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

DEFENCE R&D DÉFENSE

Computer Network Defence Situational Awareness

Information Requirements

Julie H. Lefebvre, Marc Grégoire, Luc Beaudoin
and Michael Froh

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2005-254
December 2005

Canada

Computer Network Defence Situational Awareness

Information Requirements

Julie H. Lefebvre
DRDC Ottawa

Marc Grégoire
DRDC Ottawa

Luc Beaudoin
Bologik Inc.

Michael Froh
Ratworx Inc.

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2005-254

December 2005

Abstract

Military Forces are employing Network-Centric Operations as a force multiplier, which comes with increased vulnerability to attacks given the growing complexity of Information Technology (IT). Computer Network Defence (CND) focuses on managing the vulnerabilities and risk inherent in all computer networks. Current research in the field of CND Situational Awareness (SA) is focusing on a bottom-up approach of how to define meaning out of the abundance of sensor information.

This paper focuses on defining the information requirements for CND SA from a top-down approach by analysing the larger mission questions asked by a Network Command coupled with existing work in SA. This paper asserts that Force Commands must define their Operational Capability Requirements in terms of distributed IT Services qualified in terms of confidentiality, integrity, and availability. Likewise, CND SA must provide feedback to the Command concerning defensive posture, risk, and impact using statements of potential and real reductions in these IT Services. The analysis shows that research into CND SA lacks a clear semantics for describing network missions, and an effective tool for modelling IT Services and network resources. Once these missing pieces are defined, then the existing CND SA research on managing low-level network events becomes meaningful.

Résumé

Les forces militaires utilisent, comme multiplicateur de force, des opérations réseaucentriques qui présentent une vulnérabilité accrue aux attaques en raison de la complexité grandissante de la technologie de l'information (TI). La défense des réseaux informatiques (CND) met l'accent sur la gestion des vulnérabilités et des risques inhérents à tous les réseaux informatiques. La recherche actuelle dans le domaine de la connaissance de la situation (CS) CND porte sur une approche ascendante de la façon de trouver une signification à l'abondance des renseignements obtenus grâce aux capteurs.

Le présent document porte sur la définition des besoins en information relatifs à la CS CND à partir d'une approche descendante, par l'analyse des questions générales sur une mission posées par un commandement de réseau, conjuguée aux travaux actuels sur la connaissance de la situation (CS). Ce document fait valoir que les commandements de la force doivent définir leurs besoins en matière de capacité opérationnelle en terme de services de TI répartis, désignés par la confidentialité, l'intégrité et la disponibilité. De même, la CS CND doit procurer des renseignements au commandement de la force concernant la position défensive, le risque et les répercussions à l'aide d'énoncés des diminutions potentielles et réelles de ces services de TI. L'analyse montre que la recherche en matière de CS CND manque de termes clairs pour décrire la mission d'un réseau ainsi que d'un outil efficace pour la modélisation des services de TI et des ressources de réseau. Une fois ces pièces manquantes définies, la recherche actuelle de la CS CND sur la gestion des événements d'un réseau de niveau bas devient alors significative.

Executive summary

A revolution in military affairs is underway based on the concept of information superiority. Information, information processing, and communications networks are at the core of every military activity. Network-Centric Operations is concerned with exploiting information to maximize combat power. Information Technology (IT) provides a force multiplier but with increased vulnerability to attacks and failures given the growing complexity of IT. Within the realm of Information Operations, Computer Network Defence (CND) focuses on managing the vulnerabilities and risk inherent in all computer networks.

Current research in the field of CND Situational Awareness (SA) is focusing on a bottom-up approach of how to define meaning out of the abundance of sensor information. If one is to do "Computer Network Defence", then one arguably has to also do "Computer Networks".

Force Commands must define their Operational Capability Requirements in terms of distributed IT Services qualified in terms of confidentiality, integrity, and availability. Likewise, CND SA must provide feedback to the Force Command concerning defensive posture, risk, and impact using statements of potential and real reductions in the required IT Services.

This paper focuses on defining the information requirements for CND SA from a top-down approach. An analysis of the larger mission questions asked by a Network Command coupled with existing work in SA leads to a comprehensive definition of what information is needed. The analysis shows that several pieces of the information puzzle are missing from today's research into CND SA:

> Clear semantics are needed for describing a network's mission in terms of Operational Capability Requirements as a set of IT Services in such a way that a Force Command can clearly articulate their requirements and understand the impacts of degraded network capability on their mission. Integral to these semantics are the need to articulate the quality of the services in terms of confidentiality, integrity & availability, relative priority of services, the importance of services over time, and how service quality relates to events within the environment; and
>
> An effective tool to model the IT Services and the network resources is needed. Without such a model, it is not clear if degradations in a network resource impact any mission required IT Services.

Once these missing pieces are defined, then the existing CND SA research on managing low-level network events becomes meaningful.

Lefebvre, J.H., Grégoire, M., Beaudoin, L., and Froh, M. 2005. Computer Network Defence Situational Awareness. DRDC Ottawa TM 2005-254. Defence R&D Canada – Ottawa.

This page intentionally left blank

Sommaire

On assiste présentement à une révolution dans les affaires militaires, fondée sur le concept de la maîtrise de l'information. L'information, le traitement de l'information et les réseaux de communications sont au centre de toute activité militaire. Les opérations réseaucentriques portent sur l'utilisation de l'information dans le but de maximiser la puissance de combat. La technologie de l'information (TI) offre un multiplicateur de force qui présente une vulnérabilité accrue aux attaques et aux pannes en raison de sa complexité grandissante. Dans le domaine des opérations d'information, la défense des réseaux informatiques (CND) met l'accent sur la gestion des vulnérabilités et des risques inhérents à tous les réseaux informatiques.

La recherche actuelle dans le domaine de la connaissance de la situation (CS) CND porte sur une approche ascendante de la façon de trouver une signification à l'abondance des renseignements obtenus grâce aux capteurs. Si quelqu'un doit s'occuper de la « défense des réseaux informatiques », on peut dire qu'il doit également s'occuper des « réseaux informatiques ».

Les commandements de la force doivent définir leurs besoins en matière de capacité opérationnelle en terme de services de TI répartis, désignés par la confidentialité, l'intégrité et la disponibilité. De même, la CS CND doit procurer des renseignements au commandement de la force concernant la position défensive, le risque et les répercussions à l'aide d'énoncés des diminutions potentielles et réelles des services de TI appropriés.

