Domains in order to support wireless research, including EW work. Specifically, the wireless enclaves could consist of the following specialized equipment:

- Smart phones and tablets with wireless interfaces for testing;
- SDRP – Universal Software Radio Peripheral (USRP), FatBoy, LYRtech, PS3;
- Pico/micro base stations supporting wireless interfaces such as LTE, WiMAX, Iridium, Inmarsat BGAN, Thuraya, Bluetooth, and mobile network analyzers;
- Military tactical radios;
- Wireless routers; and
- Wireless traffic monitors.

3.5 Connectivity

The intent of the CCDC is to facilitate Cyber Operations research in part through collaboration with other DRDC research centres, government departments and agencies, international partners, industry and academia. At this point in time it is unknown what level of connectivity is required, or even possible, to facilitate collaboration with the various entities. Consequently, this section is largely intended to serve as a starting point for these future considerations. It is worth noting that connectivity will also be affected by external considerations such as government policy and the mandate of Shared Services Canada (SSC).

Potential factors to consider for connectivity include, but are not limited to, the following:

- Cross-Domain Solution (CDS);
- DND Organizations & Networks;
- Internet Access from Unclassified Domain; and
- Remote Access to Unclassified Domain.

3.5.1 Cross-Domain Solution (CDS)

The Unified Cross Domain Management Office (UCDMO)[38] defines a CDS as an "*information assurance solution that provides the ability to access or transfer information between two or more security domains.*" In terms of the CCDC, a CDS is required to mediate the one-way transfer of data between the Unclassified and Classified Domains. This transfer mechanism would allow data, including software and firmware patches, to be sent from the Unclassified Domain to the Classified Domain but not in the reverse direction.

Low-to-high transfer CDS control the flow of information from a low domain to a high domain while preventing information flow in the reverse direction. Due to the requirement to prevent information flow in the reverse direction many of these CDS include a one-way data diode. Low-to-high CDS are primarily concerned with the unauthorized transfer of malicious code to the high domain. This threat is typically mitigated through the use of a data filtering mechanism.

From **[3]**, "*a data diode is a computer security device that restricts the communication along a network connection between two points so that data can only be transmitted in one direction. The data diode is configured to guarantee that no data can be passed, either explicitly or covertly, in the opposite direction.*" The data filtering mechanism is used to identify inappropriate content within specific file formats and, if possible, removes it so that the file can be transferred safely between security domains.

While it is anticipated that the CDS will be a one-way low-to-high CDS, there may be a requirement to transfer some data in the reverse direction. Given the risk of data leakage from the Classified Domain to the Unclassified Domain, in all likelihood Reliable Human Review (RHR) would need to be performed on any data to be transferred in this direction.

DRDC is encouraged to consult with the Communications Security Establishment Canada (CSEC) for this component of the CCDC. CSEC has conducted a great deal of research in the area of CDS, including developing their own CDS (e.g., Secure Data Pump (SDP) Version 2) and testing partner CDS (e.g., File Sanitization Tool (FiST)).

3.5.2 DND Organizations & Networks

Some degree of connectivity/collaboration with the following DND organizations and networks is desired:

- DREnet;
- CFNOC;
- CFTDC;
- CFWC; and

[38] The UCDMO is the group responsible for all U.S. Department of Defense (DoD) and Intelligence Community (IC) cross-domain efforts. Additional information can be found at http://www.ucdmo.gov/

- DWAN.

3.5.2.1 DREnet

The DREnet serves as the backbone for each of the eight DRDC research centres located in Canada. Its main purpose is to support research activities for defence scientists, engineering and technical staff, as well as associated administrative staff. One-way connectivity from the DREnet to the Unclassified Domain is desirable in order to facilitate the live capture of DREnet data to support cyber S&T activities.

3.5.2.2 CFNOC

One-way connectivity from specific CFNOC networks to the Classified Domain is desired in order to facilitate the transfer of limited data for analysis.

3.5.2.3 TDC/CTDC

Connectivity to the TDC and CTDC at Tunney's Pasture is desired in order to facilitate project migration from the CCDC to the CTDC. This project migration capability would allow testing to be conducted on simulated DND networks. Specifically, connectivity from the CCDC Unclassified Domain to the TDC and the unclassified CTDC is required. In addition, connectivity from the CCDC Classified Domain to the classified CTDC is required. The TDC hosts a version of the DWAN while the CTDC hosts a version of the Consolidated Secret Network Infrastructure (CSNI).

3.5.2.4 CFWC

The Canadian Forces Warfare Centre (CFWC), which is located on the same campus as DRDC Ottawa, has the mission of enabling CF joint and integrated force development through conceiving, designing and supporting the building and delivery of joint capabilities in order to enhance CF operational effectiveness and readiness.[39] Cyber Operations personnel often participate and conduct experiments in these exercises. Consequently, connectivity to the CFWC Battle Lab from the Classified Domain is desirable for a variety of exercises such as CAGE and JOINTEX.

> Note – SAMSON Deployment in CAGE II
>
> The SAMSON deployment in CAGE II consisted of three servers (two primaries and a hot backup), two crypto boxes (one primary and a hot backup) and a network switch. This hardware was used to host ten Virtual Machines (VMs) that comprise the SAMSON security services used to provide caveat separation in a coalition environment. Assuming that connectivity existed between the CCDC and the CFWC, a separate instantiation could quickly be deployed within the CCDC rather than having to deploy a separate instantiation physically to the CFWC.

[39] http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=9533

3.5.2.5 DWAN

The DWAN is an unclassified network that is used to connect the various Local Area Networks (LANs) and Metropolitan Area Networks (MANs) within DND. One-way connectivity from the DWAN to the Unclassified Domain is desirable in order to facilitate the live capture of DWAN data.

3.5.3 Internet Access from Unclassified Domain

Internet access is required from the Unclassified Domain in order to download software and firmware updates for systems in both the Unclassified and Classified Domains. In addition, an anonymized Internet connection is required. Updates could be downloaded in the Unclassified Domain and transferred across the CDS for use to the Classified Domain. In order to minimize the risk of including an Internet connection in the CCDC, its use will need to be carefully controlled. It will need to be an assigned resource, and its use will need to be limited to a carefully controlled zone such as a Public Access Zone (PAZ).[40]

3.5.4 Remote Access to Unclassified Domain

Secure remote access is required to the Unclassified Domain in order to facilitate collaboration with partners and allow Cyber Operations staff to access their experiments remotely and work from home, from another facility, or while on travel duty.

3.6 Demonstration Environment

The demonstration environment is extremely important to Cyber R&D staff who need to be able to share project outputs and technologies with colleagues, clients, and partners. Demonstrations allow researchers to engage with potential capability users in order to solicit feedback that can be used to improve the work.

3.7 Training Environment

Cyber R&D staff members have a requirement for a cyber training environment in order to train a small number of users at a time. Specifically, one initiative in the Cyber Operations & Signals Warfare Section of DRDC Ottawa has a regular requirement to train approximately eight CF analysts on cyber tools and techniques. In addition, it is envisioned that other Cyber R&D projects will periodically have training requirements. For example, the ARMOUR TDP has plans to train operators from CFNOC on the system in order to solicit usability feedback. Consequently, the training environment must facilitate training, including the provisioning and de-provisioning of systems for training. Furthermore, in order to minimize costs, power and space requirements, the training environment should be shared between both the Unclassified and Classified Domains.

[40] For a complete overview of network security zones used in GC networks readers are encouraged to consult *Information Technology Security Guideline (ITSG)-38 Network Security Zoning – Design Considerations for Placement of Services within Zones* **[4]**.

This would involve the use of non-persistent hardware that could be wiped clean at the end of each training session.

4 Design Considerations

4.1 Overview

This section of the report will examine a number of key design considerations that will have a significant impact on the detailed reference architecture discussed later in Section 6. Specifically, this section will examine the following design considerations:

- Physical or Virtualized Implementation;

- Virtualization Product Offerings; and

- Centralized Storage Technologies.

4.2 Physical or Virtualized Implementation

One of the main design considerations is whether to implement a traditional lab infrastructure or a virtualized lab infrastructure. A physical implementation has a one-to-one relationship between applications and hardware. In contrast, virtualization is used to abstract the physical characteristics of the underlying hardware from the applications and operating systems running on it. Consequently, a virtualized implementation has a many-to-one relationship between applications and hardware. This section of the report will examine the benefits and drawbacks of each approach, and will provide a recommendation as to the preferred approach for the CCDC.

4.2.1 Benefits

There are a number of benefits to a physical lab implementation. These include the following:

- Isolation – In a physical lab implementation operating systems and applications run on their own physical hardware. In contrast, in a virtualized lab environment operating systems and applications run on shared physical hardware. Due to the dedicated system resources (e.g., memory, processing) and physical separation, a physical lab implementation provides a higher level of isolation than its virtualized counterpart. This level of isolation is especially important for certain research (e.g., malware analysis);

- Metrics – A virtualized environment has different characteristics than a physical environment. In most cases this difference is inconsequential. However, for certain tasks, such as system metrics, the difference between environments is important. In order to accurately obtain some system metrics the operating systems and applications must run directly on physical hardware without any resource sharing; and

- System Access – Some security research is interested in cross-layer information exchange. In a virtualized environment this information may prove difficult to obtain or inaccurate. Consequently, a traditional physical lab implementation may be better for performing this type of research.

There are a number of benefits to virtualized lab environments. These include the following:

- Utilization – Computer systems in most organizations are significantly underutilized.[41] Virtualization allows multiple operating systems and applications to be hosted on a single system in order to dramatically increase its utilization rate. This ultimately reduces the need for additional systems resulting in reduced energy consumption, physical space requirements, capital expenditures, and operational expenditures;

- Provisioning – Virtualization of the underlying infrastructure greatly facilitates the provisioning of network environments for research. Through virtualization, the setup and provisioning of these network environments can be accomplished in a matter of minutes. In contrast, setting up the equivalent infrastructure in a physical lab would likely take days;

- Backup and Archival – Backing up or archiving a project in a virtualized environment is simply a matter of making a copy of the Virtual Machines (VMs) and network configuration on backup media. In many organizations this backup is configured to be performed automatically, even on live systems;

- Flexibility – A virtualized environment abstracts the underlying hardware, making it adaptable and easy to change, such as when moving systems and reconfiguring networks. A purely physical implementation does not have the same flexibility; and

- Management – It is estimated that an administrator can manage 50 servers in a physical environment. The same administrator can manage between 200-300 VMs in a virtual environment, and up to several thousand VMs when automation is properly implemented **[5]**.

4.2.2 Drawbacks

The drawbacks in terms of a physical lab implementation are the reverse of the benefits of a virtualized lab implementation. Specifically, they include low utilization rates, time and labour intensive provisioning, more difficult backup and archival, limited flexibility, and increased management complexity.

There are a number of drawbacks to virtualized lab environments. These include the following:

- Unsuitable for Some Research – Virtualized environments may not be a suitable platform for certain Cyber Operations research due to the fact that they abstract the underlying hardware, and due to limitations in terms of the isolation that they provide;

- Single Point of Failure – In certain environments virtualization can be problematic in that the failure of a single system can have a catastrophic effect on a number of applications. In a standard environment, the failure of a single system will in all likelihood only affect

[41] Utilization rates for most organizations are estimated to be between 5-15% of their total load capacity. (source – http://www.vmware.com/solutions/consolidation/consolidate.html)

a single application. This drawback is more applicable to production environments than it is to lab environments and can be mitigated through the use of additional safeguards (e.g., failover, redundancy); and

- Software Licensing – In many cases software is licensed differently for virtual environments. Care needs to be taken to ensure that Cyber R&D staff members do not inadvertently contravene software licensing by using multiple instantiations of a software package simultaneously.

4.2.3 Analysis

The benefits of a virtualized lab implementation greatly outweigh those provided by a physical lab implementation. Specifically, the abstraction of the underlying hardware provides a great deal of flexibility and simplifies the provisioning of systems and network environments. This is invaluable in a research and development environment where systems and network environments are constantly rebuilt. Consequently, the CCDC will adopt a primarily virtualized environment. However, in order to accommodate certain types of research ill-suited to virtual environments, the CCDC will also include a limited number of physical systems.

4.3 Virtualization Product Offerings

In terms of x86 server virtualization, there are a number of commercial and open sources offerings to choose from. These include the following:

- Citrix Systems (Xen) – Xen is an open source, bare-metal hypervisor originally developed by the University of Cambridge in 2003. Xen was supported by XenSource Inc., which was acquired by Citrix in 2007. While Xen continues to be an open source project[42], it is used in a number of commercial offerings, of which Citrix is the most widely deployed. The Citrix server virtualization product is XenServer, while its Virtual Desktop Infrastructure (VDI) product is VDI-in-a-Box. In terms of management for cloud environments, Citrix has CloudPlatform and CloudPortal;

- Microsoft – Microsoft's entry into the virtualization market came in 2003 when it acquired Virtual PC and Virtual Server from Connectix Corporation. Microsoft's most recent server virtualization product is Windows Server 2012 with Hyper-V. Microsoft also offers a VDI solution through Hyper-V and Remote Desktop Services. System Center 2012 is used for management, including in cloud environments;

- Oracle (Xen) – Sun entered the virtualization market in 2007 with Sun 8 Containers. This was followed up in 2008 with its purchase of innotek, the makers of VirtualBox. Sun was acquired by Oracle in 2010. Oracle has a wide range of products based on the open source Xen hypervisor. These include Oracle VM Server for x86 (server virtualization), Oracle Integration Management Solution (management, including cloud environments), and Oracle VDI;

[42] http://www.xen.org/

- Red Hat (KVM) – Kernel-based Virtual Machine (KVM) was originally developed at Qumranet, which was acquired by Red Hat in 2008. Red Hat's server virtualization offering is Red Hat Enterprise Virtualization for Servers; and

- VMware – VMware is widely acknowledged as the grandfather of x86 virtualization, first with VMware Workstation in 1999 and later with VMware Server in 2001. It is perhaps best known for its bare-metal hypervisor for server virtualization: ESXi. Its current offerings include VMware vSphere[43] (bare-metal hypervisor for server virtualization), vCenter Server (management) and vCloud Director (cloud computing).

