Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

UNDERSTANDING CYBER OPERATIONS IN A CANADIAN STRATEGIC CONTEXT: MORE THAN C4ISR, MORE THAN CNO

Melanie BERNIER and Joanne TREURNIET

Defence Research and Development Canada[1], Ottawa, Canada

Abstract: In the Canadian Forces (CF), cyber operations are currently considered to be primarily computer network operations (CNO), where CNO is categorized as a subset of C4ISR, providing support to operations in the physical environments. We contend that to use these capabilities to their fullest extent, an integrated operational environment is required, and that the current CNO model, comprised of three separate activities (computer network attack, computer network defence and computer network exploitation), must be abandoned in favour of an integrated model of cyber operations. In fact, cyber operations can be any combination of these activities and more, even drawing support from operations in other environments. To justify the cyber environment as its own battle space, we analyse cyber operations in terms of the CF's six functional domains: Command; Sense; Act; Shield; Sustain; and Generate. We discuss the challenges brought about by two fundamental sources: first, the cyber environment is dynamic relative to the physical environments; second, the cyber environment is indistinct in terms of boundaries, be they physical, political, socio-economic, or otherwise. We conclude by arguing that cyber strategies should be developed by looking at the full spectrum of cyber operations rather than focussing solely on CNO to ensure that all cyber effects are considered.

Keywords: computer network operations, cyber operations, Canada, battle space

1 Defence R&D Canada [DRDC CORA SL 2009-055].

INTRODUCTION

The Department of National Defence (DND) in Canada has identified the need for capabilities and flexibility in addressing asymmetric threats such as cyber attacks in the "Canada First Defence Strategy" (DND, 2008). There is great debate at the strategic level within the Canadian Forces (CF) on how to address the development of cyber capabilities. Although the concept of cyberspace has been around for some time, it is only recently that operations in the cyber environment are becoming more of a reality/necessity. The CF have been conducting computer network defence activities for some time now; however, it is considered to be tactical and a support element to operations. But as Canada's allies are developing programs for cyber capability development, the CF's senior leadership recognizes that there is a cyber deficiency that needs to be addressed. The problem that they face is that this area is not well defined, i.e. there is no agreed upon definition of what the cyber environment is and what it consists of. Consequently they cannot have a good understanding of how it will affect our future force structure.

Currently, concept development in the cyber environment is occurring under the leadership of Command, Control, Communications and Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) oversight committee; specifically, under the Command functional domain which will be described in section 2. In the CF's C4ISR Capability Development Plan (DND, 2009a, Annex D, p.1), the definition of C4ISR is given:

> *Consists of the concepts, the connectivity, the information systems, the sensors, and the tools in support of and required to achieve effective Command, Control and awareness across the entire spectrum of CF operations through the timely attainment, generation and distribution of trusted and relevant information.*

While cyber operations clearly contribute to the C4ISR capability, we will argue in this paper that the concept is sufficiently distinct to merit its own development field. The intent of this paper is twofold: to provoke discussion by challenging how the CF currently sees cyber operations and to enable better understanding for decision-makers at the strategic level by presenting some possibilities in future cyber operations for the CF; and, to provoke discussion among NATO allies regarding the concept and definitions proposed herein. We will present cyber operations in terms of the CF's six functional domains: Command; Sense; Act; Shield; Sustain; and Generate. By analyzing cyber operations in this manner, we can demonstrate the complexity of cyber operations, which will contribute to the argument that the cyber environment should be recognized as its own battle space.

In Section 1, we will set the scene for discussion by providing definitions of the cyber environment and cyber operations for this paper[2]. In Section 2, we will discuss a strategic level view of cyber operations, as described above. Challenges to carrying out cyber operations will be highlighted in Section 3, and we will conclude in Section 4 with a proposal for the way ahead for the CF on the development of future cyber operations.