Le présent document porte sur une définition des besoins en information relatifs à la CS CND, à partir d'une approche descendante. L'analyse des questions générales sur la mission posées par un commandement de réseau, conjuguée aux travaux actuels sur la connaissance de la situation (CS), mène à une définition globale de l'information requise. L'analyse montre qu'il manque plusieurs pièces au problème de l'information, à partir de la recherche d'aujourd'hui sur la CS CND :

> des termes clairs sont nécessaires pour décrire la mission d'un réseau en terme de besoins en matière de capacité opérationnelle comme un ensemble de services de TI de manière qu'un commandement de la force puisse clairement exprimer ses besoins et comprendre les répercussions d'une capacité de réseau réduite sur la mission. Il faut également que soit exprimée la qualité des services en terme de confidentialité, d'intégrité, de disponibilité, de la priorité relative des services, de l'importance des services au fil du temps et de quelle façon la qualité du service est liée aux événements;
>
> il faut un outil efficace pour modeler les services de TI et les ressources d'un réseau. Sans un tel modèle, il n'est pas clair que la diminution des ressources d'un réseau aura des incidences sur les services de TI.

Une fois ces pièces manquantes définies, la recherche actuelle de la CS CND sur la gestion des événements d’un réseau de niveau bas devient alors significative.

Lefebvre, J.H., Grégoire, M., Beaudoin, L., and Froh, M. 2005. Computer Network Defence Situational Awareness. DRDC Ottawa TM 2005-254. R & D pour la défense Canada – Ottawa.

Table of contents

List of figures

List of tables

1. Introduction

A revolution in military affairs is underway based on the concept of information superiority [1]. Information superiority is having the capability to acquire, exploit and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same [2], [3]. Information Operations (IO) aim to influence decision makers in support of national objectives and are carried out through the continuum of operations [2], [4]. IO is both offensive and defensive. Offensive IO includes approaches to influence decision makers including: psychological operations, deception, electronic warfare, intelligence, physical destruction, and computer network attack. Defensive IO is a process that integrates and coordinates policies, procedures, operations, intelligence, law, and technology to carry out Computer Network Defence (CND) [2].

CND focuses on managing the vulnerabilities and risk that are inherent in all computer networks. As modern forces become more dependent on Information Technology (IT) and networks, these IT assets become critical to supporting military operations [5], [6], [7]. The US Joint Vision 2020 defines Full Dimensional Protection as existing when the joint force can decisively achieve its mission with an acceptable degree of risk in both the physical and information domains [3]. This definition adds information as a strategic force asset to today's Force Protection focus on the physical domain.

Information, information processing, and communications networks are now at the core of every military activity. This Network-Centric Operations (NCO), or Network-Centric Warfare, is concerned with exploiting information to maximise combat power as provided by the following tenets [8]:

A robustly networked force improves information sharing;

Information sharing enhances the quality of information and shared battlefield situational awareness;

Shared battlefield situational awareness enables collaboration and self-synchronisation, and enhances sustainability and speed of command; and

These, in turn, dramatically increase mission effectiveness.

Over the last decade a significant amount of research effort has gone into NCO as evidenced by conference proceedings [9], [10], and Defense Advanced Research Projects Agency funded projects on battlefield digitization [11], [12]. Increased battlefield digitization leads to increased reliance on IT and computer networks. IT comes with a dual nature; it provides a force multiplier in NCO but its inherent vulnerability creates a growing risk to military operations given its complexity.

Situational Awareness (SA) is the underlying requirement to achieving NCO and information superiority. The bulk of the research in SA has come from studying pilot specific situations [13]. The work that has been done in CND SA has largely taken a bottom-up focus on trying to define meaning out of the abundance of data coming from Intrusion Detection Systems [14], [15], [16], [17]. A Defence Research and Development Canada workshop on CND SA took a top-down approach of articulating the questions asked by a Force command [18]; these workshop-generated Command-level questions are the starting point for this paper's top-down analysis of CND SA.

1.1 Scope

The scope of this paper is to define the information requirements for CND SA from a top-down approach using a generalized SA model.

Note that CND can include counter-Computer Network Attack (CNA) as possible courses of action (COA) against an active network attack as defined in the Computer Network Operations (CNO) part of IO [2]. However, COA is not not a focus of this paper, so counter-CNA will not be considered.

1.2 Hypothesis

Force Commands express their Operational Capability Requirements throughout their organization. A computer network provides information sharing in support of Operations. CND SA needs to provide feedback to the Command on the present and future status of these required capabilities. The semantics of this feedback must provide understandable indications of defensive posture, risk and impact to the Force Command.

This paper asserts that, in a fashion similar to abstracted layered services, Force Commands must define their Operational Capability Requirements in terms of distributed IT Services qualified in terms of confidentiality, integrity, and availability. Likewise, CND SA must provide feedback to the Force Command concerning defensive posture, risk, and impact using statements of potential and real reductions in the required IT Services.

2. Military CND Context

Traditional stovepipe networks, systems, and applications are becoming more highly integrated over common IT Infrastructure (ITI). Similarly, military are seeking the highest integration of information sharing over common networks with initiatives like NCO. For example, both pilots and weapons controllers on the ground can share target information from a smart bomb in real-time to confirm the target prior to the bomb release.

Military Commands typically deal with discrete units of resource with which they can plan their mission. For example, a tank squadron has specific attack, manoeuvrability, defensive, and degraded operation properties, which operate over a specified geographic region of the battlefield. Computer networks are also a resource in the Command's toolbox typically providing a support role to other command assets like logistic, weapon, intelligence, and communication systems. However, military Command is not well equipped to deal with computer networks as resources since they do not have adequate mental models of these resources [7]. Knight and McIntyre [5] have started this model development by providing a conceptual framework for battle in Cyberspace.