InfoWorld conducted a virtualization shoot-out in 2011[44] in which they invited Citrix, Microsoft, Red Hat, and VMware to install their products in its Advanced Network Computing Lab at the University of Hawaii. The server virtualization products were assessed in a variety of ways including ease of installation, hypervisor performance, management capabilities (e.g., templating, cloning, updates and patching, snapshots and backups, load balancing and high availability), etc. VMware vSphere 4.1 was the winner, followed by Red Hat, Microsoft, and Citrix. InfoWorld concluded that VMware "*leads the pack by a handy margin, but the gap is closing fast*." Furthermore, according to InfoWorld the difference between VMware and its competitors lies in its advanced functionality and more polished solution. InfoWorld also declared VMware vSphere 5 one of its 2012 Technology of the Year Award winners.[45]

In June 2012 Gartner released its Magic Quadrant for x86 Server Virtualization Infrastructure.[46] VMware, Microsoft, and Citrix were all considered leaders, whereas Red Hat was deemed a niche player. The report concluded that "*VMware remains the market share and technology leader, but the market continues to grow, and competitors have a growing share of the market.*"

There may eventually be a time to choose an alternative to VMware for x86 server virtualization. However, at the moment VMware provides the most feature-rich offering for x86 server virtualization, for both lab environments and cloud computing environments.

4.4 Centralized Storage Technologies

Another one of the main design considerations is the technology to be used for the centralized storage architecture. Viable options include the following storage technologies:

- Network Attached Storage (NAS);

- Internet Small Computer System Interface (iSCSI); and

- Fibre Channel (FC).

[43] ESX was VMware's original foray into a bare-metal hypervisor for server virtualization. The successor to ESX was ESXi. ESXi was rebranded to vSphere.

[44] http://www.infoworld.com/d/virtualization/virtualization-shoot-out-citrix-microsoft-red-hat-and-vmware-666

[45] http://www.infoworld.com/slideshow/24605/infoworlds-2012-technology-of-the-year-award-winners-183313#slide22

[46] http://www.gartner.com/technology/reprints.do?id=1-1B2IRYF&ct=120626&st=sg

4.4.1 NAS

NAS uses a file-sharing protocol over a standard Ethernet network. The host server communicates with the storage system that maintains the disk file system. In terms of VMware, the NAS storage system manages the file system while vSphere is in charge of the network layer. NAS has good performance, is easy to implement and is the least expensive of the storage technologies being considered for the CCDC. However, it has the lowest performance of the technologies being considered, and it uses some of the host server's Central Processing Unit (CPU) in order to allow a software client to communicate with the NAS storage system. If NAS is used, a separate 10 GB storage network is required with full TCP/IP Offline Engine (TOE) cards.

4.4.2 iSCSI

iSCSI, which stands for SCSI over IP, uses a block transfer protocol over a standard Ethernet network. VMware uses the Virtual Machine File System (VMFS), which is managed directly by the ESXi storage layer. iSCSI has very good performance, is relatively easy to implement, is fairly inexpensive, and supports authentication (Challenge Handshake Authentication Protocol (CHAP)) and encryption for security. However, it uses the CPU resources of the host server, which adds to the CPU overhead. If iSCSI is used, a separate storage network is required with full TOE cards. The storage network can be 1 GB or higher. However, if it is 10 GB then iSCSI Host Bus Adapter (HBA) cards should be used. This will increase the cost somewhat.

4.4.3 FC

FC uses a block transfer protocol over a dedicated fibre channel. Specifically, FC encapsulates SCSI packets over a dedicated FC network. FC is the most advanced of the protocols being considered, is the most reliable, and uses the least host server CPU resources. However, it requires specialized storage skills, as opposed to networking skills, and is the most expensive. It is the most expensive due to the fact that it involves building a specialized architecture consisting of FC HBA cards, switches, Small Form-factor Pluggable (SFP) ports and cables. Furthermore, since FC has fewer security controls it complicates the implementation of authentication and encryption. If FC is used, a separate FC storage network will have to be implemented. In addition, it is recommended that multiple HBA cards be installed in each host server in order to provide multiple storage array access paths.

4.4.4 Analysis

Table 2 compares[47] the various technologies according to four evaluation factors. A "1" denotes the best option for that particular evaluation factor, a "2" denotes the second best option, and a "3" denotes the least desirable option. In terms of cost and ease of implementation, NAS is the preferred choice followed by iSCSI and then FC. In terms of performance, the ranking is reversed. In terms of security, iSCSI is the best option.

[47] VMware provides a detailed comparison of the various storage technologies. This can be found at http://blogs.vmware.com/vsphere/2012/02/storage-protocol-comparison-a-vsphere-perspective.html

It is estimated that approximately 70% of VMware customers use FC for production environments as it has been the primary choice for a number of years for large datacenter environments **[5]**. However, NAS and iSCSI are becoming increasingly popular alternatives primarily due to cost. While there is no wrong choice, as all three technologies are viable options for the CCDC, the recommendation is to use iSCSI as it delivers very good performance at a good price and is relatively easy to implement. When iSCSI is implemented properly, the difference between iSCSI and FC is likely only a few milliseconds due to the overhead required to encapsulate SCSI commands within TCP/IP. In terms of iSCSI, one also needs to decide whether to use 1 GbE or 10 GbE. For the CCDC, and other Small and Medium Enterprises (SME) implementations, 1 GbE would normally suffice. Furthermore, by employing redundant 1 GbE controllers and paths to the storage array, one can effectively double the network capacity of the storage architecture.

Note 1 – While redundant 1 GbE would normally be sufficient for each of the four networks required in SME implementations, the CCDC is a special case in that Cyber Program staff will be conducting a wide range of experiments, many with high bandwidth requirements. It is for this reason that redundant 10 GbE will be used for the data network.

Note 2 – This analysis was performed for the virtualization storage component of the CCDC. However, the CCDC may also require enterprise storage, and specifically online storage, in order store lab data for use across some of the research environments. Given the limited requirement for enterprise storage in a lab environment, it is recommended that a NAS be implemented over the data network for this purpose.

Table 2 – Storage Technology Comparison

	NAS	iSCSI	FC
Cost	1	2	3
Implementation	1	2	3
Performance	3	2	1
Security	2	1	2

5 Logical Architecture

5.1 Overview

The logical architecture must support a phased implementation. Specifically, it must adhere to the three following phases:

- Phase I: S&T Lab;
- Phase II: Interactive Lab; and
- Phase III: Collaborative Lab.

5.2 Phase I: S&T Lab

Phase I is concerned primarily with providing the basic infrastructure comprising the S&T Lab so that it is fully usable for approximately twenty users. The Phase 1 S&T Lab, as illustrated in Figure 3, will consist of a number of virtualization resources, a virtualization management component and virtualization storage. It is envisioned that equivalent S&T labs will be installed in the other research centres, sized appropriately for their user base.

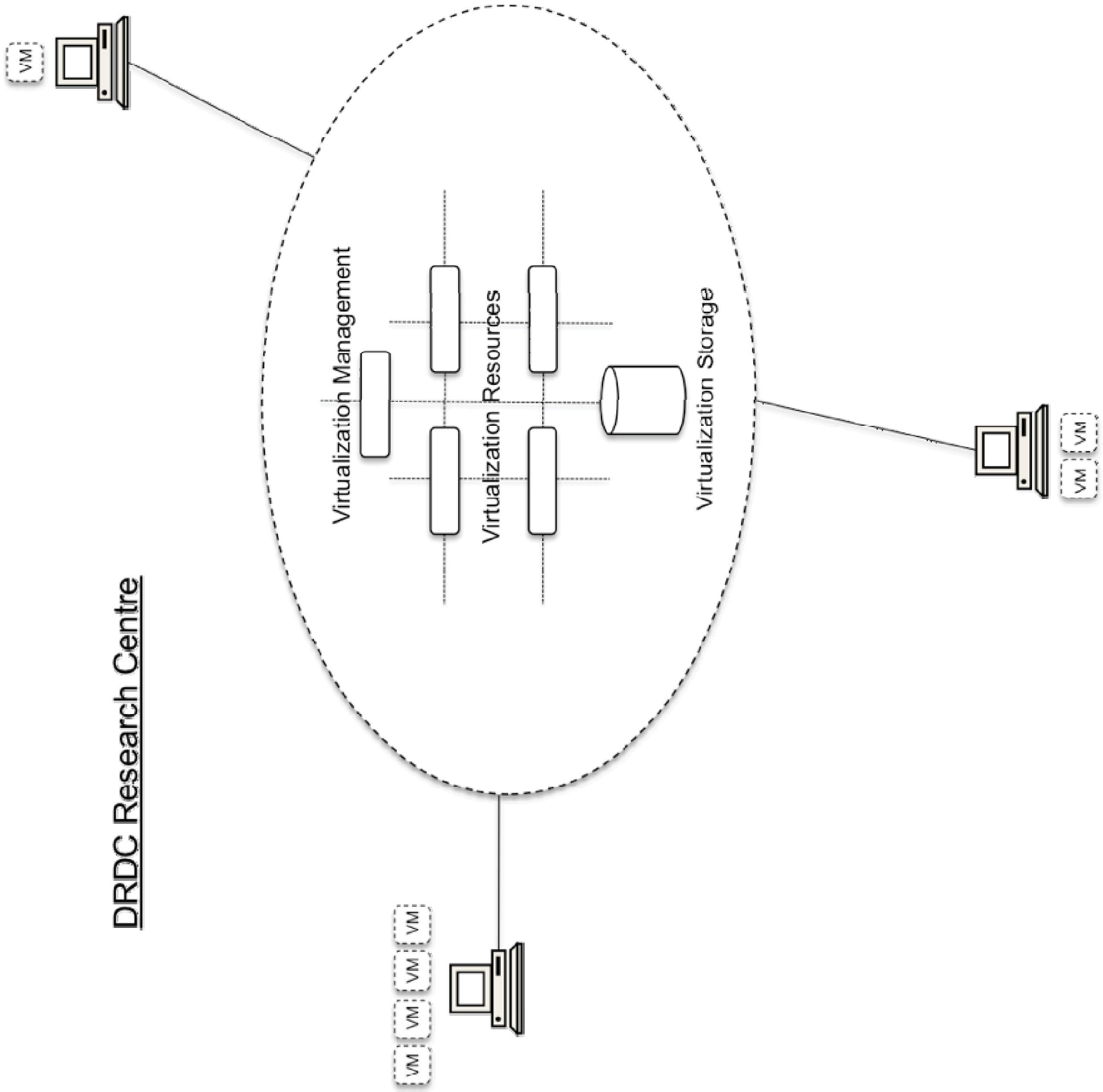

Figure 3 – S&T Lab Logical Architecture (Phase I)

5.3 Phase II: Interactive Lab

Phase II is concerned with expanding upon the basic S&T Lab capabilities built in Phase I. Specifically, the objective of Phase II is an interactive lab that is fully usable by approximately fifty users. The Phase II Interactive Lab, which is illustrated in Figure 4, will include additional virtualization resources, expanded storage capacity and training/demonstration environments. It is envisioned that equivalent interactive labs will be installed in the other research centres, sized appropriately for their user base and the number of demonstration environments required.

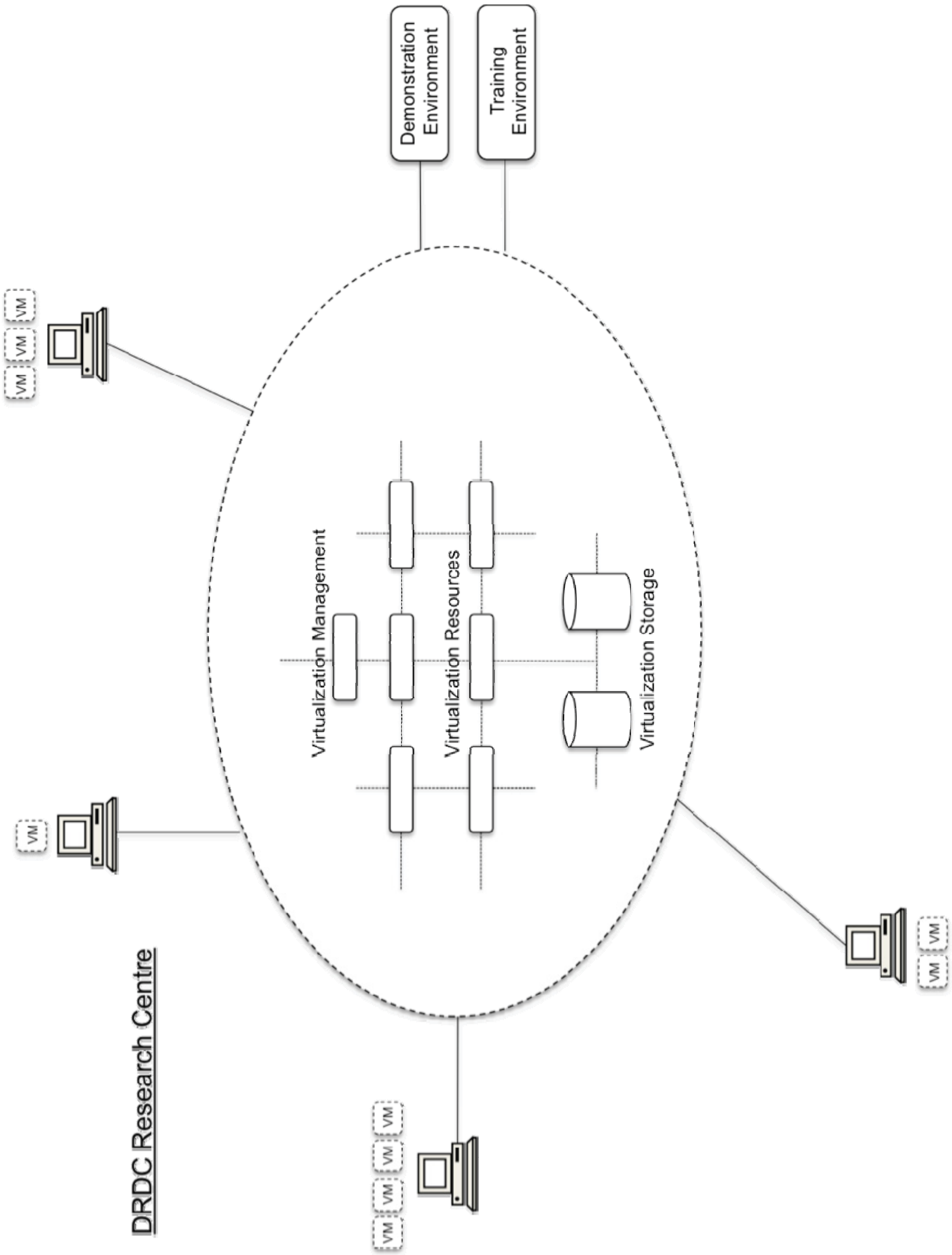

Figure 4 – Interactive Lab Logical Architecture (Phase II)

5.4 Phase III: Collaborative Lab

According to **[6]**: *"Cloud computing is a model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be provisioned rapidly and released with minimal management effort."* Phase III of the CCDC is concerned with transitioning from an interactive lab to a collaborative lab. The interactive lab (Phase II) incorporated demonstration and training capabilities, whereas the collaborative lab will add the ability to conduct research with external partners, including the other DRDC research centres.