1. ELEMENTS OF CYBER OPERATIONS

The DND/CF has no approved definition of the cyber environment, or cyberspace. Under consideration is the US Department of Defence (DoD) definition of "a global domain[3] within the information environment consisting of interdependent network information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers" (DoD, 2009, p. 139). This definition, however, does not implicitly take into account the software and information that reside on the network: these are potential targets of a cyber attack and should be included in the environment. As well, the domain may not be global, as in the case of mobile ad hoc networks. We therefore propose the following definition of the cyber environment: *A domain[4] within the information environment consisting of interdependent network information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers, and the software and information that reside within them.*

In this paper we consider operations in the cyber environment as a subset of information operations (IO) and can include elements of computer network operations, physical operations (i.e. land, air, maritime, space), psychological operations (PSYOPS), electronic warfare (EW), and Signals Intelligence (SIGINT). Computer Network Operations (CNO) is defined as "actions taken to defend, exploit and/or attack information resident on Information Systems (IS) and/or the IS themselves" (DND, 2009a, p. 37); and is comprised of the combined disciplines of Computer Network Defence, Computer Network Exploitation, and Computer Network Attack, where (DND, 2009b):

- Computer Network Defence (CND) is an activity conducted through the use of

2 The definitions are meant to provoke discussion, not to establish formal Canadian definitions. They do not represent the views of the DND/CF.

3 Domain in the US definition refers to an environment, whereas in this paper domain refers to a functional domain.

4 Domain is used here to align with the US definition.

one's own computer networks to protect, monitor, detect, analyze, and respond to unauthorized activity within computers or computer networks;

- Computer Network Exploitation (CNE) is a directed, covert activity conducted through the use of computer networks to remotely enable access to, collect information from, and/or process information on computers or computer networks; and
- Computer Network Attacks (CNA) is a directed activity conducted through the use of computer networks to intentionally disrupt, deny, degrade, or destroy adversary computers, computer networks, and / or the information resident on them.

Like IO, cyber operations can be either offensive or defensive; we propose:

- Defensive cyber operations are *actions taken in the cyber environment to protect one's own information and information flow and maintain freedom of action in the cyber environment for friendly decision-makers.*
- Offensive cyber operations are *actions taken in the cyber environment to deny the actual or potential adversary's use of or access to information or information systems and affect their decision-making process.*

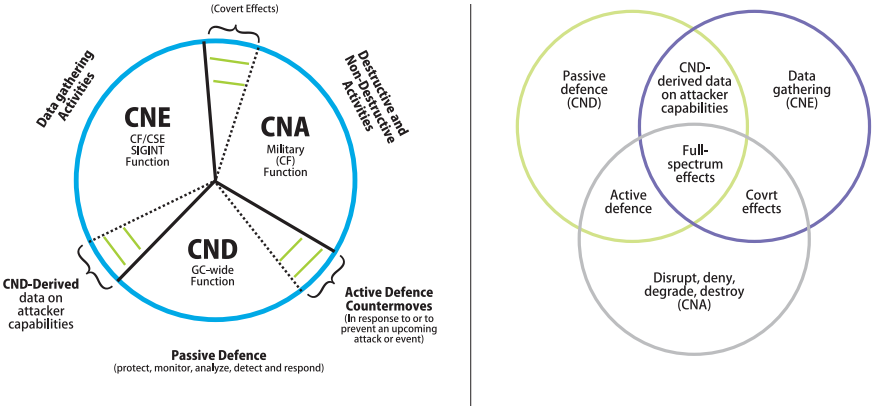

Figure 1. Current CNO model for the CF (left), and proposed model with overlap between CNO disciplines (right).

In the CF, the focus is currently on CNO because it is the main component of cyber operations and of the activities that form cyber operations, it is the least mature. Figure 1 (left) shows the current model of CNO in Canada, which was first introduced in January 2005 (Neasmith, 2005). This view can leave an impression that an operation may only be one of CNA, CNE or CND, and no overlap exists. We propose the Venn diagram shown in Figure 1 (right) because there are operations that can be simultaneously considered as CNA/CNE, CNA/CND, and CNE/CND, as well as CNE/

CNA/CND ("full-spectrum effects").