Unlike other battlefield resources, the network is unique in the sense that it is also a cyber-battlefield. Cyberspace is a battlefield where the traditional mental model of the Command is less applicable for the following reasons:

> Tempo - The pace of events in cyberspace takes place in seconds. Cyberspace is not constrained by many of the physical world restrictions on traditional battlefields like weather, the need for rest, refuelling, etc.
>
> Distance - Cyberspace distance is not measured in geographic terms, which is the military Command's most intuitive sense of the battlefield. Military Commands typically have a good sense of time and distance on a physical battlefield. In Cyberspace, distances may be measured in the number of router hops. CND safeguards, such as firewalls and encryptors, are analogous to obstacles or defences on a battlefield.
>
> Non-physical - Cyberspace players, weapons, and defences are typically software based. These can be mobile and self-modifying. Although software, at time of execution, is always mapped to some hardware element in geographic space, the correlation is getting less prevalent (for example, Java applets, viruses, mobile code, and grid computing).
>
> Non-geographic - Cyberspace does not map neatly onto a traditional battlefield map. On the Cyberspace battlefield entities are related logically and not geographically. For example, two routers can be geographically co-located but are in separate areas of Cyberspace since one is servicing a cryptographically protected network.

> Complexity - Cyberspace can be extremely complex due to the interconnectivity of systems and the fact that software itself is so complex. Military Commands already deal with very complex interrelations of battlefield entities; however, good system and cognitive models do not yet exist for Cyberspace like they do for the physical world.

CND must take a holistic approach and may include any networked enabled object. This definition is broad and not meant to place more responsibility on the Network Command, but rather all networked resources must be managed as a whole since they are all susceptible to network attacks and failures. As such, they must be considered when attempting to define CND SA. While CND SA must take into account all of the networked components, the Network Command will only have responsibility over some subset of these components. For example, several links may be outsourced to commercial organizations to supply Internet connectivity, microwave leased lines, or satellite bandwidth. In all of these cases, the Network Command must consider these components but doesn't have direct control over them.

3. Situational Awareness

An excellent review of research into SA is presented in [13]. The seminal work in defining SA is provided by Endsley, extended by McGuiness & Foy, and summarized in [13] by the following table:

Table 1. Situational Awareness Functions

SA FUNCTION	CONTENTS	PROCESSES
PERCEPTION (What are the current facts?) Provides awareness of relevant information from external sources: readouts, displays, communications, environment, and so on.	Explicit objects, events, states, values	Sensing, detection, identification
COMPREHENSION (What is actually going on?) Provides awareness of what all this means, i.e. a more abstract understanding of the situation at hand, an appropriate schema for assimilating information.	Implicit meanings, situations types	Interpretation, synthesis
PROJECTION (What is most likely to happen?) Provides awareness of how this situation may develop over time by predicting or simulating possible scenarios, including one's own actions and their dynamic effects.	Future scenarios, possible outcomes	Prediction, simulation
RESOLUTION (What exactly shall I do?) Provides awareness of the best path to follow to achieve the required outcome to the situation, drawing a single course of action from a subset of available actions.	Intention, course of action	Decision-making, planning

It is readily evident that the stages of SA closely resemble the command and control Observe-Orient-Decide-Act (OODA) decision making cycle first proposed by Boyd [19] as shown in the following table:

Table 2. Situational Awareness & OODA Comparison

SITUATIONAL AWARENESS	OODA COMMAND & CONTROL CYCLE
Perception	Observe
Comprehension	Orient
Projection	Decide
Resolution	Act

Researchers often examine two types of decision-making models: analytical and intuitive. Analytic decision-making for CND can be classified as traditional Threat and Risk Assessments (TRAs) like [20], [21], [22] which are slow, conscious, controlled, deliberate, and demanding of energy and effort. On the other hand, intuitive decision-making is a quick and relatively automated process. The reasoning done in traditional TRAs in understanding the IT system in question, possible threat paths, and relating asset value to potential impact is all needed for building CND SA; however, Martel [23] points out that TRA methods are much too cumbersome and rely too much on human experts to ever achieve real-time risk analysis in today's highly connected world.

4. CND SA Information Requirements

4.1 Top-Down Derivation from Operations

In this section, a top-down approach is used to derive CND SA information requirements. SA models ultimately have humans with a cognitive model of the situation. In the context of CND SA, these humans are the Network Command. Therefore, CND SA must provide the information to answer the fundamental questions asked by the Network Command.

The top-down approach must first examine the network's purpose, or mission. Computer networks are not usually the end purpose in and of themselves; rather, they support other organizational purposes. In the military context, the overall purpose is a task-force mission and includes many assets including personnel, material, weapon systems, etc. The network will be one of these assets and its overall function is to support other elements of the mission such as tracking target information, relaying orders, or ordering supplies.

A Force Command is given a mission and a set of resources with which to carry out the mission. The most fundamental question that a Force Command must ask is "How can I achieve my mission given my resources?" This question is continuously being considered by the Force Command prior to and during the execution of the mission. Each subsequent sub-Command is tasked with some subset of the overall mission and a subset of the resource set. Therefore, the Network Command must ask, "**How can I achieve the network mission given the network resources?**" This question leads to the following analysis based on the discussion of [18]:

> **What is the network mission?** The network mission is defined as the commitment of providing IT Services to the Force Command. Therefore, a network mission is an agreement between the Force and Network Commands that details the set of network Operational Capability Requirements. These requirements include the ability to access & process information. For example, Environment Canada has a weather portal. To access weather services, a network path to the web site must be available, the web site must be functioning, and their underlying information must be available and accurate. Operational capability requirements necessarily need to define the quality of protection (QoP) of each IT Service provided. QoP is defined in the CND context to include confidentiality, integrity, and availability/performance requirements for the information provided or processed by an IT Service.
>
> **What are the network resources?** Abstractly, networks are collections of nodes and links. Nodes can be further decomposed into entities such as hardware, software processes, local environments, etc.

What is the relationship between the network mission and the network resources? The relationship between providing IT Services using IT resources is typically a system description including the networked IT resources, or ITI. A top-down view of the ITI would show what resources support a single IT Service, while a bottom-up view would show what IT Services are supported by a single resource. Other views of the ITI might be geophysical such as showing how a data centre power outage impacts IT Services and other resources.

What is normal behaviour for my network? Networks can be hugely complex. However, there is a concept of "normal behaviour" when the network was engineered and planned. A complex network may change dynamically over time, but it always changes with some concept of expected "normal behaviour". Normal behaviour is an important concept since it provides a baseline against which other network behaviour is measured as "abnormal" or "failures". The degree to which non-normal behaviour impacts IT Service delivery is the Network Command's primary interest.

What is abnormal behaviour for my network? When a network is first designed, safeguards are included to accommodate anticipated system failures and attacks. Examples include: multiple routing paths with dynamic routing updates, or layering firewalls to provide defence in depth. Network engineering not only has to plan for IT failures, but also active attacks on the network.