The Phase III Collaborative Lab, illustrated in Figure 5 will transition into a private cloud offering Infrastructure-as-a-Service (IaaS) capabilities. A private cloud is operated solely for an organization and can be managed by the organization or a third party. The infrastructure can be located on-premises or off-premises. IaaS allows users to self-provision resources such as processing, memory, network, and storage, which would meet the needs for a flexible, collaborative S&T lab.

Specifically, the collaborative S&T lab will include additional virtualization servers, additional storage capacity and a cloud management capability. The cloud management capability provides an access point to the cloud where users can sign-up for accounts and manage the resources that they use. It is envisioned that equivalent collaborative labs will be installed in the other research centres, sized appropriately for their user base. These labs would be interconnected using encrypted leased lines or Virtual Private Networks (VPNs), thereby allowing the research centres to collaborate on research activities and share computing resources as needed.

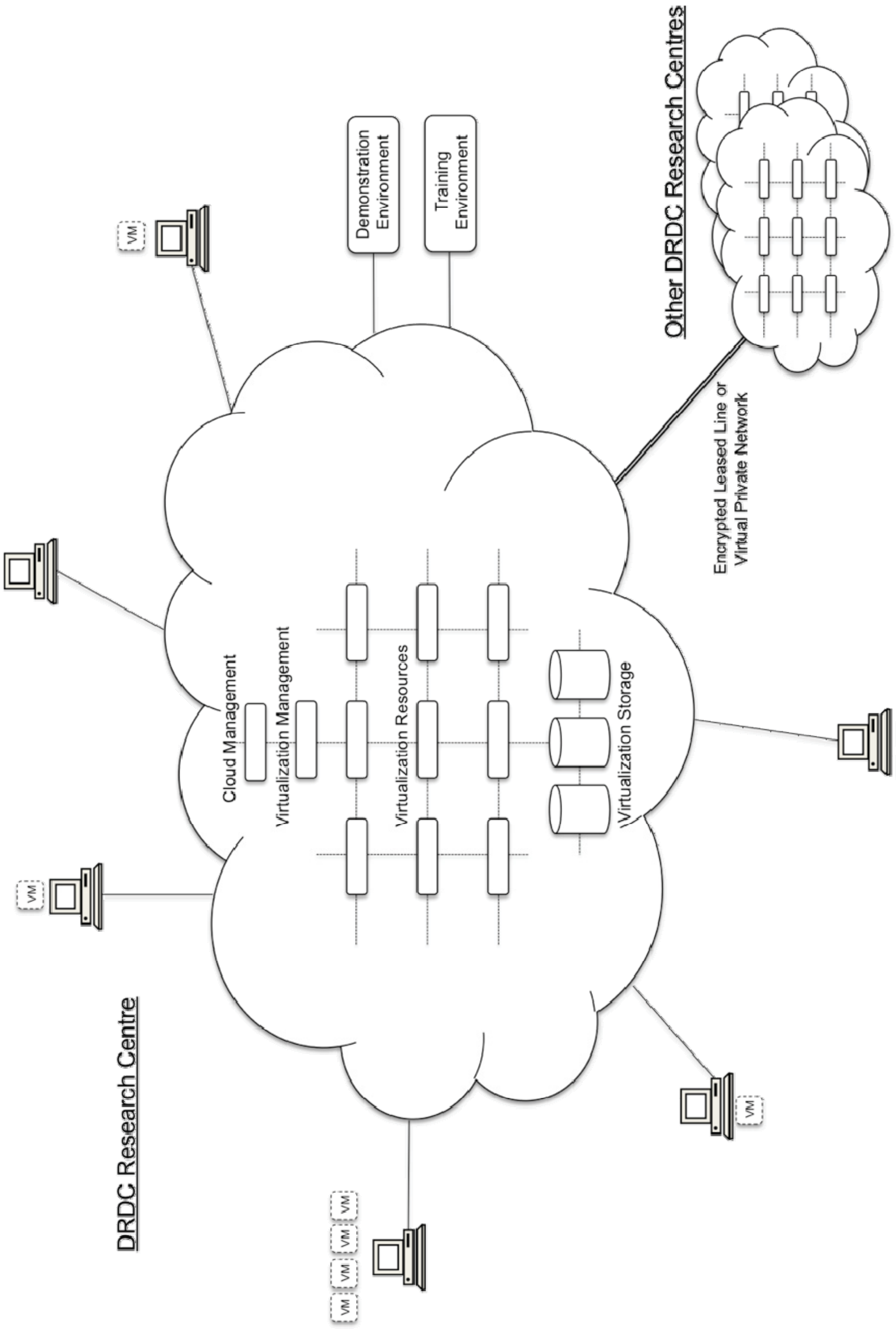
DRDC Research Centre
VM
VM
VM
VM
VM
VM
VM
VM
VM
Cloud Management
Virtualization Management
Virtualization Resources
Virtualization Storage
Demonstration Environment
Training Environment
Encrypted Leased Line or Virtual Private Network
Other DRDC Research Centres

Figure 5 – Collaborative Lab Logical Architecture (Phase III)

6 Reference Architecture

6.1 Overview

This section of the report will provide a reference architecture for the CCDC. Figure 6 provides a logical view of the reference architecture, while Figure 7 provides a physical view of the reference architecture. The reference architecture consists of the following three main components:

- Management Cluster – The Management Cluster contains the core infrastructure components needed to run the CCDC. These components are separated from the resource group in order to improve manageability. The Management Cluster will initially include the vCenter Server, the vCenter database and Active Directory (AD). It is envisioned that the AD will be used for access control, timekeeping (Network Time Protocol (NTP)) and networking (Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP)). The Management Cluster will ultimately, in Phase III, include vCloud Director. Both the vCenter Server and the vCloud Director can share the database server. However, they each require a separate database instance;

- Resource Group – The Resource Group consists of VMware vSphere hosts that are managed by the vCenter Server. These systems host end-user VMs. Initially, there will be a single cluster and resource group managed by a single vCenter Server. As the processing requirements increase in Phases II and III of the CCDC, additional vSphere servers can be added to the cluster. At some future point in time it may be necessary to group vSphere hosts into multiple clusters[48] and even group clusters into multiple resource groups[49] to be managed by separate vCenter Servers; and

- Storage – The Storage Area Network is based on iSCSI technology. As the storage requirements increase in Phases II and III of the CCDC, additional storage capacity can be added.

This section of the report will address the following aspects of the CCDC:

- Software;

- Systems;

- Networks;

- Storage;

- Management;

[48] Clusters are used to group similar servers together so that they can be viewed as though they are a single system. For example, servers with the same number of cores, memory and processors can be grouped into a cluster in order to differentiate compute resources by capacity or performance.

[49] Resource groups are used as a means to manage large numbers of VMs.

- Remote Access;
- Availability;
- Access Control & Security; and
- Staffing.

Note – The Unclassified and Classified Domains of the CCDC are identical in most respects in order to facilitate implementation and operation. This section will not differentiate between the two domains except to highlight where they differ. However, it is important to remember while reading this section of the report that the two domains, while similar, are completely separate infrastructures with limited (i.e., one-way CDS) connectivity.

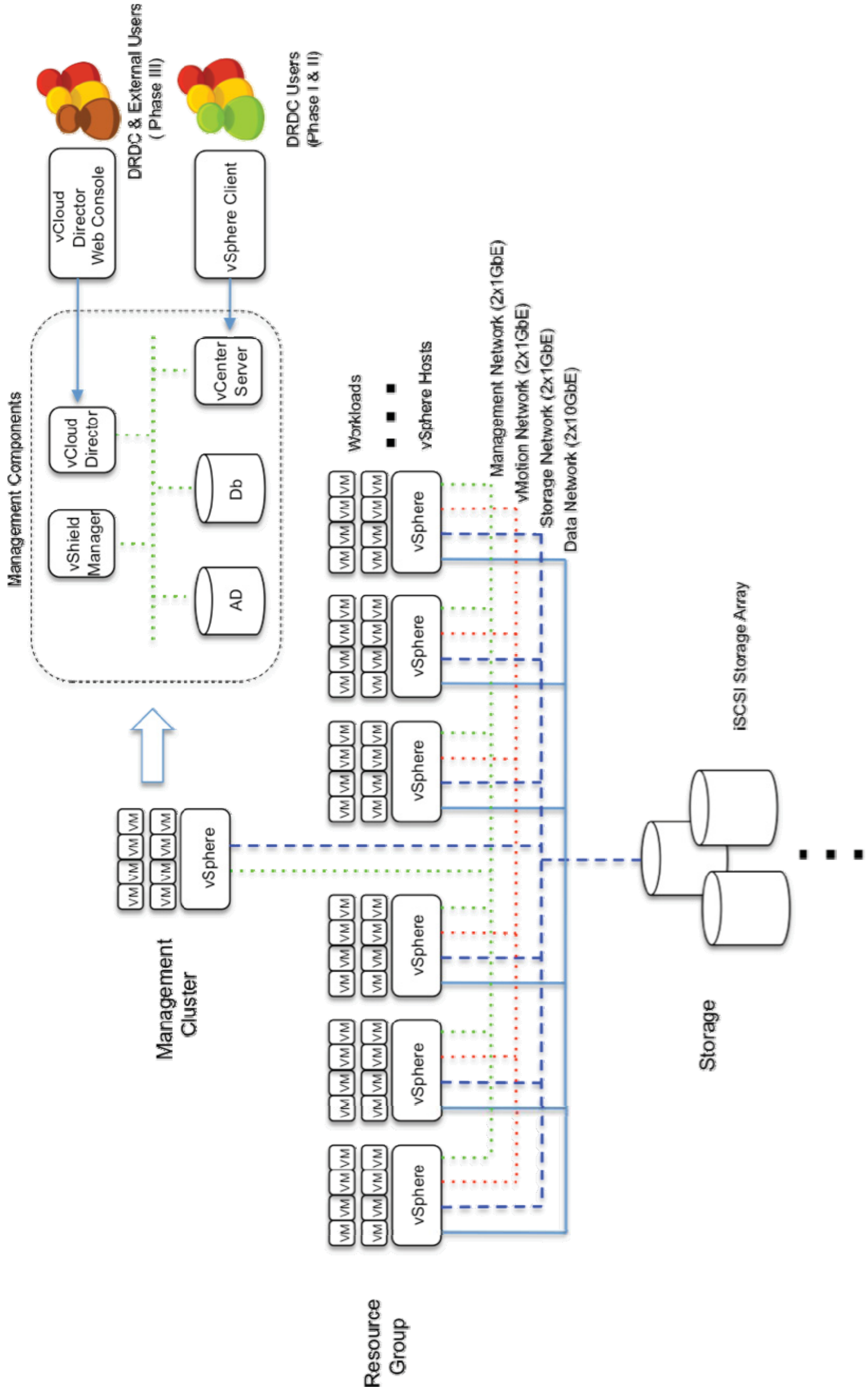

Figure 6 – CCDC Logical Reference Architecture

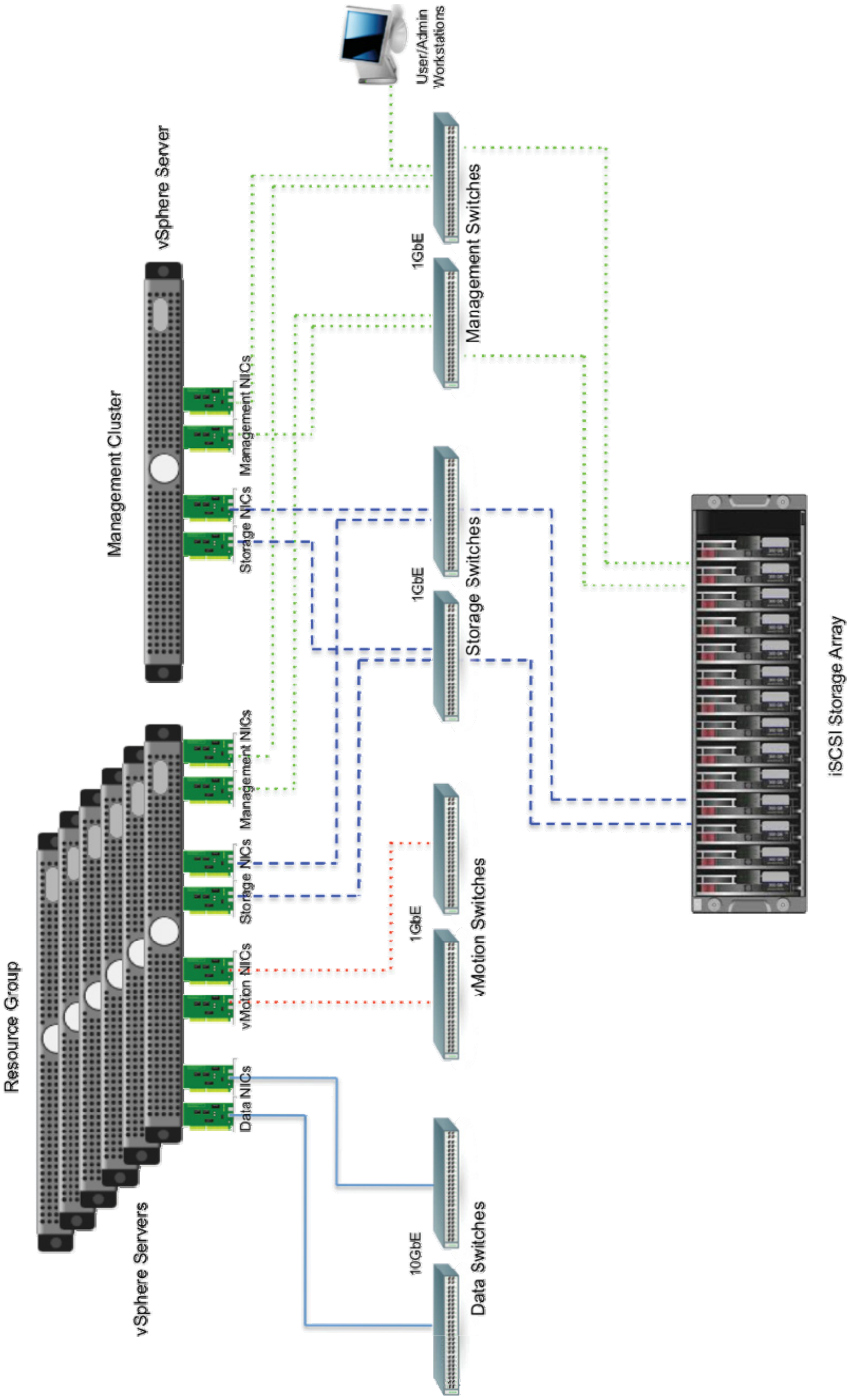

Figure 7 – CCDC Physical Reference Architecture

6.2 Software

This section of the report will provide an overview of the virtualization software required for the CCDC. Specifically, it will examine the following three VMware families of virtualization software, as well as VM images required:

- vSphere;
- vCenter Server;
- vCloud Director; and
- VM images.