Below are examples of activities that could fall within the intersection of more than one CNO discipline (Castonguay, 2009):

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

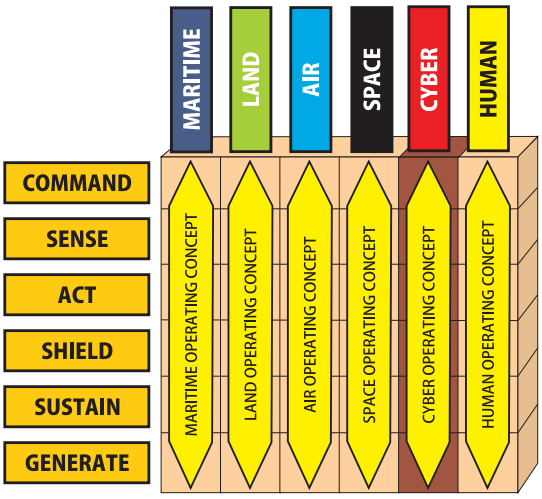

Figure 2. Capability matrix showing that capabilities can be viewed across functional domains or across environments[5].

5 This diagram is a modification of the Integrated Concepts diagram of the Integrated Capstone Concept document (DND, 2009c, p. 53).

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

2. CYBER OPERATIONS WITHIN THE DND/CF CONSTRUCT

To assist in capability development and management, the CF uses six functional domains: Command, Sense, Sustain, Act, Shield, and Generate. These domain concepts are not mutually independent, but the interdependencies have not been studied in detail and are left to future work. Capabilities can be seen either from the viewpoint of the environment, or from the viewpoint of the functional domain, as seen in Figure 2 (DND, 2009c). In section 2.1, we examine the capabilities within the cyber environment across the functional domains. In sections 2.2 and 2.3, we examine how the capabilities within the cyber environment support the other operational environments, and how capabilities in the other operational environments support cyber operations. This is not intended to be a comprehensive listing of cyber activities but suggestions leading toward discussion and dialogue.

2.1 CYBER CAPABILITIES

2.1.1 Command Domain

In capability development, Command is defined as "The human dimensions of command embedded within competency, authority, and responsibility; the creative expression of human will necessary to accomplish a mission; the establishment of common intent; and, the structures and processes necessary to manage command. As an operational function, Command sits as the nexus for the four other operational functions [Sense, Act, Shield, and Sustain. (Generate was added later)]" (CFD, 2009). By being at the nexus for all other operational functions, it ensues that the Command domain is linked to many elements of cyber operations. Cyber capabilities in the other domains are discussed in their corresponding sections to follow.

Situational awareness of the battle space enables the C2 process. In the cyber environment, understanding the battle space requires situational awareness of all networks involved in operations. These include our own networks, service provider networks, as well as enemy networks. Information acquired about these networks by using CND and CNE sensor technologies must be fused together into a Common

Operational Picture (COP) to give the commander an understanding of the cyber battle space within his operation. Knowledge of the adversary's CNO capabilities, (e.g. cyber weaknesses, and CNA capabilities) will allow for the targeting of enemy assets in the cyber battle space. Additionally, for international operations, sharing cyber information in a multi-national COP enables coordination and improved defence for all nations involved.

2.1.2 Sense Domain

The sense domain is defined as "A single comprehensive entity that collects, collates, analyses, and displays data, information, and knowledge at all levels. Tactical, operational, and strategic assets are integrated into a single continuum." (CFD, 2009) In the cyber environment, intelligence, surveillance and reconnaissance (ISR) may be obtained using CND, CNA and/or CNE activities and the dissemination of all ISR is enabled by CND.

The essential capability of the Sense domain is to provide the decision-maker with intelligence information that has been assessed and interpreted in the proper context (Fong et al, 2009). The first step is defining the information required by the decision-maker with respect to the cyber environment. The information required needs to answer questions like (note that this is not an exhaustive list):

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

The raw information pertaining to one's own network can be obtained by using a variety of tools that give a picture of the real-time structure of the network, and the activities taking place upon it, including known patterns of attack. When an attack is detected, the threat agents and their locations in the cyber environment can be marked for special attention. Open Source Intelligence (OSINT) data can be obtained from publicly available Internet sources for technical information regarding vulnerabilities.