What are my mission-critical network resources over time? This question assumes the network resources are a larger set than those specifically needed to fulfil the network mission at some instance in time. It is important to note that the definition of critical assets can vary as the situation develops and the network state changes. For example, a secondary router becomes critical when a primary router fails. Military planning must also consider the possibility of battlefield damage to significant parts of the network.

4.2 CND SA Model

Any CND SA model must have as its central focus the organization's operations or missions. In a military context, a Force Command will have a mission to accomplish. Part of its resources will be a network, which must provide specific IT Services to support that mission.

The following diagram shows how CND SA fits into the OODA Command and Control cycle for a computer network environment. Although the authors are aware that trying to capture CND SA in a simple diagram is problematic, the following diagram does provide some insight into CND SA information requirements. The diagram shows the logical network environment as distinct from the physical battlefield environment. The logical and physical environments each has their own OODA loop. The Force Command has an additional Decision & Act elements for combined logical and physical COA. Each element of the logical environment is described below and then relationships between elements are discussed.

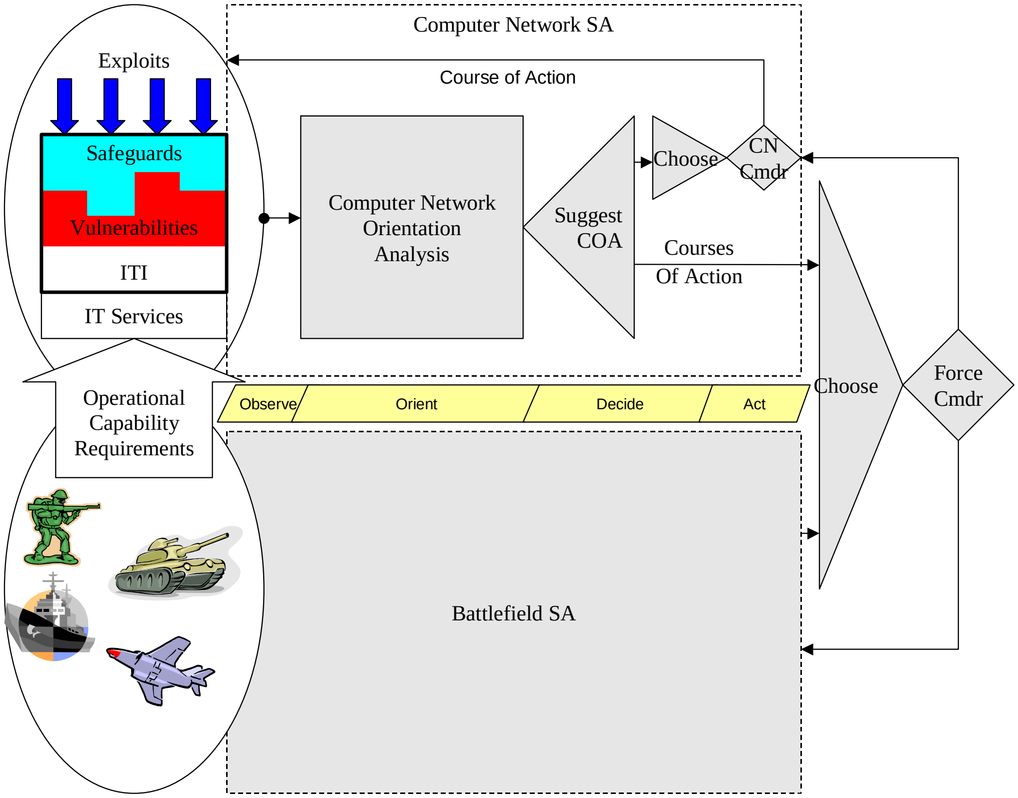


Figure 1. CND SA overlaid with OODA Cycle

In Figure 1, circles represent the physical or logical environments. **Operational Capability Requirements** show how the Force Command's plans for the physical battlefield drive the need for, and deployment of, the computer network. The network (logical) environment is divided into the following elements:

> **IT Services** collectively provide the Operational Capability Requirements. The Operational Capability Requirement does not specify how a network provides these IT Services, but rather the needed capability with its various attributes. It is also important that the Command defines the relative importance of the IT Services to each other and over time.
>
> **ITI** is the combination of all IT elements that make up the network. The ITI is not meant to show any organizational responsibility for specific IT elements (for example, a specific Intelligence database may not be under the immediate control of the Network Command). The ITI is shown in Figure 1 as the box with a heavy black border. The ITI also includes:

Vulnerabilities describe the negative CND characteristics of the ITI. Its placement is meant to show that a network has a *surface of attack*, which is made up of its inherent vulnerabilities.

Safeguards describe the positive CND characteristics of the ITI. These are the explicit security measures included in the network. Safeguard placement in the diagram is meant to show that safeguards provide protection to specific vulnerabilities and alter the inherent *surface of attack*.

Exploits describe possible and actual threat events within the network. Exploit placement in the diagram is meant to show that attackers may attempt threat events even though safeguards are in place to protect underlying vulnerabilities. The SA analyses of incident data must take into account safeguard effectiveness in countering vulnerability severity to determine impact on the IT Services.

The OODA/SA cycle is shown in Figure 1 as dotted areas. CND SA includes:

Observe. Sensor Observation within the network environment (shown as the arrow into Computer Network Orientation Analysis).

Orient. Orientation is achieved by analyzing the sensor observations to determine: defensive posture, risk, and impacts to the Operations Capability Requirements. The CND orientation analysis box is further developed in Figure 2 below.

Decide. The orientation analysis builds a cognitive model that allows a number of possible COAs to be suggested, each has a particular reduction in IT Service risk given a corresponding change to the network environment. **Courses of Action** is meant to show the Command's examination of potential courses of action. The classic SA model includes short-term prediction of the environment given specific actions.

Act. The Network and Force Commands (Cmd) choose specific actions from their list of potential COAs. Each level of Command takes actions within their realm of responsibility. The Network Command makes decisions in the network (logical) environment in order to maintain the Operational Capability Requirements. The Force Command makes decisions that coordinate actions in both the battlefield (physical) and network (logical) environments.