6.2.1 vSphere

vSphere is VMware's bare-metal hypervisor, which means that it runs directly on the server hardware. It is responsible for providing abstraction of the physical server layer in the CCDC. vSphere 5 is approximately 150 MB in size and based on the ESX hypervisor architecture but with the service console removed. VMware offers the four following versions of vSphere; vSphere Hypervisor Edition, vSphere Standard, vSphere Enterprise, and vSphere Enterprise Plus. vSphere Hypervisor Edition is a free version of vSphere that includes the basic hypervisor functionality. The major drawback to this version of vSphere is that it cannot be managed by vCenter Server. Instead, it needs to be managed by vSphere Client through a direct connection to the host. This limitation ensures that the free version of vSphere can only be used for extremely small deployments (i.e., small lab environment consisting of a couple servers) as it is unsuitable for larger deployments such as the CCDC. vSphere Enterprise Plus encompasses all of the functionality of vSphere Enterprise as well as additional functionality to facilitate deployment and management. Similarly, vSphere Enterprise encompasses all of the functionality of vSphere Standard as well as additional functionality to facilitate deployment and management.[50] For the purpose of the CCDC, it is recommended that vSphere Standard be used and that it be installed locally on each system rather than on the shared storage array. DRDC can later upgrade to vSphere Enterprise or vSphere Enterprise Plus if warranted.

In terms of management, vSphere supports the following connection methods:

- Direct Console User Interface (DCUI) – This involves administering vSphere using a local connection to the vSphere server. DCUI will seldom be used within the CCDC;
- vSphere Client – The vSphere Client allows a direct connection to the vSphere server or through vCenter. It is only available for Microsoft environments; and

[50] A good comparison of the functionality provided in each version of vSphere can be found at http://www.vmware.com/in/products/datacenter-virtualization/vsphere/compare-editions.html

- vSphere Web Client – The vSphere Web Client provides administration of the virtual environment using a browser. It is provided through vCenter; however, the vCenter Web Administration module needs to be installed. It is available for both Windows and Linux environments.

Note – Optional vSphere Components

A number of components in the vSphere family can be considered optional and may be included at some future point in time in order to increase operational efficiency. However, these components are not required at this time. These vSphere components include the following:

- vSphere High Availability (HA) – vSphere HA ensures that when a host fails, all VMs connected to the host are immediately and automatically restarted on the other servers within the cluster. HA will not initially be provided within the CCDC; and

- vSphere Fault Tolerance (FT) – vSphere FT improves upon vSphere HA by offering high availability while protecting VMs from a host server failure. Fault tolerance will not initially be provided within the CCDC.

6.2.2 vCenter Server

vCenter Server is the main management and administration tool for the VMware infrastructure. It can be used by lab administrators to manage the CCDC, as well as by researchers to manage their virtual lab environments. Users connect to vCenter Server using their Microsoft Active Directory (AD) credentials.

vCenter Server can be installed on a physical system or within a VM. It is typically installed within a VM in order to take advantage of VMware's HA capabilities. vCenter Server requires a database in order to store the state of each VM, host, user, etc. The database can be Microsoft SQL, Oracle or IBM DB2.[51] If no database is installed, vCenter Server will automatically install Microsoft SQL 2008 Express, which is limited to 5 vSphere servers and 50 VMs. vCenter Server can manage up to one thousand hosts and ten thousand running VMs with a full database. vCenter Server should be assigned a static IP rather than use DHCP.

Note – Optional vCenter Components

A number of components in the vCenter family can be considered optional and may be included at some future point in time in order to increase operational efficiency. These vCenter components include the following:

[51] If the database is eventually to be shared between vCenter Server and vCloud Director then it is recommended that either Microsoft SQL or Oracle be used. IBM DB2 does not seem to be supported by vCloud Director.

- vCenter Operations Manager – The vCenter Operations Manager is used to monitor the performance of critical applications and for capacity planning. It comes in four versions: Standard, Advanced, Enterprise and Enterprise Plus. Given that the CCDC is a lab environment, there is unlikely to be any critical applications and consequently no immediate requirement for vCenter Operations Manager;

- vCenter Configuration Manager – The vCenter Configuration Manager automates configuration management across both virtual and physical systems. Given that the CCDC is a lab environment there is unlikely to be many similarly configured VMs. Consequently, there is no immediate requirement for a solution that automates configuration management;

- vCenter Orchestrator – The vCenter Orchestrator enables the automation of provisioning and operational tasks across VMware. While vCenter Orchestrator provides useful functionality in terms of automating provisioning tasks, it is not immediately required in the CCDC due to the limited number of systems;

- vCenter Server Heartbeat – vCenter Server Heartbeat provides HA capabilities for vCenter. HA will not initially be provided within the CCDC;

- vCenter Infrastructure Navigator – vCenter Infrastructure Navigator allows organizations to visualize relationships and map dependencies of applications in order to better manage the virtual infrastructure. Given the limited nature of the CCDC, this component is not required initially;

- vCenter Site Recovery Manager – vCenter Site Recovery Manager is a business recovery solution that centrally manages Disaster Recovery Plans (DRP) and automates the resumption of production on an emergency site. DRP will not be implemented for the CCDC;

- vCenter Chargeback Manager – vCenter Chargeback Manager provides resource metering and service reporting in order to calculate service costs. For organizations where chargeback would not be used the alternative is showback. Showback is used to raise awareness of the consumption usage and cost without involving formal account procedures to bill the usage back to the consumer’s department. The CCDC will not be implementing a chargeback mechanism.

- vCenter Protect – vCenter Protect provides both patch management and asset inventory for Windows operating systems and applications for both virtual and physical machines. There are two versions: vCenter Protect Standard and Advanced. vCenter Protect Advanced provides additional functionality including anti-virus. Given that the CCDC will be used for research, including malware analysis, administrators will need to be careful about scanning VMs for malicious code. Consequently, vCenter Protect is not recommended initially; and

- vCenter Converter – vCenter Converter, which is a free component that is installed separately, is used to convert a physical machine into a VM. Cyber Operations may want to convert existing research and development systems into VMs during the transition from research lab silos to the CCDC.

6.2.3 vCloud Director

vCloud Director is virtualization software that provides enhanced infrastructure provisioning. It is the software layer that would allow the CCDC to transition from an interactive S&T lab into a private cloud providing collaborative IaaS services. Specifically, it could provide the following capabilities to the CCDC:

- vApp Catalogue – A vApp is a container for VMs that provides resource controls and management for the VMs contained inside. The systems comprising an entire TDP could be contained within a vApp. Not only would the vApp encapsulate the resource controls for the VMs but it would include the network configurations as well. Furthermore, the vApp would allow all of the VMs to be powered on, powered off, suspended, or shutdown with the click of a button. Perhaps most importantly, the vApp can be easily cloned for use in multiple research environments. vCloud Director provides a catalogue of vApps available to Cyber R&D staff. These vApps can be deployed as pre-configured virtual appliances containing VMs, operating system images, and other software;

- Self-Service Provisioning – Cyber R&D staff will be able to self-provision their research environments using a self-service web portal that provides direct access to vApp catalogues; and

- Multi-Tenant Isolation – CCDC administrators will be better able to isolate research activities using policy groups. This capability will even allow external entities to access the CCDC with isolated virtual resources, independent LDAP-authentication, specific policy controls, and unique vApp catalogues.

Note – It was initially envisioned that VMware Lab Manager would be used for the CCDC. However, Lab Manager discontinued as of February 2011, although it will continue to be supported through May 1st, 2013. In fact, vCloud Director is VMware's successor to Lab Manager.[52]

Note – Optional vCloud Components

A number of components in the vCloud family can be considered optional and may be included at some future point in time in order to increase operational efficiency. These vCloud components include the following:

- vCloud Networking and Security – vCloud Networking and Security decouples network and security from the underlying physical network hardware through software-defined networking and security. They are two versions; vCloud Networking and Security Standard and Advanced. The standard version provides firewall, Virtual Private Network (VPN), and Virtual eXtensible Local Area Network (VXLAN) functionality. The advanced version adds High Availability (HA), load balancing and data security functionality. vCloud Networking and Security is targeted primarily at production environments. While the basic version could possibly be used to more easily manage the isolation between research projects, there is no requirement for the advanced version;

[52] http://www.vmware.com/products/labmanager/overview.html

- vCloud Automation Center – vCloud Automation Center allows organizations to rapidly deploy and provision cloud services using a secure self-service portal. While vCloud Automation Center may eventually be required, it is envisioned that the self-service capabilities provided by vCloud Director will be more than sufficient for the CCDC;

- vCloud Integration Manager – vCloud Integration Manager automates service delivery and boosts operational efficiency for organizations interested in providing cloud services to customers. vCloud Integration Manager is not required for the CCDC unless it changes its business model and starts offering cloud services to customers; and

- vCloud Connector – vCloud Connector facilitates the management of organizations with both a private cloud infrastructure and public cloud infrastructures. vCloud Connector is not required for the CCDC as DRDC will only be operating a private cloud infrastructure.

6.2.4 VM Images

One of the advantages of a centralized lab is a repository of software images[53] that can be quickly provisioned in order to facilitate research and development activities. VM images (which can also be shared between research centres) to be included are as follows:

- Operating Systems – conventional (e.g., Microsoft Windows Desktop, Microsoft Windows Server, RHEL, CentOS, Fedora, FreeBSD, SUSE Linux, Ubuntu, Mac OS X, Solaris, etc.), penetration testing-specific (e.g., BackTrack, Backbox), and target environments specifically developed for penetration testing;

- Infrastructure Applications – e.g., Databases (Microsoft SQL Server, Oracle Database, MySQL), Web/application servers (Microsoft IIS, Apache Tomcat, IBM Websphere), Application Frameworks (Tomcat/Spring, JBoss, Cloudera/Hadoop), Business Applications (Microsoft Office, Microsoft Exchange, Microsoft SharePoint);

- Development Software – e.g., Statistical computing languages and environments (e.g., R), machine learning software (e.g., Rapid Miner, ELK), SDRP (e.g., USRP, FatBoy, LYRtech, PS3), kernel debuggers (e.g., WinDbg, Syser); code analysis tools (e.g., BinDiff, BinNavi, 010 Editor, HexDump, IDA);

- Simulation and Emulation – e.g., Network simulation (e.g., EXata), virtual channel emulators, virtual mobile devices, traffic generator software (network layer and application layer), system level design (e.g., MatLab, SystemVue), system emulators (e.g., Bochs, QEMU), automation frameworks (e.g., PowerShell), packet manipulation tools (e.g., Scapy); and

- Security Software – e.g., IDS/IPS sensors (e.g., Snort), SIEM software (e.g., HP Arcsight, Netwitness), endpoint protection software (e.g., Symantec Endpoint Protection), network protocol analyzers (e.g., Wireshark), monitoring tools (e.g., ProcMon, EtherApe),

[53] Software images is an inclusive term that encompasses VM templates (see note below), VM images, vApps, and software.

malware analysis systems (e.g., ValidEdge, FireEye), anti-virus/malware scanners, forensic/analysis tools (e.g., Volatility Framework, HBGary Responder), vulnerability scanners and penetration testing software (e.g., Nessus, Nikto, CORE Impact, SET).

Note – VM Templates

A VM template is identical in all respects to a VM except that it cannot be powered on. It is intended to serve as the image from which other VMs are made. VM templates are typically secure configurations of a particular operating system and/or applications. Consequently, anyone requiring a VM with a particular operating system and/or application merely has to clone a VM from the template rather than going through the process of creating and hardening the VM from scratch. VM templates cannot be powered on in order to prevent them from being inappropriately modified. However, VM templates need to be regularly patched in order to ensure that they maintain their secure configuration and to prevent users from inadvertently deploying unpatched systems.

6.3 Systems

This section will examine the physical systems comprising the CCDC. Specifically, it will examine the systems required for each of the following:

- Resource Groups; and
- Management Cluster.

Note – Hardware appropriate for use in the CCDC can be found in Annex D.

6.3.1 Resource Groups

As mentioned previously, physical systems are grouped into clusters in order to facilitate management. Systems can be dynamically added or removed from a cluster. Clusters are grouped into resource groups. Given the limited nature of the CCDC, it is envisioned that a single cluster and resource group will be employed in order to greatly facilitate management. Furthermore, it is assumed that this cluster/resource group will be compromised of new systems purchased for use in the CCDC. However, if existing systems are to be used and supplemented with new systems, then they should be grouped into multiple clusters based in a single resource group.

Any systems acquired for the CCDC should have the following characteristics:

- Hardware Compatibility List (HCL) – VMware maintains a compatibility list for hardware. DRDC staff should verify the compatibility of the hardware and its internal components prior to acquisition[54];

[54] The HCL can be found at http://www.vmware.com/resources/compatibility/search.php?action=base&deviceCategory=server

- Processor – VMware requires a 64-bit processor with support for LAHF and SAHF.[55] In order to optimize the price/consolidation ratio, and maximize lab space and energy efficiency, a dual processor server is recommended. Furthermore, since VMware licenses its software based on the number of processors, and vSphere can manage a core like a physical processor, it is recommended that processors with the highest number of integrated cores be used. In addition, the use of hyperthreading allows the creation of two logical core instances on a physical processor or core, so it is recommended. Lastly, Intel VT Flex Migration or AMD-V Extended Migration processors are required in order to support vMotion (see Section 6.4.4);

- Memory – VMware supports memory over commitment. Basically, it allows more memory to be allocated to the VMs running on a vSphere host than there is physical memory. It is recommended that memory over commitment be employed in order to benefit from a good level of consolidation. A basic rule of sizing is to have between 4 GB and 8 GB of Random Access Memory (RAM) per physical core; e.g., a server with 12 cores should have between 48 GB and 96 GB of RAM. For test, development, and preproduction applications the general rule is that the sum of memory configured in VMs can be double the physical RAM in the server; e.g., a server with 32 GB of RAM can have 32 VMs configured with 2 GB of memory each or 64 VMs with 1 GB each;

- Networking – Networking is discussed in Section 6.4. VMware advises using the maximum number of network cards. A basic rule is not to allow more than ten VMs per gigabit network card. In order to support the four networks, and provide redundancy, each ESXi host will require a minimum of two 10 Gb and six 1 Gb Ethernet ports[56]; and

- Storage – Storage is discussed in Section 6.5. Since all VMs will be stored centrally, very little local storage is required. In fact, local storage is simply required to host VMware vSphere.