Information about the adversary's networks and the Internet at large can be obtained using passive traffic analysis techniques and other active probing tools (CNE activities). It is important to understand the enemy's cyber vulnerabilities and the criticality of their network assets (Leblanc and Knight, 2005a). This may require penetration of the network to give visibility behind routers and firewalls. Signals Intelligence (SIGINT) data, processed from intercepted network traffic, can also give

a picture of the structure and activities of the enemy's networks. Over time, information can be collected from CND sensors that can reveal patterns in the enemy's tactics and assets. Information can be acquired about an attacker's goal, objectives and capabilities by using network counter-surveillance operations where the attacker is allowed to continue the attack in a risk-managed environment where his actions are observed (Leblanc and Knight, 2009). CNA methods can cause the enemy to react to a cyber attack, thereby revealing their capabilities in the cyber environment (Leblanc and Knight, 2005a). Human Intelligence (HUMINT) can be applied via infiltration of the Black Hat (unethical hacker) community, and OSINT via publicly-available Internet sources for both technical information and for actors.

2.1.3 Act Domain

In capability development, Act is defined as "The use of a capability to influence events across the spectrum of conflict and in either or both of the physical and moral domains. Act reflects an integration of capabilities from a variety of sources – tactical, operational, or strategic." (CFD, 2009) Assuming that the activities that can be carried out to produce effects in the cyber environment are entirely within the auspices of CNA, the activities are limited to operations that deny, degrade, disrupt or destroy the integrity, availability or accessibility of information on the enemy's systems.

Some examples of how the enemy may be engaged (in the cyber environment) to produce effects in the cyber environment are (modified from Leblanc and Knight (2005a, 2009)):

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

2.1.4 Shield Domain

The Shield functional domain is defined as "Force protection measures taken to

contribute to mission success by preserving freedom of action and operational effectiveness through managing risks and minimizing vulnerabilities to personnel, information, matériel, facilities and activities from all threats." (CFD, 2009) The primary cyber operations in the Shield domain are CND operations, and it refers only to the protection of network assets.

An effective and efficient Shield capability requires situational awareness (SA) of the cyber environment including IT infrastructure, security alerts, vulnerabilities present on the network, and what each asset on the network is being used for, all of which comes from Sense domain capabilities. Assessment of threats posed by the enemy's cyber capabilities may already be available from the processed Sense data. When threats and vulnerabilities have been assessed (i.e. processed relative to the criticality of the exposed and vulnerable devices and relative to the capabilities of the enemy) proactive remediation (e.g. application of patches) can begin as a proactive Shield capability.

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

- Physically unplugging the target device.
- Blocking related traffic using a firewall.
- Redirecting the attacker into a "honeypot" to observe their techniques and intent (Leblanc and Knight, 2005b), or conducting network counter-surveillance operations (Leblanc and Knight, 2009).
- Conducting CNA to disable the attacker.

The recovery process may require: restoring a device from a known clean backup image; decontaminating one or more hosts from a virus infection; and investigating possible changes to prevent a second occurrence of the attack.

The human aspect of defending against threats involves educating users about the role that they play in the security of the network, and the potential real effect of disregarding security procedures.

2.1.5 Sustain and Generate Domains

In capability development, Sustain is defined as: "A grouping of all functions necessary to generate, deploy, employ, and redeploy a force. As an operational function, the term is to be taken in it broadest possible context. Sustainment concerns are loosely grouped into three subordinate functions: materiel, personnel, and engineering." (CFD, 2009) In the cyber environment, Sustain is the capability to maintain the

networks, which consists of the cyber capabilities found in the Shield domain. The CF's ability to meet these demands is not a question of mandate but one of resources (Castonguay, 2009). As for all capabilities, personnel resources are key to their sustainment; however, the fast rate of change of technologies in cyber capabilities leads to difficulties in differentiating between Sustain and Generate (Castonguay, 2009; Allen, 2002).