The relationships between the various elements of Figure 1 are examined below:

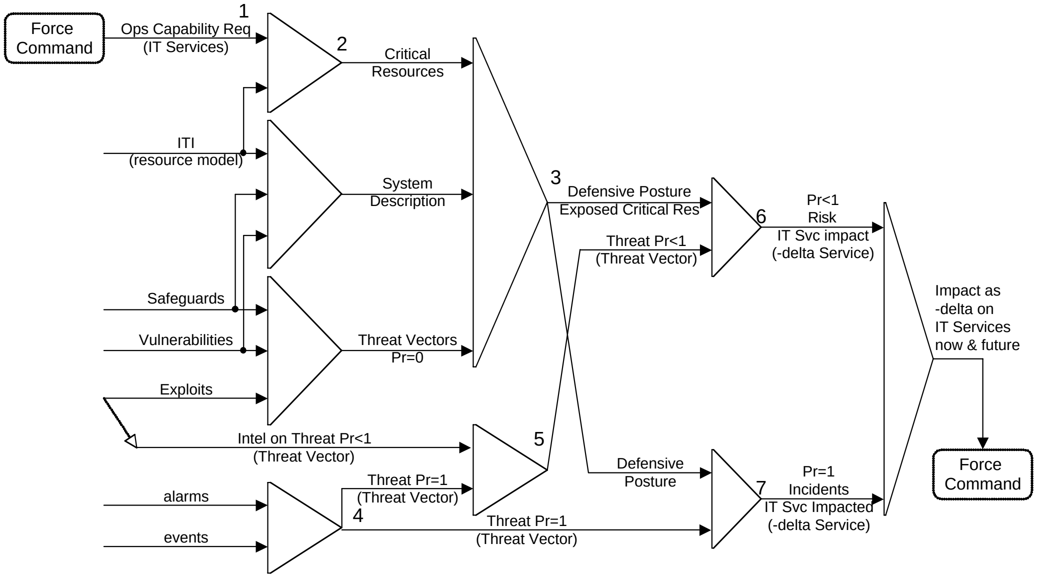
CND SA must assess impact on IT Services regardless of whether the cause is system failure or active attack.

The interface between Operations and ITI has been problematic to define since the Operations are defined as business goals (for example, provide UN Military Observers in country X to achieve Y), while the ITI is defined using information technology terms (for example, email will be provided using distributed message switches). In the future, Force Command will define network requirements as a set of IT Services (for example, messages need to be exchanged).

Safeguards decrease some vulnerability but they can also introduce other vulnerabilities particular to the safeguard (for example, smart cards reduce the vulnerability of poor password choices; however, it introduces the vulnerability of lost or damaged smart cards).

The ITI, including vulnerabilities and safeguards, is a description of the network that is time invariant relative to activity within the ITI.

The Exploits, Orientation Analysis, COA Suggestions, COA Choice, and Action phases are time variant. These describe what is happening within the network at any instance in time.



Force Command
Ops Capability Req (IT Services)
1
2
Critical Resources
ITI (resource model)
System Description
3
Defensive Posture Exposed Critical Res
Threat Pr<1 (Threat Vector)
6
Pr<1 Risk IT Svc impact (-delta Service)
Impact as -delta on IT Services now & future
Safeguards
Vulnerabilities
Threat Vectors Pr=0
Exploits
Intel on Threat Pr<1 (Threat Vector)
5
Defensive Posture
Threat Pr=1 (Threat Vector)
alarms
4
7
Pr=1 Incidents IT Svc Impacted (-delta Service)
Force Command
events
Threat Pr=1 (Threat Vector)

Figure 2. Computer Network OODA Orient Phase Information Processing

Figure 2 shows an expansion of the computer network orientation processing in Figure 1. This shows how the Force Command interfaces with the CND SA model initially by defining a set of Operational Capability Requirements in terms of IT Services, and finally by determining Operations risk based on negative deltas to those required IT Services. Note that the figure also shows a need to have environmental sensors providing coverage over known vulnerabilities, safeguards, and exploits as they apply to critical network resources. Figure 2 crystallises a number of the high-level questions raised in [18] including:

1. What is the network mission? To provide a set of IT Services which satisfies the Operational Capability Requirements.

2. What are the mission critical resources? That subset of the entire ITI which support the mission required IT Services.

3. What is my defensive posture? The set of threat vectors, which are capable of exploiting vulnerabilities in my ITI resources supporting mission critical IT Services for which there are insufficient safeguards. This may also be expressed as what are my exposed critical resources?

4. Am I under attack? The set of alarms and events that, when processed, indicate that a threat vector is realized (that is, probability = 1).

5. What is the current threat level? The combination of current threat vectors occurring in the network combined with intelligence on potential adversaries' use of threat vectors.

6. What is the level of risk to my network mission? The combination of threat level with defensive posture, which leads to the potential (that is, probability < 1) of threat vectors causing some degradation on the network ability to provide mission required IT Services.

7. What is the impact to my network mission? The combination of current threat vectors and defensive posture, which leads to actual (that is, probability = 1) degradation on the network ability to provide mission required IT Services.

4.3 IT Service Semantics

Network mission requirements are currently defined as the need to access a specific command and control network, where access implies a pre-defined suite of IT Services. Although this works today, the trend is towards greater interconnection between systems in order to increase battlefield SA. As such, merely stating network access will not suffice for tomorrow's network mission statements, and will certainly not help in providing CND SA.

The following examples from other work show various elements used to define the mission behind an IT system or communication service:

> IEEE recommended practice [24] defines a system as a collection of components organized to accomplish a specific function or set of functions. Therefore, a mission is defined as a set of functions.
>
> The NATO Technical Reference Model [25] supports the implementation of NATO Command, Control and Communication Systems. This model separates corporate data from applications and then classifies applications as either:
>
> > Mission-area or user applications (for example, personnel, material, management), and

> Support applications (that is, multimedia, communications, business processing, environment management, database utilities, and engineering support).

Internet and communications service providers typically provide a service of specific functionality (for example, a T1 link) with a specific availability defined in a Service Level Agreement (for example, the T1 link shall have a maximum Mean Time Between Failure (MTBF) of 30 days, and a maximum Mean Time To Repair (MTTR) of 5 minutes leading to a 99.99% availability rate. The service level agreement is the definition of an agreed mission between the communications service provider and the customer.

Porras *et al.* [26] define a mission specification in two parts:

> An enumeration of those data assets and services most critical to the client users of the network. Critical assets are defined as: critical computing assets, critical network services, sensitive data assets, and administrative and untrustworthy user accounts, and
>
> An identification of which classes of intrusion incidents are of greatest concern to the analyst.