The number of VMs that can be hosted on a single vSphere host depends on the application loads and the number of Logical CPU (LCPU) available. A LCPU corresponds to the number of logical CPUs available and configurable for VMs. As of vSphere 5, the maximum supported is 160 LCPUs per vSphere server. The LCPU is calculated by multiplying the number of physical processors by the number of cores by two if hyperthreading is enabled. Hyperthreading enables a single processor to act like two processors.

A virtual CPU (vCPU) refers to a VM's virtual processor. vCPUs run on physical CPUs, and by default VMs are allocated one vCPU each. One vCPU can typically handle a medium application load. Some applications may require additional vCPUs. A VM can be configured with up to 32 vCPUs. However, VMs should be configured with a minimum of vCPUs because some applications cannot benefit from multiple vCPUs.

[55] LAHF stands for Load AH from Flags and SAHF stands for Store AH into Flags. They are used for virtualization to store instructions for certain status flags. Most processors built since 2006, including AMD (rev E or higher) or Intel-VT, support LAHF/SAHF. A detailed discussion on LAHF and SAHF CPU instructions, for those interested, can be found at www.electricmonk.org.uk/2012/03/13/

[56] Eight Ethernet ports do not automatically translate to eight separate Ethernet cards. A number of manufacturers produce dual-port or quad-port network cards that provide two or four Gigabit Ethernet ports respectively on a single network adapter card.

E.g., 2 physical processors with 6 cores and hyperthreading = 24 LCPUs

This allows the configuration of a VM with 24 vCPUs or 24 VMs with one vCPU each or any combination in between. However, best practice dictates that it is best not to assign more than 70-80% of available vCPUs for a single VM.

Therefore, in order to determine the number of vSphere hosts required for each of CCDC's deployment phases, we must first determine the number of VMs running simultaneously. In order to do so we need to make a number of assumptions. First, we will assume that the hours worked in the CCDC occur during regular work hours (Monday to Friday, 37.5 hours per week) and that they are evenly distributed throughout the week. Second, we will make the assumption that the average Cyber R&D staff member runs five VMs simultaneously while working in the lab.[57]

Table 3 shows the results of these calculations. It should be noted that in many cases, Cyber R&D staff may not shut down their VMs after using them. This will obviously increase the number of simultaneous VMs and will need to be factored into the CCDC.

Interestingly enough, for the Unclassified Domain it works out to approximately one concurrent VM per person for each of the three phases. Similarly, for the Classified Domain it works out to approximately half a concurrent VM per person for each of the three phases. The actual number of systems required will be dependent on the specifications of the systems being acquired. Furthermore, an additional vSphere system should be acquired to handle performance spikes and to accommodate future growth of the CCDC.

Table 3 – Estimated Simultaneous VMs [58]

Phase	# of Users	Estimates					
		Unclassified Enclave			Classified Enclave		
		Total Hours	Concurrent Users	Total VMs	Total Hours	Concurrent Users	Total VMs
1 – S&T Lab	20	148	4	20	78	2	10
2 – Interactive Lab	50	370	10	50	195	5	25
3 – Collaborative Lab	100	740	20	100	390	10	50

[57] Higher TRL projects, such as the ARMOUR and SAMSON TDPs, typically require approximately ten simultaneous VMs, while other Cyber R&D staff will often work on a single VM. Consequently, an average of five simultaneous VMs is likely a good estimate.

[58] It should be noted that since these estimates are based on rough Cyber R&D staff usage estimates, they are by association only rough estimates. The CCDC must be capable of easily scaling to accommodate ever increasing usage.

6.3.2 Management Cluster

The management cluster is a separate vSphere server used to host the various management components. Table 4 list the various components running in VMs on this system and their requirements. Based on the guidelines provided in Section 6.3.1, a vSphere server with two physical processors with six cores[59] and 18 GB of RAM should suffice.

Table 4 – Management Cluster Component Requirements

	vCPU	Memory (GB)	Storage (GB)
vCenter Server	2	4	20
Database	4	16	100
Active Directory	2	4	50
vCloud Director	2	4	30
vCloud Networking & Security Manager	2	8	8
Total	**12**	**36**	**208**

6.4 Networks

This section will discuss the various networks required for the CCDC. While VLANs can be used in place of physical networks, physical networks are recommended for performance and security reasons. Likewise, while multiple networks can share the same physical switch, this approach does not provide the same level of isolation provided by physically separate switches. This section will discuss the four following networks:

- Data Network;
- Storage Network;
- Management Network; and
- vMotion Network.

[59] As per the guidance, a server with one physical processor with six cores and hyperthreading or any number of other combinations would also suffice.

Note – Normally network zones, as detailed in *ITSG-38 Network Security Zones – Design Considerations for Placement of Services within Zones* **[4]**, are used to segregate zones in a network architecture. However, in a laboratory architecture, network zones are not traditionally used as all systems are effectively running in the equivalent of an Operations Zone (OZ). A boundary controller (i.e., firewall) will be used to control access to and from the Internet.

6.4.1 Data Network

The data network is used for all network communications between VMs located on different ESXi hosts. Communications between VMs located on the same host are extremely fast because they are routed locally inside the ESXi server over the same vSwitch. This communication is referred to as virtual networking and it is discussed further in the note below. It is for this reason that VMs for a given project should all run on the same ESXi server or a limited number of ESXi servers. VM affinity links VMs so that they stay together on the same ESXi cluster in the event of disaster recovery.

Note – Virtual Networking

Virtual networking is the term given to network communications between VMs on a single system. In a traditional network infrastructure network traffic transits physical switches and hardware appliances where it is easily scrutinized for malware and intrusion detection purposes. Due to the fact that communications travelling over a virtual network are confined to a single system, network devices, and in particular security devices, typically have no visibility into this traffic.

Virtual networking can be used to either isolate groups of VMs or facilitate communications between groups of VMs. For example, all VMs that connect to the same port group belong to the same network within the CCDC even though they may reside on physically different hosts. Furthermore, Virtual Local Area Network (VLAN) support can be configured for a port group in order to allow segmentation of the network. This is one way in which to provide logically separate network environments in which to conduct research.

Another approach that could be used to provide isolation for research and development is the use of vApp networks. vApp networks are created by vCloud consumers and connect multiple VMs in a vApp together. vApp networks segment vApp VMs from the workloads in the organization virtual datacenter network. An isolated vApp network provides no connection to outside networks. Communication is restricted to the VMs in the vApp.

It is envisioned that an external Internet connection will be provided in the Unclassified Domain of the CCDC for the purpose of software downloads and updates. This will likely be provided through an existing, preconfigured vSphere port group.

6.4.2 Storage Network

The storage network is used for all iSCSI communications between the vSphere servers and the iSCSI storage array where the virtual disk files that constitute VMs are stored. The storage network is typically a physically isolated network due to the sensitivity and bandwidth requirements of the storage traffic. While CHAP and Internet Protocol Security (IPsec) can be used to secure the storage network communications, it is probably not warranted at this time due to the isolation of the lab environment.

6.4.3 Management Network

The management network is used to manage all aspects of the virtual infrastructure including the hypervisors, the VMs, the virtual network, and the virtual storage. The management network, which connects the vSphere management console to the vSphere servers, is typically a physically isolated network due to the sensitivity of the management traffic.

6.4.4 vMotion Network

As the name implies, the vMotion network is used for all vMotion communications. vMotion is used to migrate a VM from one physical server to another but without moving the files that make up the VM. It is typically used to migrate an active VM from one vSphere host server to another without any service interruption. Consequently, it can be used for planned maintenance operations, such as firmware updates, or when adding components such as memory. vMotion works best if the processors used in the two vSphere servers are of the same generation and family. vMotion requires a one gigabit network and takes advantage of Intel VT Flex Migration and AMD-V Extended Migration processors. The vMotion network is typically a physically isolated network due to the sensitivity and bandwidth requirements of the vMotion traffic.

6.5 Storage

As mentioned previously, a 1 GbE Storage Area Network (SAN) will be used for all iSCSI communications between the vSphere servers and the central iSCSI storage arrays. As with the physical systems and the network, virtualization provides a layer of abstraction that is used to hide and manage the complexity and differences between physical storage subsystems. It provides a simple model to allocate storage space of individual VMs without exposing them to the complexities of the storage technologies underneath. An acceptable product has been provided in Annex D.

All components in the SAN architecture should be made redundant. This includes network cards, physical switches, and storage array controllers. vSphere supports Multipath I/O (MPIO) that allows an automatic switch to a redundant path when the primary connection is severed. In terms of the storage array itself, many vendors support mirrored cache memory, redundant controllers, and multiple disk access paths within the array. Furthermore, some storage arrays also support de-duplication. De-duplication ensures that identical files, or blocks, are only written once. Since VMs are often created from a template there tends to be a great deal of duplication on a storage array. This is especially true for R&D environments. De-duplication should result in significant savings in terms of storage space required.

In addition, a NAS should be implemented for enterprise storage, and specifically online storage. It would provide Cyber R&D staff with a location in which to access and store data required for their research. The NAS would leverage the data network.

6.6 Management

The management of the virtual infrastructure is extremely important. If the virtual infrastructure is not effectively managed no one will use it. Similarly, if it is managed improperly the end result could be VM sprawl, which is the uncontrolled proliferation of unmanaged VMs. DRDC must find the right balance between managing the virtual infrastructure and allowing Cyber R&D staff to provision their own networks, systems and applications. Furthermore, DRDC must attempt to provide a certain level of separation of duties so that one administrator isn't responsible for the entire CCDC. In a vCloud infrastructure there are normally two types of administrators: an infrastructure administrator (vSphere/vCenter) and a cloud administrator (vCloud). The vSphere Web Client is the core administrative interface for vSphere. It connects to the vCenter Server using Hypertext Transfer Protocol Secure (HTTPS) on port 443.

6.6.1 Configuration Management

Malware and attackers typically focus on unpatched or poorly patched systems. An effective patch management strategy is one of the most effective ways to protect an IT network from external threats. vSphere Update Manager, which can be installed on the same system as vCenter Server, provides centralized and automated management of updates and patches for VMware vSphere hosts. In the past, it could also be used to patch guest operating systems and applications. This is no longer the case as guest operating systems and applications must now be managed using software delivery tools such as Microsoft's System Center Configuration Manager (SCCM) or IBM's Landesk. Another option for patching is VMware Go Pro, which also includes IT asset management and help desk. IT asset management can be used to maintain positive control over VMs and prevent the uncontrolled proliferation of VMs (VM sprawl). Help desk functionality can be used to prioritize and resolve issues by level of severity.

6.6.2 Initiating

vApp provides a means of grouping VMs into a single unit in order to facilitate resource controls and management. It allows administrators to define the boot order of the VMs in the vApp and to boot them with a single click. For example, the management cluster can be placed in a vApp and the boot order specified. With the click of a button VMware will boot the AD VM (with DNS), the vCenter database and the vCenter Server. Likewise, research VMs can be grouped into vApps.

6.6.3 Monitoring

VMs are monitored from within vCenter Server. Monitoring within a virtualized infrastructure is essential due to resource sharing amongst VMs. It is important to ensure that VMs have sufficient resources to run their applications. Consequently warnings and alarms should be configured to alert administrators prior to VMs exceeding their resource limits. For example, at 75-90% CPU usage a warning could be given, while any level above 90% would result in an alert being sent.

The VM monitoring functionality determines whether a VM is non-responsive by using a heartbeat exchange between the host server and the VMware Tools installed in the VM. This exchange takes place every thirty seconds.

6.6.4 Provisioning

vCenter includes a number of mechanisms to easily provision VM images for research and testing. Specifically, these include clones and templates. A clone is an image of an existing VM. The image can be identical, including the same network identifiers (e.g., Service Set Identifier (SSID), Media Access Control (MAC) address), or identical with regard to content but unique on the network. A template is basically an inactive VM that cannot be booted. Since it cannot be booted it cannot be modified. In order to modify it, the template would first need to be converted into a VM.

vCenter provides services to manage VM libraries and deploy them to vSphere servers. Furthermore, it provides a central point of control for managing, monitoring, provisioning and migrating VMs. vCloud takes this one step further by providing an Application Catalog containing a list of available applications and vApps.

6.7 Remote Access

While local access from within the lab will be provided, both lab users and administrators will need remote access to the Unclassified Domain. This can be accomplished in the two following ways:

- vSphere Client – vSphere Client connects to vCenter Server over port 443. Alternatively, it can connect directly to the ESXi hosts using ports 902 and 903; and

- Remote Desktop – Another possibility is to allow remote desktop access to vCenter Server.

6.8 Availability & Business Continuity

Availability is typically measured as a percentage. In addition to availability, Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are also used. RPO is the maximum amount of time that data can be lost. For example, an RPO of zero indicates that no data loss is acceptable whereas an RPO of 24 hours indicates that 24 hours' worth of data (or work) can be lost due to IT service interruptions. RTO is the maximum acceptable duration of the IT service interruption. As one would expect, the lower the RPO and RTO times, the more expensive the solution is to implement.

The availability for the CCDC was determined to be 99% based on the requirements gathering process (see Section 3.2.1). Since high-availability starts at five nines, or 99.999%, we can conclude that high-availability is not required for the CCDC. It is worth noting that the greatest periods of unavailability (79%) are due to planned maintenance. A 24 hour RPO is likely realistic, which can be addressed through the use of daily backups. A 24 RTO is desirable, which can be addressed using tapes stored at the local site.

Even though the CCDC does not require high availability, there are a number of design steps that can help to minimize disruptions. For example, it is considered best practice to make all hardware redundant. This practice eliminates Single Points of Failure (SPoF) and will greatly enhance availability.