Generate is defined as "The process by which military forces are assembled, equipped, trained, certified, and deployed to meet a force employment requirement." (CFD, 2009) In order to meet the requirements of the cyber environment it is important to hire and retain the right people with the right capabilities for the entire CNO spectrum (to conduct CNA/CNE/CND). The personnel resources required to support cyber capabilities need a high level of expertise in their field, which is not supported by the CF's career management cycle where personnel are rotated every two to four years. Therefore, by the time military personnel have gained enough expertise to be proficient in their role it is almost time for them to move on to their next post (Castonguay, 2009). As we move towards more network-enabled the need for cyber expertise will increase and due to the fast rate of change in cyber technologies, training becomes an almost constant requirement. This highlights the importance of retaining these individuals and consequently the need for revising the career management structure for the cyber-trained military personnel.

2.2 OTHER OPERATIONS SUPPORTED BY CYBER CAPABILITIES

Capabilities used in full spectrum operations conducted in the traditional environments are often supported by cyber capabilities (mostly through CND). Current and future operations in general are heavily based on information. Having the right information at the right time implies that the information required for the decision process must be available, its transmission confidential, and it must be stored in such a way as to ensure its integrity. Sharing information with a COP, whether nationally or with allies, requires secure communication and storage to ensure confidentiality, integrity and availability, which is enabled by CND capabilities.

The planning of operations is also enabled by CNA/CNE capabilities. Through CNE, intelligence information about an adversary's plans may be obtained if they are stored on a computer. Planning is enhanced with knowledge of the adversary's CNO capabilities, for example, knowledge of the enemy's cyber weaknesses, and what their CNA capabilities are, including whether they could produce effects in the physical environments. If the network could be penetrated as far as the enemy C2 systems, one could access their operational plans and commander's intent. This

knowledge could also be gained by using network counter-surveillance operations (Leblanc and Knight, 2009). Such information comes from the Sense domain and directly influences the decision cycle. The cyber environment also contributes CNA to the arsenal of weapons from which the commander can choose when forming a plan. CNA capabilities were discussed under the Act domain. The cyber environment also enables the social networking required to plan operations among individuals at different locations by providing software and mobile devices.

In the psychological space, one may influence behaviour by dispersing information via Internet radio, web sites, e-mail. One may send false information by using these same avenues. Denial of service tactics can be used to deny or disrupt information to the enemy, and one can provide alternate routes to the Internet to those for whom Internet access has been blocked. The recent incidents in Iran are an example, as well as Burma (Diebert and Rohozinski, 2009).

The availability of networks and the Internet enables many other functions required for planning operations. For example, the availability of online services and remote access to resources allows for the use of the cyber environment for recruitment, training, and procurement.

2.3 CYBER OPERATIONS SUPPORTED BY OTHER CAPABILITIES

Similar to how cyber operations can support capabilities within other environments, the reverse is also true: cyber effects can be supported or delivered by capabilities that exist within the other environments. Some examples of how the enemy may be engaged in the other environments to produce cyber effects are:

- Kinetic means: using kinetic weapons either land, air or sea base to destroy servers and/or communications link thus denying/limiting the enemy access to the cyber environment.
- Implanting cyber spyware: in order to implant hardware such as a network taps or keyboard sniffers on enemy networks, the use of Special Forces may be required to physically implant the devises.
- EW capabilities: using electronic attack techniques, such as jamming or electronic deception, to deny enemy access to wireless network devices and command and control systems or to confuse enemy ISR systems.
- PSYOPS capabilities: using social engineering techniques to encourage the enemy to disclose network information or inject malicious code, e.g. obtaining

passwords.

- C4ISR capabilities: Intelligence collected through conventional means (e.g. SIGINT, Intelligence report) can contain information about the people, e.g. those involved in a terrorist group's social networks.