Traditional TRAs [20], [21], [22] often value assets under confidentiality, integrity, and availability. There is an underlying assumption in traditional TRAs that the valuable assets (typically data and processing ability) are the reason behind having the IT system in the first place and therefore assets define the IT system mission.

All of the above examples provide elements of what is required in a comprehensive IT Service semantics. The top-down analysis of the information a Network Command needs, plus the elements of the Force Command defining Operational Capability Requirements, leads to the following set of requirements for a comprehensive IT Service semantics:

The semantics must **define a set of high-level IT Services**, which represents the Operational Capability Requirements. For example, real-time communication may be required between all units, which includes the ability to convey more information than just the written word. In this case, traditional phone services, Voice over Internet Protocol, videoconferencing, and combat net radio would all be acceptable methods of fulfilling this service. Although Interpersonal Messaging is real-time, it is still unacceptable since it lacks the implied verbal requirement.

The semantics must **define the confidentiality, integrity, and availability QoP for each IT Service**. For example, real-time communication between units must be highly confidential, of moderate integrity, and available 99.99% of the time. The majority of work in this field has been on Quality of Service (QoS), which deals with availability. Some promising work on extending commercial QoS work to a Military-QoS is shown in [27]; however, it still only covers availability.

The semantics must **define the required QoP over time**. For example, real-time communication availability between units in a garrison must be 99% available with a 15 minute MTTR pre-deployment and 99.99% available with a 3 minute MTTR during deployment. It is envisioned that not all IT Services are required 100% of the time. Distinguishing when services are needed and to what degree allows us to build an SA model that provides insight into how services should be supported over time.

The semantics must **define the confidentiality, integrity, and availability of IT Services relative to each other**. For example, a targeting system may value integrity over availability over confidentiality. As such, a Network Command may allow this system's information flows to proceed over a weak cryptographic link.

The semantics must **define an IT Service relative to other IT Services in this network mission**. For example, real-time communication between units is more important than email connectivity. Note that [27] tries to handle this type of situation where each service has its own hard QoS parameters but the network doesn't have enough capacity to handle the aggregate hard QoS requirements. It is important in these situations that appropriate degradation of services be performed according to relative priorities.

The semantics must **define an IT Service relative to other IT Services in other network missions**. For example, real-time communications between units of mission X is more important than email connectivity of mission Y. It is generally recognized that strategic IT resources will support many concurrent missions. When multiple missions are supported by the same set of IT resources, the Network Command must have some guidance on what missions' IT Services should be supported in times of degraded network capability. Note that this implies that QoP needs to be defined on an absolute scale and not just relative to a single mission. An absolute scale will allow differing missions to define their requirements as part of a collective whole.

The semantics must **define an IT Service relative to environmental events**. For example, access to port maps and harbour master notices becomes highly critical as ships are coming into port. Other examples might include the availability of air targeting services in the hours preceding Air Operations. The interesting thing to note with this requirement is that it pre-supposes SA sensors in the operating environment that will detect such events. This is relatively trivial for friendly force planned actions but significantly harder for adversary-triggered events.

The authors believe that semantics satisfying the above requirements would provide a sufficiently rich method of defining network missions. However, we acknowledge that several of these requirements are still research items, particularly confidentiality and integrity QoP. It is important to note that these semantics must fit with the requirement specified in the next section of ITI Modelling.

Note that these mission-defining semantics become the lexicon of describing risk and impact to the Force Command. That is, the language used to indicate impact and risk to the Force Command must be the same as that used by the Force Command to describe his Operational Capability Requirements. Impact is the description of actual network events that have degraded an IT Service. For example, real-time communication is currently down to Unit X and the MTTR is 30 minutes, which exceeds the stated requirement by 25 minutes. Risk is the description of probability of future mission impacting network events based on the current network state. For example, there is also a 30% chance that the MTTR will extend to three days should the adversary execute a CNA on Server X. Note that it is feasible to have an ongoing network attack, which does not impact current missions, nor represent any mission risk. In this case, the network attack is of no consequence to the Force Command since none of the network resources being used to support their mission is impacted.

4.4 IT Infrastructure Modelling

A comprehensive ITI model is the missing link in CND SA to correlate a clear definition of network mission requirements with sensor information covering vulnerabilities, safeguards, threat events, and critical resources. The ITI model must capture the interdependencies between network resources and relate how they collectively provide IT Services. An ITI model tool must satisfy the following requirements:

Able to map mission-required IT Services onto network resources.

Able to combine network resources into IT Service offerings that support a required confidentiality, integrity, and availability QoP.

Able to show physical & logical network connectivity (as possible attack ingress paths, or threat vectors) as graphs of nodes and links.

Able to describe security safeguards as attributes of network resources.

Able to describe vulnerabilities as attributes of network resources.

Able to describe network resources as interdependent elements.

Able to map threat events onto network resources with vulnerability and safeguard attributes.

Able to relate threat events to safeguard effectiveness and vulnerabilities.

Able to map sequences of threat events into threat vectors applied to the network resource connectivity.

Able to map areas of responsibility onto IT Services & network resources.

Able to generally decompose a large network into smaller networks.

Able to support geographic representations of network physical components.

Able to support layered abstraction based on services definitions in order to support coalition networks, joint task force networks, and externally provided network services such as Internet Service Providers (ISPs) and satellite providers.

4.4.1 Abstract Layer Modelling

Abstract layer modelling, like that used to model Open System Interconnection protocol layers, is required to support real-world scenarios such as coalitions, ISP connectivity, and joint task forces. Layered abstractions mean any one layer need only know about the services it offers to a higher layer (Force Command in our case), its own resources (network resources), and services provided by lower layers (satellite links, leased lines, *etc*). Figure 3 shows an example of an abstracted layered representation showing email services being provided by User Agents (UA) and Message Transfer Agents (MTA) using network services. The strategic network has a collection of switching nodes and links including an ISP provided network link. In the case of normal outages/failures, details on what has failed in a lower layer service is unimportant; we're just interested in when will it be restored. However, in the network attack scenario, we might want to know details on the outage and attack vectors from the lower layer in order to protect our network; however, this breaks the abstract layering principle of not having insight into adjoining layers.

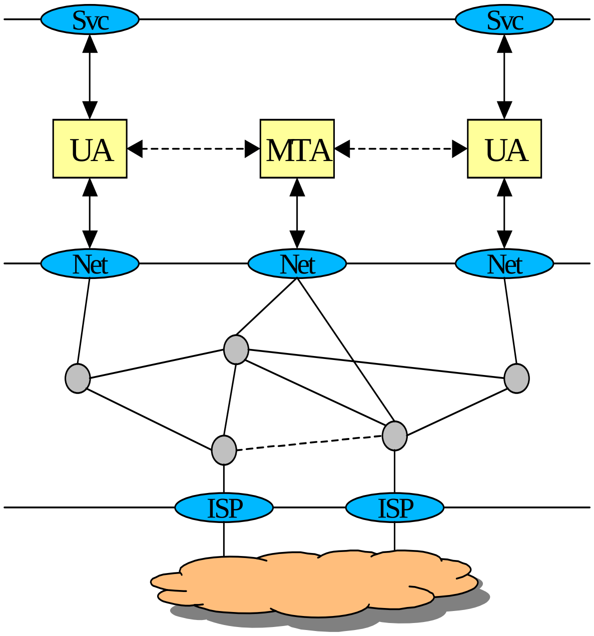


Figure 3. Abstract Layered Services

As an example exists to this last point where the Network Command may report attack details not resulting in any mission impact to the Force Command since the Network Command typically would not have any COA capability that involves physical attack on offending cyber attack threat agents, whereas the Force Command might.

5. Conclusion

Computer networks are a resource in the Force Command's toolbox that is becoming pervasive in military affairs. This heavy reliance on complex IT leads to a significant vulnerability in a Command's ability to carry out military operations. CND is a part of IO and ensures that friendly forces retain access to the information they need. This paper has examined CND SA from a top-down approach; whereas existing work in CND SA has focused on a bottom-up approach of trying to define meaning out of the abundance of sensor data.

The approach taken in this paper has been to examine the types of questions that a Force Command would like answered by CND SA, providing a framework to examine the information requirements of CND SA. This top-down analysis leads to two distinct areas requiring additional work, which are key in providing CND SA:

> Clear semantics are needed for describing Operational Capability Requirements as a set of IT Services in such a way that a Force Command can clearly articulate their requirements and understand the impacts of degraded network capability on their mission. Integral to the semantics is the need to articulate: the quality of the services in terms of confidentiality, integrity & availability; relative priority of services; the importance of services over time; and how service quality relates to events within the environment.
>
> An effective tool to model how the above mission requirements map onto the network resources is needed. Without such a model, it is not clear if degradations in a network resource impact any mission required IT Services.

Once these missing pieces are defined, then the existing CND SA research on managing low-level network events becomes meaningful since they can be related to the network mission requirements.

5.1 Future Research

The following research is needed in order to fully specify network requirements semantics:

> The semantics and syntax for describing IT Services required by the Force Command to support operations is an area for further research. It is envisioned that the semantics will include value statements for confidentiality, integrity and availability. Of these three qualities, availability seems to be understood the best.
>
> A simple mathematics for defining relative requirements is needed. These mathematics will likely be tied into the semantic values for each of the three qualities of service. The relationships between QoP values cannot be finalized until the value semantics is defined.

> When defining IT Services, some definition of a QoP that must be maintained will be defined. In our model, impact is also defined as the lack of providing an agreed set of IT Services at some defined QoP. The notion of how impact changes over time with respect to the IT Service definition is not well understood and requires further research. For example, if the email capability is specified as requiring an availability with a MTBF of 7 days and a MTTR of 4 hours, what is the impact of the following scenarios: a 3 hour outage, a 7 hour outage, or three 15 minute failures within 3 days?

A comprehensive system-modelling tool is needed which can fully integrate the mission requirement IT Service definitions. The authors note some initiatives in this area [28], [29] but have not performed an exhaustive search of system modelling methodologies. In a complex network, low-level resources such as a router will support a number of IT Services. Our model says that a resource value at any instance in time will be derived from the values assigned to the IT Services it supports. The question of how one aggregates multiple IT Service values into a specific resource value is an area for further research. It is not clear whether an absolute or relative valuation is required. It is likely that an absolute valuation is a tougher problem to solve.

6. Reference

1. C.N. Cardinal, “Delivering joint information superiority,” *Joint Force Quarterly*, Volume 23, pages 47-50, Autumn/Winter 2000. Available: http://www.dtic.mil/doctrine/jel/jfq_pubs/aw9900.htm

2. Department of National Defence (DND), *CF Information Operations*, B-GG-005-004/AF-010, National Defence, 15 Apr 1998.

3. Department of Defense (DoD), *Joint Vision 2020*, Washington, D.C., Jun 2000. Available: http://www.dtic.mil/jointvision/jv2020.doc

4. E. Waltz, *Data Fusion in Offensive and Defensive Information Operations*, Veridian Systems, Ann Arbor, MI, 1 Jan 2001.

5. LCol R. Knight, Dr. M. McIntyre, “An operational framework for battle in network space,” in *Proc of Tenth International Command and Control Research and Technology Symposium (ICCTRS)*, McLean VA, 2005, Final Paper #173. Available: http://www.dodccrp.org/events/2005/10th/CD/papers/173.pdf

6. Lt. Col. B.M. Lenfant, *Protecting Our Critical Information Technology Systems*, Naval War College, Newport, RI, 11 May 2004.

7. Lt. Cmdr. R.J. Virden, *Critical Vulnerability: Defending the Decisive Point of United States Computer Networked Information Systems*, Naval War College, Newport, RI, 3 Feb 2003.

8. J. Erbetta, “Attrition in network centric warfare,” in *Proc of RTO SAS Symposium on "Analysis of the Military Effectiveness of Future C2 Concepts and Systems"*, The Hague, 2002, RTO-MP-117, pp A4-1/8.

9. R. Suresh (editor), *Proc of SPIE Volume 3080 "Digitization of the Battlefield II"*, Orlando, 1997, ISBN 0-8194-2495-1.

10. R. Suresh (editor), *Proc of SPIE Volume 3393 "Digitization of the Battlefield III*”, Orlando, 1998, ISBN 0-8194-2842-6.

11. T.A. Crites, “Battlespace awareness overview,” in *Proc of SPIE Vol. 3080 “Digitization of the Battlespace II*”, Orlando, 1997, pp 2-5, ISBN 0-8194-2495-1.

12. Defense Advanced Research Projects Agency (DARPA) internet site http://web-ext2.darpa.mil/body/darpaoff.html

13. R. Breton, R. Rousseau, *Situation Awareness: A Review of the Concept and its Measurement*, Defence R&D Canada - Valcartier, Technical Report DRDC Valcartier TR 2001-220, Feb 2003.

14. T. Bass, “Cyberspace situational awareness demands mimic traditional command requirements,” *AFCEA Signal Magazine*, Feb 2000.

15. Electronic Warfare Associates-Canada (EWA), *Information and Functional Requirements for IDS and Network Data Fusion*, Document No. 1453-001-D001, Version 2.0 (Final), 28 Mar 2003, unpublished.

16. S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, C.S. RAghavendra, “Impact analysis of faults and attacks in large-scale networks,” *IEEE Security & Privacy*, Sep/Oct 2003.

17. S. Mathew, C. Shah, S. Upadhyaya, “An alert fusion framework for situation awareness of coordinated multistage attacks,” in *Proc of Third IEEE International Information Assurance Workshop (IWIA)*, Washington D.C., 2005, to be published.

18. Defence R&D Canada – Ottawa, *C-IA COP & JNDMS Information Requirements Workshop Results*, Ottawa, ON, 13-15 May 2003, unpublished.

19. Col. J. Boyd, *Organic Design for Command and Control*, Presentation Slides, May 1987. Available: http://www.d-n-i.net/boyd/pdf/c&c.pdf

20. C. Alberts, A. Dorofee, J. Stevens, C. Woody, *Introduction to the OCTAVE(r) Approach*, Carnegie Mellon Software Engineering Institute, Networked Systems Survivability Program, Aug 2003.

21. *Threat and Risk Assessment Working Guide*, ITSG-04, Oct 1999. Available: http://www.cse-cst.gc.ca/en/publications/gov_pubs/itsg/itsg04.html

22. C. Morton, M. Froh, “Automating the assessment of risk in IT systems,” in *Proc of the 8th Annual Canadian Computer Security Symposium*, Ottawa, 1996, pp 175-189.

23. S. Martel, *A New Model for Computer Network Security Risk Analysis*, Thesis, Carleton University, Ottawa, ON, 2002.

24. *IEEE Recommended Practice for Architectural Description for Software-Intensive Systems*, IEEE-1471-2000, 09 Oct 2000. Available: http://standards.ieee.org/reading/ieee/std_public/description/se/1471-2000_desc.html

25. *Allied Data Publication 34 (ADatP-34) - NATO C3 Technical Architecture - Volume 2 - Architectural Descriptions and Models*, Version 5.1, ISSC NATO Open Systems Working Group, 3 Mar 2004.

26. P.A. Porras, M.W. Fong, A. Valdes, “A mission-impact-based Approach to INFOSEC alarm correlation,” Lecture Notes in Computer Science in *Proc of Recent Advances in Intrusion Detection*, Zurich, 2002, pp 95-114.

27. M. Kwiatkowski, *A Concept of Defence Core Communication Infrastructure Supporting M-QoS*, Defence Science and Technology Organization, Edinburgh, Australia, DSTO-TR-1220, Oct 2001. Available: http://www.dsto.defence.gov.au/corporate/reports/DSTO-TR-1220.pdf

28. Microsoft Corporation, *Windows Server System – System Definintion Model Overview*, April 2004.

29. Y. Atamna, "NETWARS: toward the definition of a unified framework for modeling and simulation of joint communication systems," in *Proc of SPIE Vol. 3393 "Digitization of the Battlespace III"*, Orlando, 1998, pp 162-169, ISBN 0-8194-2842-6.

List of symbols/abbreviations/acronyms/initialisms

Cmd	Command
CNA	Computer Network Attack
CND	Computer Network Defence
CNO	Computer Network Operations
COA	Coarse of Action
IEEE	Institute of Electrical and Electronic Engineers
IO	Information Operations
ISP	Internet Service Provider
IT	Information Technology
ITI	IT Infrastructure
MTA	[email] Message Transfer Agent
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
NATO	North Atlantic Treaty Organization
NCO	Network-Centric Operations
OODA	Observe – Orient – Decide – Act
QoP	Quality of Protection
QoS	Quality of Service
SA	Situational Awareness
TRA	Threat and Risk Assessment

UA	[email] User Agent
UN	United Nations
US	United States

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. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

   Defence R&D Canada - Ottawa
   Ottawa ON K1A 0Z4

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

   UNCLASSIFIED

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

   Computer Network Defence Situational Awareness: Information Requirements (U)

4. AUTHORS (Last name, first name, middle initial)

   Lefebvre, J.H., Grégoire, M., Beaudoin, L., Froh, M.

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

   December 2005

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

   32

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

   29

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.)

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

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)

   15bo06

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

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

   DRDC Ottawa TM 2005-254

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

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

   (X) Unlimited distribution
   (   ) Distribution limited to defence departments and defence contractors; further distribution only as approved
   (   ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
   (   ) Distribution limited to government departments and agencies; further distribution only as approved
   (   ) Distribution limited to defence departments; further distribution only as approved
   (   ) Other (please specify):

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

   Unlimited

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

Military Forces are employing Network-Centric Operations as a force multiplier, which comes with increased vulnerability to attacks given the growing complexity of Information Technology (IT). Computer Network Defence (CND) focuses on managing the vulnerabilities and risk inherent in all computer networks. Current research in the field of CND Situational Awareness (SA) is focusing on a bottom-up approach of how to define meaning out of the abundance of sensor information.

This paper focuses on defining the information requirements for CND SA from a top-down approach by analysing the larger mission questions asked by a Network Command coupled with existing work in SA. This paper asserts that Force Commands must define their Operational Capability Requirements in terms of distributed IT Services qualified in terms of confidentiality, integrity, and availability. Likewise, CND SA must provide feedback to the Command concerning defensive posture, risk, and impact using statements of potential and real reductions in these IT Services. The analysis shows that research into CND SA lacks a clear semantics for describing network missions, and an effective tool for modelling IT Services and network resources. Once these missing pieces are defined, then the existing CND SA research on managing low-level network events becomes meaningful.

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.)

computer network defense, network situational awareness, computer security, network risk management, information warfare, network security model

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 DÉFENSE

www.drdc-rddc.gc.ca