This section will examine availability and business continuity within the CCDC. Specifically, it will examine the following aspects of availability and business continuity:

- Resource Sharing;
- Power Failure;
- Air Conditioning Failure;
- System Failure;
- Network Failure;
- Storage Failure; and
- Backup.

6.8.1 Resource Sharing

VMware provides a number of mechanisms to ensure that VMs have sufficient resources. Reservations can be used to guarantee a certain amount of resources for a VM. However, reservations are typically only used for critical applications (e.g., AD, vCenter). A better approach for most VMs is the use of shares, in which the VM is assigned a priority with respect to other VMs.

When vCloud is implemented, it is recommended that DRDC adopt a pay-as-you-go model for resource allocation. In this model, resource commitments for CPU (GHz), memory (GB), and storage (GB) are committed only when VMs or vApps are instantiated within the target organization virtual datacenter in vCloud Director. In addition, vCloud allows administrators to configure the total number of running (running VM quota) and stored (stored VM quota) VMs.

6.8.2 Power Failure

The CCDC server room includes a very large Uninterruptible Power Supply (UPS) battery backup unit that is connected to a backup diesel generator.[60] Given the current availability requirements of the CCDC, this configuration is more than sufficient.

6.8.3 Air Conditioning Failure

A Practical Designs Temperature Humidity USB (Universal Serial Bus) Monitor THUM sensor, which measures ambient temperature and humidity levels, is currently being used in the ARMOUR lab.[61] This sensor can be used to trigger alerts and even initiate the controlled shutdown of CCDC systems if temperature and humidity thresholds are breached.

6.8.4 System Failure

As was discussed previously, sufficient capacity should be included in the CCDC to allow for the majority of research activities to continue in the event that vSphere server is unavailable for a period of time. The VMs hosted on the inoperative server would simply be transferred over to the vSphere server with available capacity.

6.8.5 Network Failure

As discussed previously, all four networks (data, management, storage, live migration (vMotion)) are implemented with redundant hardware, including network paths. Consequently, the failure of any network component should not adversely affect the operation of the CCDC.

6.8.6 Storage Failure

Redundant Array of Independent/Inexpensive Disks (RAID) 1 will be used within the CCDC. RAID 1 makes a complete copy of all data within the iSCSI storage array. Consequently, if one hard drive in the array fails then a complete backup of the data is available on another hard drive within the storage system.

6.8.7 Backup

vCenter Data Recovery is vSphere 5's infrastructure backup solution. It is fully integrated into vCenter Server and allows for the hot backup of running VMs. Within the CCDC vCenter Data Recovery will be used to perform a full backup. A weekly backup will be performed onto removable media which will be stored at an alternate location within DRDC Ottawa. This backup strategy will be supplemented by discretionary VM snapshots. Cyber Operations staff will be advised to use this capability to take a snapshot of a VM when it is in a healthy state prior to making any significant modifications.

[60] *ARMOUR TD Laboratory Design*, Draft 0.1, March 2012

[61] *ARMOUR TD Laboratory Design*, Draft 0.1, March 2012

6.9 Access Control & Security

This section of the report will examine access control and security. Specifically, this section will examine the following aspects of access control and security:

- Access Control;
- Isolation/Containment;
- Endpoint Security; and
- Trusted Hardware.

6.9.1 Access Control

It is recommended that role-based access using Microsoft Active Directory groups and users be used with vCenter and vCloud. Administration can be delegated so that technical staff in the various research groups can manage access for that particular group.

6.9.2 Isolation/Containment

While physical separation and isolation are required for certain research, most notably for malware analysis, the separation provided in a virtualized infrastructure is sufficient for the vast majority of research. Virtualization effectively isolates each application so that the failure of one application does not affect any others. VMs, which are already isolated from one another when it comes to sharing server resources, can be further isolated in terms of network communications. vShield Zones provide a firewall capability at the level of vSwitches. The firewall can be used to prevent any communication or block or allow certain protocols.

6.9.3 Endpoint Security

Endpoint security, and specifically malicious code scanning, for VMs is complicated due to the uncontrolled proliferation of VMs. Invariably, these VMs are created and used without any malicious code scanning capability. Once compromised, these infected VMs can then serve as launch points with which to corrupt other VMs and potentially even the underlying virtual infrastructure. Fortunately, VMware built the VMsafe API, which allows vendors to provide endpoint security for their VMs without having to install agents in the VMs. Specifically, it allows VMs to be scanned from the outside without an agent. For example, vSphere Endpoint offloads antivirus functions to a hardened security VM.

6.9.4 Trusted Hardware

Modern processors[62] typically include trusted hardware that uses a TPM[63] to provide secure start-up and attestation. A TPM is a computer chip that can be used to securely store artifacts (e.g., platform identity keys, hash values). These artifacts can be used to authenticate the platform and attest to the integrity of the kernel.

VM supports the use of a TPM through VMkernel Protection. VMkernel Protection measures the VMkernel and a subset of the loaded modules (VMware Installation Bundles (VIBs)) and stores the measurements into Platform Configuration Register (PCR) 20 of the TPM. Each time vSphere boots any change to these VIB measurements will be detected.

Theoretically the TPM can also be virtualized so that its secure storage and cryptographic functions are available to operating systems and applications running in VMs. Some research on the use of virtual TPMs (vTPMs) includes the following:

- vTPM: Virtualizing the Trusted Platform Module [7];
- Virtualization and the Trusted Platform Module [8]; and
- Protecting the Filesystem Integrity of a Fedora 15 Virtual Machine from Offline Attacks using IMA/EVM [9].

6.10 Staffing

This section will examine staffing requirements for the CCDC. Specifically, it will examine staffing for the following aspects of the CCDC:

- Lab Implementation;
- Lab Administration; and
- Experiment Support.

6.10.1 Lab Implementation

It is anticipated that each phase of the lab implementation will necessitate a week or two of full-time effort by a suitably trained technical resource. The technical resource would implement the requisite hardware, including physical servers, storage, and networking, as well as any software required. There will also be a knowledge transfer component in which the technical resource trains the lab administrator on any new lab components.

[62] Intel’s version is called Trusted Execution Technology (TXT), while AMD has plans to extend ARM TrustZone security technology into x86-based hardware.
[63] Additional information on TPM can be found at the Trusted Computing Group (TCG) web site – http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

6.10.2 Lab Administration

A lab administrator is required to provide some assistance in terms of installing, configuring and maintaining lab hardware and software. In addition, the lab administrator may be required to maintain the main software catalogue that will be leveraged by Cyber R&D staff. It is anticipated that the demands placed upon the lab administrator are likely to increase with each phase of the implementation. While 0.25 Full-Time Equivalents (FTEs) may be required in Phase I, this will likely increase to 0.5 FTEs in Phase II, and a full FTE in Phase III. Furthermore, the lab administrator will need to be assisted by a representative at each DRDC campus participating in the CCDC.

6.10.3 Experiment Support

In addition to a lab administrator, there was also a requirement for a computer scientist/technologist to support lab experiments and field trials. It is envisioned that the experiment support required would vary considerably between research groups as some Cyber R&D staff are more technically inclined and prefer to perform this work themselves, while others would prefer to delegate this technical work in order to focus on their research activities.

7 Conclusion & Recommendations

This report provides a detailed overview of the CCDC, including formalized requirements, conceptual architecture, design considerations, logical architecture, and reference architecture. The formalized requirements are a collection of approximately 120 S&T-related CCDC requirements that were derived from questionnaires and subsequent interviews with Cyber R&D staff. These formalized requirements were used to develop first a conceptualized architecture, and then a logical architecture, for the CCDC.

The vision for the CCDC is to facilitate collaboration within the Cyber Operations and Signals Warfare Section of DRDC Ottawa, between DRDC research centres (including DRDC Valcartier and DRDC CORA), and with external partners (including academia, industry and government). This will be accomplished by providing a centralized cyber lab capability that will allow Cyber Operations staff to easily conduct, share, and demonstrate their research experiments. The CCDC architecture consists of two primary domains (the Unclassified Domain and the Classified Domain), supplemented with research enclaves containing specialized research equipment or with specific containment/isolation requirements.

The CCDC will be implemented in three phases. Phase I is concerned primarily with providing the basic infrastructure comprising the S&T Lab so that it is fully usable for approximately twenty users. Phase II will expand upon the capabilities built in Phase I by transitioning to an interactive lab complete with training/demonstration environments and usable by approximately fifty users. Phase III will transition the interactive lab to a collaborative lab in order to facilitate collaborative research with other DRDC research centres and external partners. Specifically, this phase will transition the interactive lab into a private cloud offering IaaS capabilities. It is envisioned that ultimately the collaborative labs in the various DRDC research centres would be interconnected using encrypted leased lines or VPNs, thereby allowing the research centres to collaborate on research activities and share computing resources as needed. The reference architecture details how the CCDC can be built using virtualization/cloud software from a leading vendor.

It is recommended that a phased implementation of the CCDC, as outlined in this report, be implemented. Not only will the CCDC provide a lab capability that will enable Cyber R&D staff to conduct their research both efficiently and effectively, but it will provide a means by which staff can interact and collaborate with Cyber R&D staff located at other DRDC campuses and with external partners.

References

[1] A. Joseph et al., *Experience with DETER: A Testbed for Security Research*, IEEE TridentCom, 2006.

[2] T. Faber and J. Wroclawski, *A Federated Experiment Environment for Emulab-based Testbeds*, IEEE TridentCom, 2009.

[3] M. Stevens, *An Implementation of an Optical Data Diode*, DSTO-TR-0785, May 1999.

[4] *ITSG-38 Network Security Zones – Design Considerations for Placement of Services within Zones*, CSEC, May 2009.

[5] E. Maille and R. Mennecier, *VMware vSphere 5 Building a Virtual Datacenter*, VMware Press, 2013.

[6] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, SP-800-145, NIST, September 2011.

[7] S. Berger et al., *vTPM: Virtualizing the Trusted Platform Module*, 15th USENIX Security Symposium, 2006.

[8] R. Perez, *Virtualization and the Trusted Platform Module*, Second Workshop on Advances in Trusted Computing, December 2006.

[9] P. Kruus, *Protecting the Filesystem Integrity of a Fedora 15 Virtual Machine from Offline Attacks using IMA/EVM*, Linux Security Summit, September 2011.

Annex A DRDC Ottawa Cyber Lab Questionnaire

Background

DRDC is in the process of designing and subsequently building a cyber lab in order to facilitate research and testing activities.

Objective

The purpose of the cyber lab questionnaire is to help develop a set of business requirements that can be used to develop a cyber lab logical architecture. You are being asked to think about how you would like to be able to interact with the cyber lab, and collaborate with colleagues in this environment, in order to most effectively conduct your research.

The questionnaire will be followed by an interview, which will serve to further develop and ultimately prioritize the list of requirements. Ultimately we would like to be able to understand and differentiate your cyber lab requirements for the short-term (i.e., now), medium term (i.e., next couple of years) and long term (i.e., three or more years from now).

The questionnaire will take approximately fifteen minutes to complete. It can be completed and saved as a Word file. All questionnaires should be submitted via email to Jonathan Risto no later than 3pm on Monday, December 10th. Your cooperation is greatly appreciated.

Contact Information

- Name:
- Position:
- Section/Group:
- Research Areas:
- Email:
- Telephone #:

Access

This section of the questionnaire will attempt to determine how, when and the frequency with which you might access the cyber lab.

a. Do you envision working primarily in the cyber lab itself or accessing it remotely from your desk? □ Cyber Lab □ Remotely □ Both

b. Do you envision requiring access to the cyber lab from outside of the DRDC campus? Yes

c. How many hours per week (on average) do you envision using the cyber lab (either directly or remotely)?

d. How many hours per week (on average) do you envision using the cyber lab (either directly or remotely) in approximately four years time?

e. Do you envision requiring access to the cyber lab outside of normal working hours? Yes

f. What would be the effect on your research activities if the cyber lab were to be unavailable for a relatively short period of time (i.e., hours)?

□ No negative effect
□ Little negative effect
□ Some negative effect
□ Detrimental
□ Highly detrimental

g. What would be the effect on your research activities if the cyber lab were to be unavailable for a longer period of time (i.e., days)?

□ No negative effect
□ Little negative effect
□ Some negative effect
□ Detrimental
□ Highly detrimental

h. Do you foresee needing access to a classified lab/testing space? Yes

What percentage of your work would require this?
What percentage of your work would require this in approximately four years time?

i. In terms of access requirements, is there anything that you would like to add? If so, please elaborate in the space provided below.

Collaboration

This section of the questionnaire will attempt to determine with whom and the manner in which you might use the cyber lab to collaborate.

a. Do you have a requirement to collaborate with DRDC Ottawa colleagues in the cyber lab? Yes

b. Do you have a requirement to collaborate with DRDC colleagues (e.g., Valcartier) in the cyber lab? Yes

c. Do you have a requirement to collaborate with colleagues in other Government of Canada (GC) departments and agencies (e.g., CSEC, Public Safety, RCMP) in the cyber lab? Yes

d. Do you have a requirement to collaborate with external partners (e.g., university collaborations, industry partners) in the cyber lab? Yes

e. In terms of collaboration within the cyber lab, what form of collaboration do you envision? Select all that apply.

   □ Capability demonstrations
   □ Data exchange
   □ Providing access
   □ Other Specify:

f. Do you foresee needing access/connectivity to CFWC for exercises such as CWID, JOINTEX, CAGE? Yes

g. Do you foresee requiring access to previous/current/upcoming TDP results for your work? e.g. SAMSON, JNDMS, ARMOUR, TEC3? Yes

   Specify:

h. In terms of collaboration requirements, is there anything that you would like to add? If so, please elaborate in the space provided below.

Interaction

This section of the questionnaire will attempt to determine the manner in which you might interact with the cyber lab.

a. Do you envision installing applications on existing operating systems within the cyber lab? Yes

b. Do you envision installing specific operating systems on systems within the cyber lab? Yes

c. Do you envision making physical changes to systems within the cyber lab? Yes

d. Do you envision installing network components (e.g., routers, switches, firewalls) within the cyber lab? Yes

e. In terms of lab administration, what level of support are you envisioning for the cyber lab?

   □ Limited assistance (lab administrator provides power and rack space)
   □ Some assistance (lab administrator installs/configures hardware)
   □ Full support (lab administrator installs/configures hardware and software)

f. In terms of interaction requirements, is there anything that you would like to add? If so, please elaborate in the space provided below.

Research

This section of the questionnaire will attempt to determine how you might conduct research within the cyber lab.

a. What type of experiments do you require cyber lab space for?

b. Are there any general requirements for the cyber lab that you are aware of, such as space/power requirements, physical location, partner connectivity, etc.?

c. Are there any specific hardware requirements for the cyber lab that you are aware of, such as trusted computing hardware, embedded platforms, wireless networks, mobile devices, biometrics, cryptographic devices?

For example, if you are involved in research on wireless/MANETs, what might you require from the lab to make it useful for your work? For any work on wireless networks that you might be involved in, would you require any micro-base stations for wireless devices? What interfaces would be needed to connect to the wired networks? (e.g., Bluetooth, LTE, WiMAX, etc.)

d. Are there any specific software requirements for the cyber lab that you are aware of, such as cloud computing, traffic generators, simulation software, DETER testbed, sensors?

e. What data do you envision requiring for your research? Select all that apply.

□ Internally generated
□ Client capture relay
□ Live feeds
□ PREDICT dataset
□ Other Specify:

f. Describe any CF equipment or capabilities that are (or will be) required within the cyber lab for development/enhancement.

g. When you are working on experiments within the cyber lab, would you require access to the environment after you have completed your work? Yes

How long afterwards would you estimate that you might need to go back to old data/configurations to make changes or re-run experiments?

h. Are you currently using virtualization for your work? Yes
If yes, what virtualization software are you using and how are you using it?

i. In terms of research requirements, is there anything that you would like to add? If so, please elaborate in the space provided below.

Final Thoughts

Do you have any cyber lab requirements, thoughts or concerns that you would like to discuss that you do not feel were covered elsewhere in the questionnaire? If so, please elaborate in the space provided below.

Annex B DRDC Valcartier Cyber Lab Questionnaire

Background

The Cyber Operations group within DRDC Ottawa is in the process of designing and subsequently building a cyber lab in order to facilitate research and testing activities.

Objective

The purpose of the cyber lab questionnaire is to help develop a set of business requirements that can be used to develop a cyber lab logical architecture. You are being asked to think about how you would like to be able to interact with the cyber lab, and collaborate with colleagues in this environment, in order to most effectively conduct your research.

Ultimately we would like to be able to understand and differentiate your cyber lab requirements for the short-term (i.e., now), medium term (i.e., next couple of years) and long term (i.e., three or more years from now).

The questionnaire will take approximately ten minutes to complete. It can be completed and saved as a Word file. All questionnaires should be submitted via email to Jonathan Risto no later than February 19th. Your cooperation is greatly appreciated.

Contact Information

- Name:
- Position:
- Section/Group:
- Research Areas:
- Email:
- Telephone #:

Malware Analysis

This section of the questionnaire will attempt to determine how the cyber lab can be used to facilitate malware research.

a. Simulation tools are typically required for malware research in order to provide all of the resources needed by the malware. What simulation tools do you employ for malware research?

b. Forensic/analysis tools are typically required for malware research in order to analyze the malicious code. What forensic/analysis tools do you employ for malware research?

c. Malware research typically necessitates the use of a controlled environment in which all information is recorded for later use. Describe the configuration of this controlled environment.

d. Malware research necessitates that the research environment be isolated from other network environments in order to prevent the inadvertent spread of malicious code. How is this typically accomplished?

e. Malware research necessitates the use of a library of malicious code. Where is this library stored and how is access to this library controlled?

f. Given that some malware incorporates code to detect virtualized environments, and alters its behavior accordingly, can a virtualized environment be used for malware research? Yes

If yes, can virtualized environments used for malware research be sufficiently isolated from other virtualized environments in the same computer lab or is physical isolation required? □ Yes, virtualized environments can be sufficiently isolated □ No, physical isolation is required

g. In terms of malware research requirements, is there anything that you would like to add? If so, please elaborate in the space provided below.

Penetration Testing

This section of the questionnaire will attempt to determine how the cyber lab can be used to facilitate penetration testing research.

a. What penetration tools (e.g., metasploit framework) do you employ for penetration testing research?

b. What penetration testing-specific operating system distributions (e.g., Blackbuntu) do you employ for penetration testing research?

c. Penetration testing research typically necessitates the use of a target environment in order to assess the effectiveness of the tools being developed. Describe the target environments used for penetration testing research.

d. Does penetration testing research require isolation from other research environments? Yes

   If yes, can virtualized environments provide the level of isolation required or is physical isolation a necessity? □ Yes, virtualized environments can be sufficiently isolated □ No, physical isolation is required

e. In terms of penetration testing research requirements, is there anything that you would like to add? If so, please elaborate in the space provided below.

Annex C Requirements Mapping

This section of the report takes the requirements presented in Section 2 and maps them to the logical design in Section 3. This ensures that all of the requirements collected during the questionnaire and interview process are incorporated into the logical design and ultimately the reference design. A mapping to the specific section of the logical design can be found for each requirement.

C.1 Access Requirements

Requirement #	Requirement	Applicability	Mapping
A-1	Cyber Operations staff must be able to access the CCDC from within the CCDC lab environment(s).	U/C	3.2.1
A-2	Cyber Operations staff must be able to access the CCDC remotely from their respective offices.	U	3.2.1
A-3	Cyber Operations staff must be able to access the CCDC remotely from outside the DRDC campus.	U	3.2.1 & 3.5.4
A-4	Cyber Operations staff require access to the CCDC on average 8.6 hours per week.	U/C	3.2.1
A-5	Cyber Operations staff expect to require access to the CCDC on average 11.3 hours per week in approximately four years' time.	U/C	3.2.1
A-6	Cyber Operations staff must be able to access the CCDC outside of normal working hours.	U/C	3.2.1
A-7	The CCDC should be available for use most of the time with relatively limited downtime.	U/C	3.2.1
A-8	The CCDC must support classified research and testing.	C	3.2
A-9	Cyber Operations staff require access to classified lab facilities for 22% of their work.	C	3.2.1

Requirement #	Requirement	Applicability	Mapping
A-10	Cyber Operations staff envision requiring access to classified lab facilities for 34% of their work in approximately four years' time.	C	3.2.1
A-11	The CCDC must provide a mechanism to transfer data between the unclassified and the classified lab environments.	U/C	3.5.1
A-12	The CCDC must accommodate a phased implementation consisting of the following three phases: • S&T Lab – basic S&T lab with approximately twenty users; • Interactive Lab – S&T lab with a demonstration and training environment, and in excess of fifty users; and • Collaborative Lab – S&T lab that facilitates collaboration by providing connectivity with external users.	U/C	3.2.1
A-13	The CCDC must provide Internet connectivity in order to facilitate firmware and software updates.	U	3.5.3

C.2 Collaboration Requirements

Requirement #	Requirement	Applicability	Mapping
C-1	The CCDC must facilitate collaboration with Cyber R&D staff within the same DRDC campus.	U/C	3.2.2
C-2	The CCDC must facilitate collaboration among Cyber R&D staff at different DRDC campuses.	U/C	3.2.2, 3.3 & 3.4.3
C-3	The CCDC must facilitate collaboration with DRDC CORA colleagues.	U/C	3.2.2 & 3.3

Requirement #	Requirement	Applicability	Mapping
C-4	The CCDC must facilitate collaboration with colleagues in other Government of Canada (GC) departments and agencies.	U/C	3.2.2
C-5	The CCDC must facilitate collaboration with external partners (e.g., university collaborations, industry partners).	U/C	3.2.2
C-6	The CCDC must facilitate capability demonstrations.	U/C	3.2.2 & 3.6
C-7	The CCDC must facilitate data exchange with collaborating partners.	U/C	3.2.2
C-8	The CCDC must allow partner access to projects.	U/C	3.2.2
C-9	The CCDC must facilitate training, including the provisioning and de-provisioning of systems for training.	U/C	3.7
C-10	The CCDC must provide access/connectivity to the CFWC Battle Lab for exercises such as CWID, JOINTEX and CAGE.	C	3.5.2.4
C-11	The CCDC must provide access to previous/current/upcoming TDPs (e.g., SAMSON, JNDMS, ARMOUR, TEC3).	U/C	3.2.2
C-12	The CCDC must provide connectivity to the testing Development Centre (TDC) and Classified Testing Development Center (CTDC) at Tunney's Pasture in order to facilitate project migration.	C	3.5.2.3
C-13	The CCDC must provide connectivity to the Canadian Forces National Operations Centre (CFNOC).	C	3.5.2.2
C-14	The CCDC must provide connectivity to the DREnet.	U	3.5.2.1
C-15	The CCDC must provide connectivity to the DWAN	U	3.5.2.5

C.3 Interaction Requirements

Requirement #	Requirement	Applicability	Mapping
I-1	The CCDC must allow Cyber Operations staff to install applications on existing operating systems within the CCDC.	U/C	3.2.3
I-2	The CCDC must allow Cyber Operations staff to install specific operating systems on systems within the CCDC.	U/C	3.2.3
I-3	The CCDC must allow Cyber Operations staff to make limited physical changes (e.g., memory, processors) to systems within the CCDC.	U/C	3.2.3
I-4	The CCDC must allow Cyber Operations staff to install network components (e.g., routers, switches, firewalls) within the CCDC.	U/C	3.2.3
I-5	Cyber Operations staff must have administrative access to their own lab systems.	U/C	3.2.3
I-6	The CCDC must be staffed so as to provide some assistance to DRDC researchers in terms of installing, configuring and maintaining lab hardware and software.	U/C	3.2.3

C.4 Research Requirements

C.4.1 General Requirements

Requirement #	Requirement	Applicability	Mapping
RG-1	The CCDC must facilitate Cyber Operations research to the greatest extent possible. Specifically, the CCDC must support a variety of Cyber Operations research capabilities. These capabilities, which are listed in no particular order, include the following: • Traffic and data analysis; • Testing and measurement of networks, systems, and technologies; • Red-teaming and blue-teaming experiments; • Network and host behaviour classification; • Course-of-action cost analysis experiments; • Electronic warfare / cyber convergence experiments; • Vulnerabilities of wireless interfaces and systems; • Simulation for wireless MANET security such as access control, routing security, attack detection, and traffic analysis; • Development of DSP algorithms and implementation on SDR; • Network, system and application modeling and simulation experiments; • IDS alert correlation; • Defensive posture evaluation; • Operating system vulnerability assessments; • Malware analysis;	U/C	3.2.4.1

Requirement #	Requirement	Applicability	Mapping
	• Network data recovery and analysis; • Attack detection and validation; and • Testing prototype cyber defence tools.		
RG-2	The CCDC must be partitionable into multiple independent experimental testbeds that can be used simultaneously.	U/C	3.2.4.1
RG-3	The CCDC must be capable of supporting multiple simultaneous environments including development and demonstration environments.	U/C	3.2.4.1
RG-4	The CCDC must support the archiving of completed or dormant projects for at least two years.	U/C	3.2.4.1
RG-5	The CCDC must be capable of hosting an instantiation of whatever cyber operations products are in use by the DND and/or Canadian Forces CF.	U/C	3.2.4.1
RG-6	The CCDC must support scalable hardware and software performance.	U/C	3.2.4.3 & 3.2.4.4
RG-7	The CCDC must support ease of management and require minimal administrative expertise.	U/C	3.2.3
RG-8	The CCDC must support system image archival.	U/C	3.2.4.1

C.4.2 Network Requirements

Requirement #	Requirement	Applicability	Mapping
RN-1	The CCDC must be capable of providing a reasonable facsimile of the DREnet.	U	3.2.4.2
RN-2	The CCDC must be capable of providing a reasonable facsimile of the DWAN.	U	3.2.4.2
RN-3	The CCDC must be capable of simulating wireless networks.	U/C	3.2.4.2
RN-4	The CCDC must facilitate the research and development of MANETs.	U/C	3.2.4.2
RN-5	The CCDC must support flexible and easy network configuration to allow for the isolation of research environments.	U/C	3.2.4.2
RN-6	The CCDC must provide isolated network segmentation and configuration from other staging and production environments.	U/C	3.2.4.2
RN-7	The CCDC must be capable of duplicating Canadian Forces (CF) environments (e.g., deployed networks).	U/C	3.2.4.2
RN-8	The CCDC must be capable of simulating/emulating very large networks.	U/C	3.2.4.2
RN-9	The CCDC must support integration with the EW enclave.	C	3.4.4
RN-10	The CCDC must include a DETER testbed.	U	3.4.3
RN-11	The CCDC must include a CFNOC environment for the testing and evaluation of R&D outputs.	C	3.2.4.2

C.4.3 Hardware Requirements

Requirement #	Requirement	Applicability	Mapping
RH-1	The CCDC must have cryptographic components such as KG84C, TACLANEs, etc.	C	3.4.2
RH-2	The CCDC must support removable storage units in order to support chain of custody rules required for investigations.	C	3.2.4.3
RH-3	The CCDC must facilitate the use of military tactical radios.	U/C	3.4.7
RH-4	The CCDC must provide system access in order to support research into cross-layer information exchange.	U/C	3.4.6
RH-5	The CCDC must have an extremely large storage capacity (i.e., >10TB) in order to support large datasets. Furthermore, the storage capacity must be able to be easily expanded to accommodate future requirements.	U/C	3.2.4.3
RH-6	The CCDC must support very fast access to disk in order to support large number of simultaneous disk reads.	U/C	3.2.4.3
RH-7	The CCDC must be capable of supporting port mirrors and network taps.	U/C	3.2.4.3
RH-8	The CCDC must be capable of distributing processing workload across multiple systems.	U/C	3.2.4.3
RH-9	The CCDC must be capable of supporting highly process-intensive applications.	U/C	3.2.4.3
RH-10	The CCDC must be capable of supporting Trusted Platform Modules (TPMs).	U/C	3.2.4.3
RH-11	The CCDC must be capable of supporting pico and micro base stations supporting a variety of wireless interfaces including LTE, WiMAX, Iridium, Inmarsat BGAN, Thuraya, and Bluetooth.	U/C	3.4.7
RH-12	The CCDC must be capable of supporting mobile	U/C	3.4.7

Requirement #	Requirement	Applicability	Mapping
	devices, such as smart phones and tablets, with wireless interfaces for testing.		
RH-13	The CCDC must be capable of supporting hardware-based traffic generators.	U/C	3.2.4.3
RH-14	The CCDC must be capable of supporting wireless routers.	U/C	3.4.7
RH-15	The CCDC must be capable of supporting both traditional and wireless traffic monitors.	U/C	3.4.7
RH-16	The CCDC must be capable of supporting web filtering and firewall appliances.	U/C	3.2.4.3
RH-17	CCDC personnel must be capable of dedicating specific hardware resources to experiments.	U/C	3.2.4.3

C.4.4 Software Requirements

Requirement #	Requirement	Applicability	Mapping
RS-1	The CCDC must be capable of managing version control for development projects.	U/C	3.2.4.4
RS-2	The CCDC must be capable of supporting virtual channel emulators.	U/C	3.2.4.4
RS-3	The CCDC must be capable of supporting virtual mobile devices.	U/C	3.2.4.4
RS-4	The CCDC must be capable of supporting multiple operating systems simultaneously.	U/C	3.2.4.4
RS-5	The CCDC must provide a standard library of images for vendor software and operating systems.	U/C	3.2.4.4

Requirement #	Requirement	Applicability	Mapping
RS-6	The CCDC must provide access to a variety of Operating Systems (OS) for vulnerability assessment work.	U/C	3.2.4.4
RS-7	The CCDC must support malware analysis tools.	U/C	3.2.4.4
RS-8	The CCDC must support traffic generator software (network layer and application layer).	U/C	3.2.4.4
RS-9	The CCDC must support simulation/emulation software.	U/C	3.2.4.4
RS-10	The CCDC must support network IDS/IPS sensors and Security Information/Event Management (SIEM) software.	U/C	3.2.4.4
RS-11	The CCDC must support statistical computing languages and environments.	U/C	3.2.4.4
RS-12	The CCDC must support open source machine learning software.	U/C	3.2.4.4
RS-13	The CCDC must support Software Defined Radio Platforms (SDRP)	U/C	3.2.4.4
RS-14	The CCDC must support CAD tools.	U/C	3.2.4.4
RS-15	The CCDC must be capable of supporting network protocol analyzers.	U/C	3.2.4.4
RS-16	The CCDC must be capable of supporting cloud computing software.	U/C	3.2.4.4
RS-17	The CCDC must be capable of supporting endpoint protection software including virus scanners.	U/C	3.2.4.4

C.4.5 Data Requirements

Requirement #	Requirement	Applicability	Mapping
RD-1	The CCDC must support the use of internally generated data.	U/C	3.2.4.5
RD-2	The CCDC must support the use of client capture relay data.	U/C	3.2.4.5
RD-3	The CCDC must support the use of live data feeds.	U/C	3.2.4.5
RD-4	The CCDC must support live capture of DREnet data.	U	3.2.4.5 & 3.5.2.1
RD-5	The CCDC must support live capture of DWAN data.	U	3.2.4.5 & 3.5.2.5
RD-6	The CCDC must support the use of PREDICT datasets.	U/C	3.2.4.5
RD-7	The CCDC must be capable of supporting blended datasets.	U/C	3.2.4.5
RD-8	The CCDC must have access to, and support the use of, CF data sources and joint exercise/experiment data.	U/C	3.2.4.5
RD-9	The CCDC must have access to, and support the use of, Unmanned Aerial Vehicle (UAV) or Link 16 capture data.	U/C	3.2.4.5
RD-10	The CCDC must have access to, and support the use of, military SATCOM data.	U/C	3.2.4.5
RD-11	The CCDC must support JNDMS and ARMOUR feeds.	U/C	3.2.4.5

C.5 DRDC Valcartier Requirements

C.5.1 Common Requirements

Requirement #	Requirement	Applicability	Mapping
VC-1	The CCDC must support monitoring tools to facilitate malware analysis and penetration testing research.	U	3.3.1
VC-2	The CCDC must support a variety of operating systems to facilitate malware analysis and penetration testing research.	U	3.3.1
VC-3	The CCDC must support a variety of hardware platforms, both conventional and unconventional, to facilitate malware analysis and penetration testing research.	U	3.3.1
VC-4	The CCDC must provide an appropriate level of separation for malware analysis and penetration testing research activities.	U	3.3.1
VC-5	The CCDC must facilitate collaboration between Cyber R&D staff in DRDC Ottawa and DRDC Valcartier by providing connectivity between their respective lab networks.	U	3.2.2 & 3.3
VC-6	The CCDC must provide Cyber R&D staff in DRDC Valcartier with complete control and setup of their own network.	U	3.3.1
VC-7	The CCDC must support a direct (unfiltered and anonymized) connection to the Internet in order to allow malware to call home or to download additional components.	U	3.3.1
VC-8	The CCDC must support a GPU cluster in order to facilitate password cracking research.	U	3.4.1

C.5.2 Malware Analysis Requirements

Requirement #	Requirement	Applicability	Mapping
VM-1	The CCDC must support malware analysis systems.	U	3.3.1
VM-2	The CCDC must support anti-virus/malware scanners.	U	3.3.1
VM-3	The CCDC must support emulators to facilitate malware analysis research.	U	3.3.1
VM-4	The CCDC must support kernel debuggers to facilitate malware analysis research.	U	3.3.1
VM-5	The CCDC must support code analysis tools to facilitate malware analysis research.	U	3.3.1
VM-6	The CCDC must support task automation frameworks to facilitate malware analysis research.	U	3.3.1
VM-7	The CCDC must support forensic/analysis tools to facilitate malware analysis research.	U	3.3.1
VM-8	The CCDC must provide a large body of malware with which to conduct malware analysis research.	U	3.3.1
VM-9	The CCDC must provide a repository for the safe storage and retrieval of malware.	U	3.3.1

C.5.3 Penetration Testing Requirements

Requirement #	Requirement	Applicability	Mapping
VP-1	The CCDC must support vulnerability scanners and penetration testing software to facilitate penetration testing research.	U	3.3.1
VP-2	The CCDC must support packet manipulation tools to facilitate penetration testing research.	U	3.3.1
VP-3	The CCDC must support Intrusion Detection and Prevention Systems (IDS/IPS) to facilitate penetration testing research.	U	3.3.1
VP-4	The CCDC must support penetration testing-specific operating system distributions to facilitate penetration testing research.	U	3.3.1
VP-5	The CCDC must support target environments specifically developed for penetration testing.	U	3.3.1

Annex D Suitable Hardware

This section will identify suitable hardware for use in the CCDC. Dell hardware was chosen for this purpose due to the fact that they have hardware available for purchase through the National Master Standing Offer (NMSO) and the ease with which pricing can be obtained through their website. However, this report does not endorse the purchase of Dell hardware, but merely provides it as an example of suitable hardware. Specifically, this section will examine suitable hardware for the server resources, the management cluster, and the iSCSI storage.

Note – This hardware has been recommended based on the information provided on the vendor website. Additional consultation is required with the hardware vendor prior to acquisition to ensure that the recommended hardware is the best fit for the CCDC.

D.1 Server Resources

The Dell PowerEdge R720[64] is a suitable server resource for the CCDC. First and foremost, it is listed as compatible hardware on the VMware HCL. It comes equipped with two Intel Xeon E5-2670 2.60 GHz processors with 8 cores and hyperthreading. An appropriately configured system, including the requisite number of network adapters (one dual-port 10 Gb and three dual-port 1 Gb) and 64 GB of memory, would cost approximately CDN$7335.[65] It would be capable of supporting 32 VMs with 4 GB of memory assigned to each. Local hard drive specifications, including RAID support, were minimized on this system due to the use of an iSCSI SAN for VM storage.

D.2 Management Cluster

The Dell PowerEdge R620[66] is a suitable system for the management cluster for the CCDC. First and foremost, it is listed as compatible hardware on the VMware HCL. It comes equipped with two Intel Xeon E5-2620 2.00 GHz processors with 6 cores and hyperthreading. An appropriately configured system, including the requisite number of network adapters (two dual-port 1 Gb) and 36 GB of memory, would cost approximately CDN$4005.[67] It would be capable of supporting the management VMs detailed in Table 4. Local hard drive specifications, including RAID support, were minimized on this system due to the use of an iSCSI SAN for VM storage.

[64] Additional information on this system can be found at http://premierconfigure.us.dell.com/dellstore/config.aspx?cs=RC1065473&oc=rcRC1065473-3160924

[65] Effective 29 March 2013.

[66] Additional information on this system can be found at http://premierconfigure.us.dell.com/dellstore/config.aspx?cs=RC1065473&oc=rcRC1065473-3516308&fb=1&c=ca&l=en

[67] Effective 29 March 2013.

D.3 iSCSI Storage

The Dell PowerVault MD3200i iSCSI SAN[68] is a suitable storage system for the CCDC. It is a 1 GbE iSCSI SAN with 12 bays. An appropriately configured system, with 6 4 TB hard drives,[69] would cost approximately CDN$13,665.[70]

Note – The addition of a NAS for enterprise storage, and specifically online storage, is required. However, it is believed that an existing DRDC NAS can be repurposed for this use.

[68] Additional information on this product can be found at http://premierconfigure.us.dell.com/dellstore/config.aspx?cs=RC1065476&oc=rcRC1065476-3112004

[69] It is recommended that the system be equipped with the largest hard drives (4TB) in order to maximize the total disk space available (48TB).

[70] Effective 29 March 2013.

List of symbols/abbreviations/acronyms/initialisms

AD	Active Directory
AES	Automated Experiment System
ARMOUR	Automated Computer Network Defence
BGAN	Broadband Global Area Network
C	Classified
CAD	Computer Aided Design
CAGE	Coalition Attack Guidance Experiment
CCDC	Cyber Capability Development Centre
CDS	Cross-Domain Solution
CF	Canadian Forces
CFNOC	Canadian Forces Network Operations Centre
CFWC	Canadian Forces Warfare Centre
CHAP	Challenge Handshake Authentication Protocol
CPU	Central Processing Unit
CORA	Centre for Operational Research and Analysis
CS	Computer Scientist
CSEC	Communications Security Establishment Canada
CSNI	Consolidated Secret Network Infrastructure
CTDC	Classified Testing Development Centre
CWID	Coalition Warfare Interoperability Demonstration
DCUI	Direct Console User Interface
DETER	Cyber-Defence technology Experimental Research
DFA	DETER Federation Architecture
DHCP	Dynamic Host Configuration Protocol
DND	Department of National Defence
DNS	Domain Name Service
DRDC	Defence Research & Development Canada
DREnet	Defence Research Establishment Network
DRP	Disaster Recovery Plan
DSP	Digital Signal Processing

DWAN	Defence Wide Area Network
EW	Electronic Warfare
FC	Fibre Channel
FiST	File Sanitization Tool
FOB	Forward Operating Base
FT	Fault Tolerance
HA	High Availability
HBA	Host Bus Adapter
HCL	Hardware Compatibility List
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure-as-a-Service
IC	Intelligence Community
IDA	Interactive DisAssembler
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
iSCSI	Internet Small Computer System Interface
ITSG	Information Technology Security Guideline
JNDMS	Joint Network Defence and Management System
JOINTEX	Joint Exercise
KVM	Kernel-based Virtual Machine
LAHF	Load AH from Flags
LAN	Local Area Network
LCPU	Logical Central Processing Unit
LTE	Long Term Evolution
MAC	Media Access Control
MAN	Metropolitan Area Network
MANET	Mobile Ad-hoc Network
MCCS	Mission Critical Cyber Security
MPIO	Multipath I/O
NAS	Network Attached Storage
NMSO	National Master Standing Offer

NTP	Network Time Protocol
OS	Operating System
OZ	Operations Zone
PAZ	Public Access Zone
PCR	Platform Configuration Register
PREDICT	Protected Repository for the Defence of Infrastructure against Cyber Threats
ProcMon	Process Monitor
R&D	Research & Development
RAM	Random Access Memory
RAID	Redundant Array of Inexpensive/Independent Disks
RHR	Reliable Human Review
RPO	Recovery Point Objective
RTO	Recovery Time Objective
S&T	Science & Technology
SAHF	Store AH into Flags
SAMSON	Secure Access Management for Secret Operational Networks
SAN	Storage Area Network
SCCM	System Center Configuration Manager
SDP	Secure Data Pump
SDRP	Software Defined Radio Platform
SET	Social-Engineer Toolkit
SFP	Small Form-factor Pluggable
SIEM	Security Information/Event Management
SME	Small and Medium Enterprise
SPOF	Single Point Of Failure
SSC	Shared Services Canada
SSID	Service Set Identification
TACLANE	Tactical Local Area Network Encryption
TCG	Trusted Computing Group
TD	Technology Demonstrator
TDP	Technology Demonstrator Project
TEC3	Tactical Edge Cyber Command and Control

THUM	Temperature Humidity USB Monitor
TOE	TCP/IP Offline Engine
TXT	Trusted Execution Technology
U	Unclassified
U/C	Unclassified/Classified
UAV	Unmanned Aerial Vehicle
UCDMO	Unified Cross Domain Management Office
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
USRP	Universal Software Radio Peripheral
vCPU	Virtual Central Processing Unit
VDI	Virtual Desktop Infrastructure
VIB	vSphere Installation Bundle
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMFS	Virtual Machine File System
VPN	Virtual Private Network
VSA	Vector Signal Analyzer
vTPM	Virtual Trusted Platform Module
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network

DOCUMENT CONTROL DATA

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

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

IBISKA Telecom, Inc.
130 Albert Street
Ottawa, ON
K1P 5G4

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

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC JUNE 2010

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

Cyber Capability Development Centre (CCDC) Science & Technology (S&T) Requirements, Logical Architecture & Reference Design:

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

Magar, A.

5. DATE OF PUBLICATION (Month and year of publication of document.)

July 2013

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

112

6b. NO. OF REFS (Total cited in document.)

9

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

Contract Report

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

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

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.)

05bp00

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

W7714-135711

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

DRDC Ottawa CR 2013-057

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

Unlimited

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

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

In order to support short- and long-term cyber science and technology (S&T) delivery, Defence Research and Development Canada (DRDC) requires an agile and effective infrastructure for cyber research, experimentation, testing and evaluation, demonstration, and training. This capability is referred to as the Cyber Capability Development Centre (CCDC). This report provides a detailed overview of the CCDC, including formalized requirements, conceptual architecture, design considerations, logical architecture, and reference architecture. Specifically, it proposes a phased implementation of the CCDC that culminates in a private Infrastructure-as-a-Service (IaaS) cloud that will enable DRDC research centres to collaborate on research activities and share computing resources as needed.

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

Cyber Range; Virtualization; Cloud Computing

Defence R&D Canada

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

R & D pour la défense Canada

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

DEFENCE R&D DÉFENSE

www.drdc-rddc.gc.ca