3. CHALLENGES

There are two root causes of major challenges that will have to be addressed to advance cyber operations. First, the environment in which cyber operations take place is far more dynamic than the physical environments. Actions in the cyber environment can literally take place as fast as the speed of light, and technologies evolve very quickly, relatively to technologies in other environments (e.g. Moore's Law). Second, the cyber environment is indistinct in terms of boundaries, be they physical, political, socio-economic, or otherwise. Both of these characteristics lead to challenges that are more problematic in cyber operations than in other types of operations.

The production of policies and legislation is a challenge in both areas. Policymakers at all levels need to be conscious that the mechanics of cyber operations will require changes in the policy realm. This implies a commitment to provide those policymakers with the necessary education to raise awareness. Scientific support through an advisory role can enable good decision-making in both policy and cyber operations.

3.1 DYNAMIC ENVIRONMENT

The dynamic nature of the cyber environment leads to challenges in operations; for example in defensive operations software vulnerabilities are announced faster than they can be addressed. Similar examples can be found in other types of cyber operations. This can be addressed by increasing the number of personnel with specialized training, all of whom will need continuous training to keep abreast of changes in technologies (e.g. vulnerabilities) as they evolve. Continuous education and security awareness is also required for end-users; research into the human aspects of cyber security is sparse and should be augmented to yield more useable security technologies and processes.

Because of the rate of change in technology and the speed at which actions occur, the challenge lies in our capability to minimize risk and respond appropriately to an attack. For this, we will need to have a dynamic threat and risk assessment rather than the static ones used today, and dynamic situational awareness of our networks and how they are being used operationally. Research and innovation is needed to

produce technologies to automate the laborious and complex task of a complete network risk assessment that includes the operational consequences of an attack.

New infrastructures will be required that will promote the agility and flexibility of our forces, as required by the Canada First Defence Strategy (DND, 2008). Because new technologies are being developed at such a fast pace, these infrastructures must be built in such a way that their implementation can be done in the least disruptive manner possible.

The policy realm also faces challenges due to the dynamic nature of the cyber environment. Scientific and technological advances are moving faster than the accountability and responsibility control mechanisms, and faster than the ability to implement public policy and legislation.

3.2 UNDEFINED BOUNDARIES

The Internet was built to be resilient to outages. Redundant routes are introduced to ensure that there is always a path connecting any two nodes. The downside to this design is that these networks are all connected: one poorly secured network introduces a risk to all other networks. Detection of the proliferation of hostile technology, intent and behaviour is more complicated due to the extent of the cyber environment. Even when a threat is detected, preventive actions (both in the physical and cyber environments) are difficult due to legislative context, anonymity of the users, and the use of free hosting services. A central regulating agency to monitor the cyber environment, national or global, would improve threat detection. With a national regulatory agency, a nation can monitor activities within their own borders (as ill-defined as they are in the cyber environment); however, excessive regulation will likely not be possible due to the commercial aspects of the Internet. On a global scale, a central regulating agency would enable the creation and enforcement of international cyber laws. Clearly, this will present a major challenge in the global policy and legislation realm.

In the cyber environment, it is very difficult to positively attribute an activity to a person or nation, or to a physical location. If we could positively attribute an attack to a nation, this could constitute an act of war. In this case, we have to be prepared for cyberwarfare, which will require development of policies, legal frameworks and procedures with respect to these cyber capabilities. Policy for CNE/CNA activities outside of one's own network boundaries is currently undefined and is a potential barrier to CNE/CNA in cyber operations. As an example, portions of the Internet are owned and controlled by privately owned Internet Service Providers, who may object to surveillance activities being carried out via their property. In cyberwarfare, it must be recognized that actions taken will leave the boundaries of the virtual

world and have effects in physical and cognitive/human space. There needs to be an augmented Sense capability that can assess these nonphysical effects. As well, a change of mindset is required when approaching effects assessment. This requires ways of applying the same notions of detecting, identifying, classifying, etc., to nonphysical effects. Research in cyber, cognitive, and social systems may provide some insight in how to do this.

Another challenge stemming from the lack of boundaries in the cyber environment is information sharing. Departmental policy frameworks and behavioural norms lag behind the requirement to share and exploit information. The institutionalization of restrictive policies and barriers concerning information and intelligence is a result of the mindset of "need to protect" rather than the more productive "need to share". The risk is that necessary information will not get to the right people at the right time, and that they will remain information "deprived" and therefore unable to obtain situational awareness and consistently engage in effective decision-making. To mitigate the risk of leakage of sensitive information, policies and procedures must be developed to ensure that the right information is shared with the right people, on a regional, national, and global scale. Research and development could help to determine the information required for good decision-making.

Once the information sharing policies are in place, a common network and/or an effective information sharing capability is required, both within a nation and between nations. The establishment of trusted networks or enclaves with secure identity and access management will encourage users to collaborate and share information in a secure environment. Some countries, e.g. Australia, have established this national capability. In the CF, there is a need for the design and development of command and control systems that integrate cyber situational awareness with other operational awareness. These systems must be interoperable with OGDs and agencies, NGOs, and allied systems. Interoperable standards and common exchange formats to support exchange of SA information, when and if authorized, have not been agreed upon; this will take time to develop into policy. There are also legislative limits on how the CF can handle information gathered while conducting CNE types of operations, e.g. privacy rights.

4. DISCUSSION

The sections above demonstrate that cyber operations are ubiquitous. The cyber environment as a battle space will consist of joint cyber operations that touch all of the other environments (land, sea, air, space, human/cognitive) by producing effects in these environments or by acting as a supporting element in a joint campaign plan. Likewise, operations in the traditional environments can support and provide

capabilities to cyber operations.

It was previously described that CNA, CNE, and CND are closely coupled. As a result, they cannot be categorized individually into the functional domains. For example, CND does not exclusively fall under the Shield domain, CNA under the Act domain, and CNE under the Sense domain. CNO has links into each of the six functional domains. It can be both a capability and a support element. Figure 3 illustrates the relationships (as capability or support links) between CNA, CNE, CND and the six functional domains of Command, Sense, Act, Shield, Sustain, and Generate, as described in the above sections. A dashed line indicates that a CNO element is supporting a domain, and a solid line indicates that a cyber capability exists in a domain.

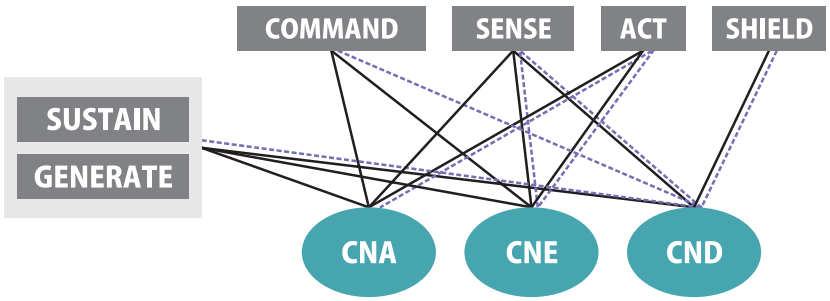

Figure 3. CNO and Functional Relations. The solid lines indicate that a cyber capability exists in a domain, and a dashed line indicates that a CNO element is supporting a domain.

The complexity of the interdependencies between cyber capabilities, the CF's functional domains, and the other traditional environments supports the position that the cyber environment should be treated as an independent battle space with its own inherent capabilities. In addition to those described in section 3, it also gives rise to challenges in operating in such an environment: doctrine and ownership issues result in duplication of effort, which ultimately costs money.

CNO capability development is currently grouped under C4ISR in the CF's C4ISR Capability Development Plan (DND, 2009a). Although the CF recognizes that CNO, and consequently cyber operations, are more than C4ISR and that these operations span a number of domains, senior leadership gave direction that CNO and cyber-related issues be brought forward though the Command domain as a primary reporting mechanism. This mechanism provided a way forward for the development of new draft polices for CF CNO (currently in review), and the initiation of a CNO strategy (in development). The same is needed for cyber operations. Considering cyber operations as CNO and having CNO as an element of C4ISR is not conducive to force development in the cyber environment. The CF needs to establish an organizational

infrastructure to address cyber-related issues and programs.

The CF is making progress towards this goal. Since this work began, it has been proposed that a cyber task force be established by summer 2010 to address cyber force development and generation, and to establish a cyber domain with inherent network exploit and network attack/effects capabilities (BGen S. Noonan, personal communication, 2 February, 2010). This is an important development because treating the cyber environment as a battle space will challenge current doctrine and will involve further concept development and experimentation. A cyber strategy and campaign plan will need to be developed, followed by concepts and doctrine for cyber operations.

As cyber attacks can target critical infrastructures and citizens, a whole-of-government approach will be needed to develop cyber policies and capabilities in a coordinated manner. There are several key players in cyber operations at the whole-of-government level, each of which has a mandated area of responsibility. The interrelationships of these mandates can be extremely complex. Consequently, depending on the type of cyber activity, the CF may or may not play a lead role. Concept and doctrine development, as well as policies, within the CF must reflect this change of mindset. Without a whole-of-government approach, the CF will not be able to effectively fulfil its mandate to defend Canada in the cyber environment.

On the research and development side of DND/CF, there are currently initiatives in developing a CNO Science and Technology (S&T) Strategy that will guide S&T efforts supporting the development and sustainment of cyber capabilities of the CF, and exploring the aforementioned cyber effects.

REFERENCES

- Allen, Maj F.J., 2002. CN(EH?) – *A Recommendation for the CF to Adopt Computer Network Exploitation and Attack Capabilities.* CSC 28 Thesis, Canadian Forces College, Toronto.
- Castonguay, LCol F., 2009. *Evaluating Canada's Cyber Semantic Gap.* JCSP 35 Master of Defence Studies Research Project, Canadian Forces College, Toronto.
- Chief of Force Development (CFD), 2009. *Capability Domains – Definitions.* Retrieved 1 May 2009, from DND intranet http://cfd.mil.ca/sites/page-eng.asp?page=4281.
- Department of National Defence, 2008. *Canada First Defence Strategy.*
- Department of National Defence, 2009a. *C4ISR Capability Development Plan.*
- Department of National Defence, 2009b. *Canadian Forces (CF) Computer Network Operations (CNO) Policy Draft Version 2.1.*
- Department of National Defence, 2009c. *Integrated Capstone Concept Draft.*
- Diebert, R., Rohozinski, R., 2009. Ottawa needs a strategy for cyberwar. *Information Warfare Monitor.* Retrieved 8 February 2010 from http://www.infowar-monitor.net/2009/06/blog-1/
- Fong, V., Cantlie, C., Farrell, P., Geling, G., Hughes, S. (2009). *Capability Domain Concept Sense Capability Domain.* Defence R&D Canada - Center for Operational Research and Analysis, DRDC-CORA-TM-2009-026.
- Leblanc, S. P., Knight, G. S., 2005a. Information Operations in Support of Special Operations. In D. Last and B. Horn (eds.), *Choice of Force - Special Operations for Canada* (pp. 173-185). Montreal: McGill-Queen's University Press.
- Leblanc, S. P., Knight, G. S., 2005b. *Engaging the Adversary as a Viable Response to Network Intrusion*, Workshop on Cyber Infrastructure – Emergency Preparedness Aspects, University of Ottawa, Ottawa.
- Leblanc, S. P., Knight, G. S., 2009, *When Not to Pull the Plug – The Need for Network Counter-Surveillance Operations.* In Czosseck, C. & Geers, K. (eds.), The Virtual Battlefield: Perspectives on Cyber Warfare (pp. 226-237), Amsterdam: IOS Press.
- Neasmith, Col. D., 2005. *CNO: Considerations for DND/CF Requirements.* Retrieved 3 February 2010, from http://www.afceaottawa.ca/uploads/CNO%20Briefing%2011Jan05.ppt
- US Department of Defense, 2009. *Joint Publication 1-02 Dictionary of Military and Associated Terms.* Retrieved 7 February 2010, from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf