CN(EH?): SHOULD THE CF ADOPT COMPUTER NETWORK EXPLOITATION AND ATTACK CAPABILITIES?

by Lieutenant-Colonel Frances Allen, CD, BSc, MDS

INTRODUCTION

> A Revolution in Military Affairs (RMA) is clearly under way, and it will have significant implications for Canadian Forces operations and activities, and on the military capabilities needed for the future.
>
> — General J.M.G. Baril[1]

The revolutionary way in which the Information Age has enveloped all aspects of life is nearly a commonly accepted phenomenon. Advances in technology have influenced the methods and speed with which the world trades, educates, and communicates. The In-ternet weaves connectivity between societies and has been likened to being "the greatest learning tool for people everywhere since the invention of the printing press."[2] It is equally used as a platform for education, propaganda, and activism. The ability to harness information and use it to advantage is seen as a key enabler to improved enlightenment, pro-ductivity and effectiveness.

The systems that focus and channel this abundance of information have quickly become staples in our lives, from automated banking machines, and computer-controlled power grids, to stock markets and networked telecommunications systems. Our reliance on these systems, however, can also be a weakness; their disruption can lead to chaos. The potential threat this disruption poses to our society is unlike any that has come before. In the past, a nation's security was based on its ability to respond to threats of force or economic coercion, usually with a conventional military force of some kind. With critical vulnerabilities now being linked to information systems and infrastructure that support heavily information-reliant economies, protection from these threats has become a serious consideration. This concern is evident in the government-led efforts that many nations are making to establish critical infrastructure protection programmes.[3]

The nearly universal influence of information and information systems can, however, be leveraged for defensive purposes. Foreign relations and politics have always relied on communications to convey political policy and intent, and on intelligence to gain an understanding of the intent of adversaries.

> Nations collect intelligence to deter or minimize the likelihood of surprise attack; to facilitate diplomatic, economic, and military action in defense of a nation in the event of hostilities; and, in times of 'neither peace not war,' to deter or defend against actions by indi-viduals, groups, or a nation that would constitute a threat to international peace and security (such as acts of terrorism).[4]

In today's information age, then, one of the best means of gaining this intelligence is by accessing the networks, information and information systems that support an adversary's planning, decision and execution cycle. This capability is called Computer Network Exploitation (CNE). Acting offensively based on this information, to neutralize an adversary's ability to use information and information systems against oneself, is known as

Computer Network Attack (CNA). This denial, destruction or disruption of an adversary's ability to adequately plan, deploy and sustain military forces could effectively complement existing conventional military capabilities, and enhance the level of defence for the nation that practises it.

The purpose of this paper is to demonstrate that the Canadian Forces should adopt CNE and CNA as military capabilities. In considering this scenario, it will be necessary to examine the issues that pertain to the development of this capability: namely, the rationale for developing the capabilities, the legal and political aspects, and the CF organization establishment considerations. As a nation with high educational and technical training standards, we should certainly consider the establishment of capabilities such as these to be within our national intellectual resources. Within the CF, however, the development of a military capability must be assessed within a defined Strategic Capability Planning model, to determine how well it meets the overall needs. Reviewing CF capability goals will allow CNE/CNA to be compared to this requirement, resulting in a mea-sure of appropriateness for the further pursuit of this capability.

The use of CNE/CNA, like any military capability, must be considered in the light of existing international law and political sensitivities. The function of CNE is truly an intelligence gathering capability, and thus its employment will need to be set in the context of Canada's traditional intelligence capabilities. Nations implicitly tolerate intelligence gathering, within the restrictions of sovereignty and prohibitions against threats of force. An examination of international law, as it pertains to the management of conflict and the use of force, will be instrumental in assessing how the use of CNE and CNA will be considered within the international community.

Next, this paper will propose a model for the development of CNE/CNA capabilities: the Special Operations Forces (SOF) development model. In this chapter the nature of special operations will be discussed and parallels drawn between traditional SOF missions, such as those assigned to Canada's JTF2, and CNE/CNA operations. Once it is established that CNE/CNA should be treated as a SOF mission, the specialized training requirements for CNE/CNA will be discussed, and the importance of implementing a well-defined training programme for these special activities will be presented. This will be followed by an analysis of the SOF command and control requirements and the current JTF2 command and control structure. Based on these best practices, a proposal for the implementation of a new SOF capability, including CNE/CNA, will be presented, identifying the importance of high-level control, and the necessary coordination with existing mili-tary operation command and control structures.

Finally, these issues will be brought together to conclude that the development of CNE/CNA as a military capability is an important and legally and politically acceptable activity that should be approached as a SOF mission. The training and organizational structure necessary to implement this capabil-ity must clearly reflect this SOF consideration. The paper's recommendations can serve as a starting point from which the planning, training, mission development and execution of CNE and CNA can commence.

RATIONALE FOR DEVELOPING CNE/CNA CAPABILITIES

CNE/CNA are capabilities that together have the flexibility to provide non-lethal and lethal effects, are relatively inexpensive, and are extremely adaptable. However, while

it is simple to assert that it would be worthwhile to develop them within the CF, in practical terms all military capabilities are in competition for the ever-shrinking defence dollar. Thus, before deciding to develop any military capability, the CF must determine how well that capability meets military requirements. Consequently, the CNE/CNA capabilities must be examined within the larger context of military requirements. This chapter will examine the roles of CNE and CNA within the broader Information Operations strategy and consider our increasing de-pendence on information systems. With this understanding, an overview will be conduct-ed of how the CF currently determines its ca-pability requirements. Knowing the capabil-ities that the CF needs, we should use this baseline to assess the effects that the CNE/ CNA capabilities can provide.

CNE/CNA and Information Operations

Computer Network Attack (CNA) is a specific offensive military capability that is part of a larger military strategy known as Information Operations (IO). Within the CF, information operations are defined as "actions taken in support of national objectives which influence decision-makers by affecting others' information while exploiting and protecting one's own information."[5] The activities that support IO occur across the spectrum of conflict, from peacetime through to war, and are defensive or offensive in nature.

Defensive IO activities are categorized as those actions that protect one's own information and ensure that friendly forces have timely access to the information they need to make relevant and accurate decisions.[6] In broad terms, this includes implementing the processes and procedures necessary for computer network defence (CND), ensuring cryptographic, transmission and emission se-curity, exercising operations security techni-ques, and supporting these activities with good public affairs and civil affairs campaigns.[7]

Offensive IO activities are mounted to actively influence real or potential adversarial decision-makers. It includes the elements of psychological operations, deception, electronic warfare, operations security, physical destruction and CNA.[8] Public affairs and civil affairs are supporting capabilities because public and Non-Governmental Organizations' (NGOs') support for, and their understanding of, military operations and objectives are critical in modern society. While there are many differing technical definitions of CNA, this paper adopts that put forth in United States Joint Doctrine: "operations to disrupt, deny, degrade or destroy information resident in computers, or the computers and networks themselves."[9] Within this definition, the following effects are possible through the use of CNA:

- The destruction of data in an adversary's information systems
- The deceiving of an adversary through the manipulation of his information system
- Denying an adversary the use of his information systems

The methods by which these effects can be produced are numerous, but reflect actions that might exploit different aspects of the targeted system. In the book, *The Law of Information Conflict: National Security Law in Cyberspace*, author Thomas Wingfield represents these aspects in a graphical representation, which is reproduced in a slightly modified manner in Figure 2.1 below.[10]

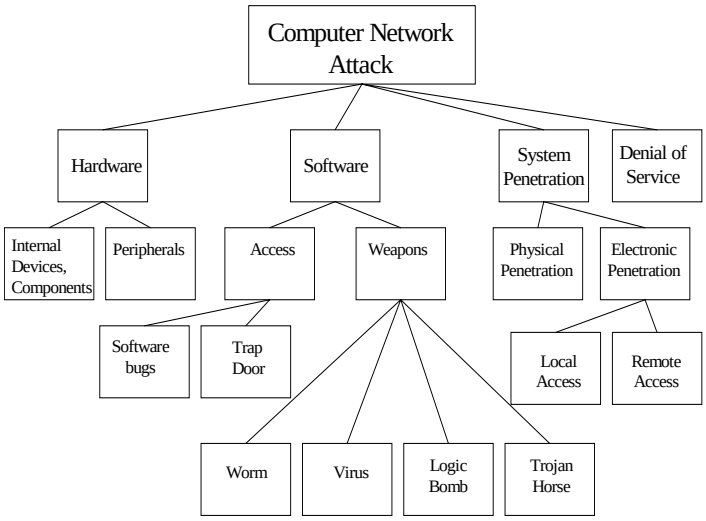


Figure 2.1 — CNA Methods

It is important to realize that defensive and offensive IO activities are complimentary functions, and that when engaging in offensive IO activities, one must also take defensive IO measures. For example, if one's offensive objective is to deceive an adversary by manipulating data in his information system, it is essential that the operation be conducted in a manner that maximizes operational security, a defensive IO capability. The ability to conduct such a mission requires adequate preparation through the collection and analysis of relevant intelligence information.

This intelligence can be acquired in whole or in part through the reconnaissance and surveillance of targeted information systems, or computer network exploitation (CNE). The difference between CNE and CNA can be very slight; the surveillance that is part of CNE can turn into CNA with the few keystrokes needed to plant a destructive command or program. Examples of the objectives of CNE include:

- The collection of government or military information from an adversary's information systems; and
- The analysis of how an adversary uses his information systems, from which operating procedures and dependencies can be deduced.

The information needed for CNA can be gathered from a variety of sources, includ-ing open source intelligence, network mapping and probing, network infiltration and data capture, or through other more tradition-al intelligence sources such as human and signals intelligence. The fusion of this intel-ligence information will provide a picture of the target information system that includes as a minimum the architecture, the operating systems and applications, security measures and processes, system management functions, the types of information available, and the external systems that rely on or contribute to the information databases. Using this infor-mation, we can initiate CNA activities to disrupt the adversaries' information systems, de-ny them their use, or deceive and confuse them through manipulation or destruction of their own information. The offensive poten-tial of CNE and CNA is also clearly reflected in the Canadian Government's concern and action to protect Canada from cybernetic threats through the creation

of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

Formed on 5 February 2001, to "develop and implement a comprehensive approach to protecting Canada's critical infrastructure,"[11] OCIPEP has identified six sectors of national critical infrastructure:

- Energy and Utilities
- Communications
- Services (such as financial services, food distribution and health care)
- Transportation
- Safety (such as nuclear safety, search and rescue, emergency services)
- Government

The concern for Canada's critical infrastructure is over both physical and cybernetic threats. The seriousness of the cybernetic threat is reflected in content of the OCIPEP web site, where over 90% of the alerts, advisories, information notes and other analytical products posted focus exclusively on computer network vulnerabilities.[12] Recent OCIPEP presentations have highlighted the increasing speed and monetary cost of cybernetic incidents, quoting a 2000 Price Waterhouse Coopers report that identified a total cost of US$1.39T for all security breaches in 2000.[13] Computer Economics, an independent research organization, has produced figures of US$13.2B for the economic impact of malicious code incidents in 2001.[14] These economic costs are large, but do not include the possible impact on national security issues. OCIPEP's concern about the broader impact of incidents such as these indicates that Canada is seriously concerned about the protection of its critical infrastructure from cybernetic threats.

Within the CF, information protection has been a focus for a considerable time, as witnessed by the long-standing cryptographic programme. However, the increasing reli-ance on computer systems for command and control, and the need to securely integrate and interconnect the existing stovepipe infor-mation systems, compete with the requirement to access the Internet for unclassified information processing and to comply with the Government On-Line (GOL)[15] directives. As a result of these requirements and the need to protect our systems against the range of threats from script kiddies[16] and hacktivists[17] to foreign covert operations,[18] CF efforts have focused on CND,[19] with intelligence gathering performed by a number of Government agencies, including DND, the Communications Security Establishment (CSE)[20] and the Canadian Security Intelligence Service (CSIS).[21] CNE and CNA, however, have re-mained relatively undeveloped beyond the definitions and concepts contained in the CF IO policy. As the tide begins to turn in meet-ing the CND challenges, it is appropriate that attention is now paid to the capabilities that CNE/CNA can provide to the Canadian Forces. However, to determine whether they will be valuable to the CF, it is important to understand what the CF capability requirements are and how they are determined.

How the CF Selects Military Capabilities

That CNE/CNA have military applications is clear, but the potential for military employment alone is not sufficient to invest funds in developing the capability. Indeed, there are many military capabilities that the CF currently neither has nor is soon likely to possess; for example, the air force does not have an integral Airborne Warning and Control System (AWACS), the Navy does not have aircraft carrier capabilities, and the Army possesses no heavy artillery or heavy

mechanized forces. Selecting the capabilities the CF will possess is, instead, a reflection of functionality, affordability and, of course, Government policy.

The military capabilities that the CF develops must reflect the Canadian defence policy, which in turn should reflect Canadian foreign policy. With the 1994 White Paper on Defence acting as the current Canadian Government direction and guidance, it has been determined that the CF must maintain "multi-purpose combat-capable forces."[22] With this guidance and the further direction provided in DND's *Strategy 2020*, the Canadian Forces has established a Strategic Capability Planning framework that reflects a capability-based approach to force development. From this approach has been created a Canadian Joint Task List (CJTL) which de-scribes and relates different types and levels of capabilities that are currently required of the CF. The CJTL addresses eight major ca-pability areas:[23]

- Command;
- Information and Intelligence;
- Conduct of Operations;
- Mobility;
- Protection of Own Forces;
- Sustainment;
- Generation of Forces; and
- Coordination with Other Government In-itiatives (Coord with OGIs).

These major capabilities are subdivided into three levels of tasks: those carried out at the military strategic level, the operational level and the tactical level. The strategic military level is concerned with identifying the military objectives and desired end states needed to meet the direction and constraints that have been provided by the political leaders. It outlines the military action needed, and allocates resources to accomplish this activity.[24] The operational level is involved in producing and sequencing the military and other resources assigned to an operation to reach the desired end state and meet strategic objectives.[25] Finally, the tactical level is involved in the planning and directing of military resources in battles or engagements within the confines of a larger operation.[26]

To provide a guide in evaluating what capabilities the CF should possess or develop, a matrix has been constructed that identifies, from a high-level perspective, the relative importance of each goal at each military level. Using a scale of High (H), where the CF seeks a high degree of capability, Medi-um (M), where a medium or moderate level of capability is acceptable, and Low (L), where only a low degree is needed, the following matrix was established in 2000 as the Capability Goals for the CF:[27]

Level	Command	Info & Intel	Operations			Sustain	Generate	Coord with OGI
			Conduct	Protect	Mobility			
Military Strategic	H	H	L	L	H	L	M	H
Operational	M	M	L	L	L	M	L	M
Tactical	M	M	M	M	M	M	M	H

Table 2.1 — Capability Goals for the CF

Ratings of Medium or Low reflect not only the perceived risks associated with achieving only a moderate or low level of capability, but also an assessment that the CF cannot independently achieve a high degree of capability in this area of military activity, because of either complexity or cost. The level of assessment in each category can best be understood by considering the example for the Command Capability taken from the *Strategic Capability Planning for the Canadian Forces* policy:

> A 'High' level of command capability at the military strategic level of war is assessed as necessary for the CF because it is at this level of conflict that the CF must advise national and multinational commanders regarding Canadian military options. The CF cannot rely on allies to perform this capability for them, and must therefore be independently competent at the military strategic level. The degree of command capability required at the operational level is less easy to determine. Ideally, the CF would have a "high" level of capability here as well, but this is not assessed as essential because the CF will conduct operational-level military efforts as part of a coalition or alliance unless it is a domestic operation. Therefore a 'Medium' level of capability is reasonable. A similar rationale is the reason for only a 'Medium' level at the tactical level.[28]

What advantages, then, do CNE/CNA provide in these fundamental military capability areas? For a true value-focused assessment, CNE/CNA should be assessed against other capabilities to determine which best meet defence objectives, based on the benefits, costs and risks.[29] Given the detailed evaluation required, this type of comparative assessment is beyond the scope of this paper. Instead, an individual assessment will be considered of how well CNE/CNA support the criteria.

Command and Intelligence

The functions of command and intelligence are inextricably linked, in that a commander who achieves information superiority has greater situational awareness and will be able to take rapid, precise offensive and defensive action.[30] With the concept of Network Centric Warfare (NCW)[31] emerging as a military response to the information age,[32] the use of CNE/CNA to exploit and attack the NCW information, and sensor and engagement grids, will provide commanders with tactical and operational advantage. At the operational and strategic levels, acquiring key intelligence from an adversary's information systems can provide excellent indica-tors of intent. This then can be used to attempt to influence the adversary not to adopt a particular course of action, or be used to better structure one's own capabilities for combat. Thus, CNE/CNA contribute well to the CF desire for a high strategic command and intelligence capability, while also supporting the moderate operational- and tactical-level requirements.

Operations

CNE/CNA operations will be most effective against an adversary that is highly dependent on his information systems. But is it probable that Canada or the United States, for example, would enter into conflict with any such states? In answering this question, it is important to recognize the shift that has taken place in the way the CF determines its military requirements. A shift from a threat-based scenario to a capability-based scenario means that requirements are not based on a single dominant threat, but on the capabilities necessary to meet many types of hostile intent. In simple terms, capabilities

are not developed based on who we think our enemies are, but rather what capabilities will be of advantage across the spectrum of conflict. Naturally, capabilities that are widely applicable across the spectrum of conflict are most attractive.

What then would CNE/CNA bring to a conflict with a technologically less dependent adversary? Considering the extreme ends of this situation, one could first consider a large but not technically advanced military force such as the Chinese People's Liberation Army (PLA). Despite the significant inroads that China is making to improve its telecommunications and information infrastructure,[33] China is not yet highly dependent on its information infrastructure to conduct military operations. However, Chinese military concepts consider Information Warfare (IW) as an unconventional warfare weap-on that should be used by the inferior to ov-ercome the superior: in essence, for the Chi-nese, it is a pre-emptive weapon.[34] While CNA may not be a widely applicable capabil-ity to counter this type of an adversary, CNE activities could clearly be effective in deter-mining the capability and source of possible cybernetic threats, and developing means and methods of defending against them. An ad-versary cannot develop a CNE/CNA capability of his own without being connected to an infrastructure common to us both: the Internet, phone systems, etc. Thus, CNE efforts to determine his methods and intent, and CND to protect us from those intentions, are critical requirements in countering this type of asymmetric threat.

A different extreme for conflict resides in the possible capabilities of small non-state adversaries, for whom asymmetric attack with Weapons of Mass Destruction (WMD) or other conventional weapons is possible. While the execution of these activ- ities does not need to rely on information or information systems, their planning and coordination is rarely accomplished without them. In a Threat Analysis paper published on 21 December, 2001, OCIPEP commented that despite the relative technological isolation of Afghanistan itself "there has been significant, albeit unsubstantiated, reporting that bin Laden and his Al-Qaida organization are sophisticated users of computer and telecommunication technology. For example, it has been reported that Al-Qaida personnel use the Internet for sending encrypted communications."[35] With effective cuing by oth-er intelligence sources, including Human and Signals Intelligence, CNE could again be used to focus on the information systems used by these adversaries to identify their in-tent and capabilities, and develop countermeasures. Thus, while CNA is most effective in conflict situations that incorporate in-formation systems in their offensive action, CNE is effective even in situations that are not. In less overtly hostile situations, such as peace support operations, CNE/CNA must al-so be able to provide an effective capability.

For over a decade now, the demand for Canadian Forces involvement in international peace operations has been increasing dramatically.[36] The nature of these operations varies from humanitarian assistance to peace enforcement, with the CF needing to maintain its core combat effectiveness as well. As a result, our military capabilities should be effective tools within the restraints imposed by Peace Support Operations, while still being capable of delivering and support-ing combat capabilities when necessary.

The use of IO, in particular Public Information and PsyOps, as a non-lethal means of influencing adversaries has had a significant effect in past military operations such as

in the NATO Implementation Force (IFOR) in Bosnia.[37] The development of non-lethal CNE/CNA capabilities to influence adversaries in a similar fashion would prove to be an effective capability at the tactical and operational levels. For example, by confronting an adversary with advance knowledge of his plans and intentions, or by denying him his command and control systems, it may be possible to dissuade him from proceeding. An example of the possible strategic effects that CNE/CNA can have was seen in the widely reported allegation that United States hackers accessed banking networks and systems to threaten Slobodan Milosevic with the removal of funds from his bank accounts.[38] The US Department of Defense denied their involvement in any such activity, citing international legal constraints that would prohibit it.[39] The legal and political issues associated with such actions are, indeed, considerable and will be addressed further in Chapter III; however, given acceptable circumstances, the possible strategic benefits from influencing activities in this way is appealing.

At the tactical and operational levels, CNE/CNA has already been used to support military operations. US Air Force General John Jumper confirmed to the media in 1999 that CNA penetration techniques were conducted against a Yugoslavian military computer system to manipulate it for the protection of a US or NATO attacking force.[40] Thus, through its ability to deceive an adversary, CNE/CNA can provide Force Protection to friendly forces.

Force protection requirements for those conducting CNE/CNA will be dependent upon whether remote access or physical access is required for the activity. Obviously for remote operations, the need for protec-tion is limited, as the force will not be within the area of operations, and is thus not at risk of enemy fire. In a society that tolerates on-ly low casualty rates, this could make the re-mote CNE/CNA capability a very attractive option. For those instances in which physical access is required, force protection will be required, either for the military asset that engages in the physical destruction of the in-formation system, such as a bomber aircraft, or for the special forces capability that will escort the CNE/CNA team to the targeted system. Thus, the greatest dividends will be paid, with respect to force protection, when remote operations are conducted.

In a similar manner, CNE/CNA operations are extremely effective in meeting the third Operations capability, Mobility. Again, the ability to conduct remote operations neutralizes the traditional CF concern for a high level of strategic mobility, as no movement from the protected centre of operations is required to carry out the function. For those instances in which kinetic destruction is required, the use of air assets, for which mobility is a key characteristic, will meet the tactical requirements. For non-destructive activities that require physical access, the likely choice of escort by special forces, who train and operate for mobility, will meet the tactical requirement.

Sustainment and Force Generation

As in the case of mobility, the fact that CNE and CNA activities can be conducted remotely greatly reduces the sustainment and force generation requirements that accompany other deployed military capabilities. The troop rotation, airlift, and logistics requirements that add complexity to deployed operations do not need to be addressed, unless CNE/CNA activities require a physical presence in an area of operations. Instead, the static environment of the Department's headquarters organizations will address the traditional needs for sustainment and force

generation.

As previously discussed, with limited funding available for the establishment of new capabilities, the development of CNE/CNA capabilities is extremely inexpensive for the possible effects. This is because the equipment needed for CNE/CNA is commonly available, with specialized programming, hardware and personnel training comprising the majority of the costs. The procurement cost for a single F/A–18C aircraft currently runs at approximately US$24M,[41] whereas the cost to purchase 20 state-of-the-art computers would be approximately US$444K.[42] Thus the capital costs for force generation and sustainment are relatively small in comparison to those of other capabilities.

Coordination with Other Government Initiatives

Interoperability with our allies, especially the United States, is a key requirement for the CF.[43] The interconnected nature of our existing defence agreements, intelligence, and surveillance capabilities reflects this relationship. Future investments in the Joint Space Project and the Military Satellite Communications Project are seen as investments both in interoperability and in access to other intelligence and information sources.[44] In essence, contributions made in one particular area can result in access to other areas of interest. From a CNE/CNA perspective, a combined approach to conducting global network surveillance would be to the benefit of both nations, each feeding the larger intelligence database for analysis and exploitation as needed. With the existing agreements for intelligence sharing from other sources, extending the interoperability to the fields of CNE/CNA is not beyond reasonable expectation. It does, however, require an effective capability contribution on behalf of the CF. With this agreement in place at the strategic level, tools and techniques developed for use at the tactical level can be exchanged, with Canada and the US each assuming areas of expertise. In this way, CNE/CNA support the requirement for high levels of coordination with other governments at strategic, operational and tactical levels.

Final Assessment

Upon examination of how CNE/CNA would contribute to the CF Capability goals, it is clear that across all levels, they support the high and medium capability requirements and frequently exceed low capability requirements. The remote nature of CNE/CNA operations supports the requirements for mobility, force protection, sustainment and force generation, while the contribution to strategic intelligence allows command to be more effectively executed.

Thus we can see that CNE/CNA meet and exceed CF capability goals. For a true value-based approach to capability selection, formal comparisons to other capabilities should also be conducted to determine their priority with respect to other candidate capa-bilities. However, given their low procure-ment cost in comparison to other capital pro-curements and the recognized importance of strategic intelligence, CNE/CNA deliver sig-nificant “bang for the buck”. This should re-sult in favourable consideration for development.

While it is clear that CNE/CNA are capabilities that have much to offer the CF, it is still necessary to consider other factors in determining their usefulness. Key among these is the issue highlighted by the US Department of Defense, when it denied use of CNA against Slobodan Milosevic: what are the legal and political restraints to employing CNE/CNA? These factors will be examined next.

LEGAL AND POLITICAL

CONSIDERATIONS

The past decade has witnessed increasing debate over the legality and the political sensitivity of CNE and CNA. Within Canada, however, this debate has not had significant prominence for two reasons. First, Canadians tend not to think of themselves as aggressive in nature. As evidence, consider how the use of the term "Canadian peacekeeper" in our vernacular has nearly replaced the more accurate term "Canadian soldier". Our historical involvements in conflict strongly belie this pacifistic self-perception, yet it remains a tangible element of the Canadian psyche. As a result, debate on the development and use of new military capabilities is perhaps seen as "inappropriate" and is thus avoided. A second possible reason why this debate has been muted is the historical secrecy that has surrounded Canadian intelligence agencies and their mandates. If the CF is to consider the use of CNE/CNA, this aversion to discussing military and intelligence issues must be overcome; the realities of the legal and political issues need to be publicly addressed.

This chapter will address the legal and political considerations of executing CNE/ CNA capabilities. It will begin by reviewing Canada's traditional involvement in intelligence activities, and then outline our current intelligence collection and analysis capabilities. Increased concern over terrorism and the introduction of Bill C-36, the Anti-Ter-rorism Act, passed by Canadian Parliament on 28 November 2001, sets the stage for CNE by formally recognizing the importance of gathering intelligence through the exploitation of the global information infrastructure. To assess the legality of CNE/CNA activities, a review will be conducted of the international laws that guide the management of conflict and the conduct of warfare. It will become evident that changes in the nature and perception of "use of force" concepts will re-quire Canada to consider not only the methods by which CNE and CNA are executed, but also the possible and actual effects of those activities. Finally, recommendations will be made for the politically acceptable and legal use of CNE and CNA in Canada.

Canada's Intelligence History

Canada had been involved in intelligence gathering and processing[45] since the First World War, but it was not until the middle of the Second World War that the use of intelligence was developed for other than internal security and counter-intelligence func-tions.[46] While Canada participated in a num-ber of allied intelligence operations, including the establishment of Camp X, an espionage and sabotage training facility near Toronto,[47] Canada's greatest involvement was in the de-velopment of its signals intelligence and, to a lesser degree, its code-breaking capabilities. In the quid pro quo relationship that exists in the world of intelligence, "Canada found it-self actively and intimately involved in a great power intelligence alliance."[48]

As World War II was drawing to a close, the future peacetime role of the new Canadian intelligence capability began to be debated. The Canadian Joint Intelligence Committee developed a proposal for a peacetime strategic intelligence capability, "under which were subsumed the fields of military, political, scientific, economic, demographic and geographic intelligence as the key to successfully facing the challenges of an uncertain future."[49] These concepts were formalized in 1945, when Lieutenant-General Charles Foulkes, the Chief of the General Staff, produced a paper entitled *A Proposal for the Es-tablishment of a National Intelligence Orga-nization*, in which he argued that Canada's foreign policy and national

security were de-pendent on access to good intelligence from allies, and that to get it, Canada must itself make a meaningful contribution.[50]

However, this concept of a centralized multidisciplined intelligence organization did not emerge. To some degree, the resource re-quirements for such an ambitious plan played against its chances of succeeding.[51] Certain-ly the discovery of Soviet espionage activities in Canada in 1945 tended to focus intelligence needs on internal security matters.[52] Ultimately, the signals intelligence and code-breaking capabilities were transferred to the Communications Branch of the National Re-search Council,[53] now called the Communications Security Establishment (CSE), which was transferred by an Order-in-Council to the Department of Defence in 1975.[54] While the Joint Intelligence Bureau was eventually es-tablished in 1946, the multifaceted intelligence collection and analysis capability envisioned by Foulkes never appeared. Instead, with all major intelligence committees being chaired by External Affairs,[55] it was determined that Canada "…could rely upon its allies to supply the information it required, provided that it made acceptable contributions though its efforts in the field of signals intelligence. The principle of quid pro quo functions independently of the means used to collect foreign intelligence."[56] Signals intelligence, therefore, has been key to Canada's access to strategic information necessary for the development of its foreign and national security policies. With the intelligence-gathering role of CNE, Canada could provide a new capability to the shared intelligence com-munity.

Moving on from Signals Intelligence?

Information about Canada's intelligence capabilities and roles has remained, for understandable reasons, under a shroud of secrecy. But recently, in the wake of the "9/11" al-Qaida terrorist attacks in the United States, Canada's efforts to fight terrorism have brought the missions and roles for CSE into the public spotlight. CSE's increased focus on protecting Canadians has led to a stated desire to focus more closely on transnational issues.[57] In keeping with this new objective, one element of the new Anti-Terrorism Act amends the National Defence Act to formalizing the role and mandate of the CSE, and set out its role in combating terrorism. In particular, Article 273.64(1) establishes that:

The mandate of the Communications Security Establishment is:

a. to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intel-ligence priorities;

b. to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

c. to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[58]

Of interest in the inclusion of Article 273.64(1)(a) are the clear provisions for the use of the "global information infrastructure for the purpose of providing foreign intelligence…." This global information infrastructure is formally defined to include "…electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to

those emissions, systems or networks."[59] Further, in accordance with Article 273.65(6), "[t]he Minister of National Defence may is-sue directions for the Canadian Forces to sup-port the Establishment [CSE] in carrying out activities authorized under this section."[60] What does this mean for the development of a CNE capability?

Primarily, these formal mandates and relationships provide a legal framework through which CSE, the CF, or both could undertake intelligence gathering using CNE techniques. The inclusion of this type of operation in the mandate recognizes the interconnectedness of states through commercial land-line and satellite networks, and the value that can be gained by exploiting information systems to gather strategic intelligence. Operations in this realm need not focus solely on covertly accessing classified information systems. Rather, as theorized by Sherman Kent, an influential American intelligence official both during and after World War II, "over 90 per cent of the intelligence information required by a government could be found through careful examination of openly available material."[61] Extrapolating this from its mid-twentieth-century context to the present, the examination of networks connected to, and information available on, the Internet will also yield information of intelli-gence value. The use of CNE can then be combined with other intelligence sources, to enhance Canada's ability to pursue its foreign and national security policies.

For the CF, the CNE function can also provide important information that Canada and its allies need to meet military intelligence requirements and to support the use of CNA as an offensive military capability. How and when new capabilities such as CNE and CNA can be used, however, requires an examination of the legal framework surround-ing the use of force and espionage.

International Law and the Use of Force

In modern society, the law essentially serves two purposes: first, to regulate the affairs of all persons, be they individuals, corporations or governments; and second, to set a standard of conduct and morality. While each nation or state establishes laws to regu-late its internal affairs, there also exists the body of law known as international law, which governs the relationships between states.[62] International agreements between states are considered binding once these states have expressly agreed to comply with them. In addition, there is a body of law known as customary international law "which consists of practices that have been so widely followed by the community of nations, with the understanding that compliance is mandatory, that they are considered to be legally obligatory."[63] One of the greatest contributions of international law has been in the regulation of conflict between nations. Specifically, there are two strains of international law directly relating to conflict: *jus in bello*, the standards for the conduct of war, and *jus ad bellum*, the laws relating to the management of conflict between states.

The law of armed conflict, as *jus in bello* is commonly referred to, does not concern itself with the legality or illegality of re-sorting to conflict, but rather, it addresses the actual conduct of warfare itself. Many rules of war existed as customary international law for centuries; these were practices common-ly carried out and respected by combatants but not specifically covered in treaties. The act of codifying the law of armed conflict be-gan in the nineteenth century, and since that time it "…has generally developed into two regimes: the Hague regulations that govern the means and methods of warfare, and the Geneva conventions that govern the protection of victims of war."[64] These rules embo-dy three main concepts: military necessity, humanity and

chivalry.[65] Based on these con-cepts, armed forces must comply with a number of operational principles.

The first of these principles is *distinction*, which means that commanders are obliged, using the information available to them, to distinguish between legitimate targets, civilian objects and the civilian population. The second principle is known as *non-discrimination*, which means that the law of armed conflict is binding on both parties in a conflict, regardless of which is deemed the aggressor. In addition, this principle requires that the laws of armed conflict be applied consistently without distinction as to race, colour, religion or faith, gender, birth or wealth.[66] The third principle is that of *proportionality*, which creates a relationship between the idea of military necessity and humanity. In this regard, the principle implies that "…collateral civilian damage arising from military operations must not be excessive in relation to the direct and concrete military advantage anticipated from such operations."[67] Finally, the fourth principle of *reciprocity* refers to the concept that military forces must treat their enemies in the same manner in which they would like to be treated, as set down in the Hague and Geneva conventions.

That these rules exist, and that nations are bound to abide by them, does not, unfortunately, mean that they are respected. The recent history of conflict in Vietnam, Somalia, and the Balkans, clearly provides instances of failure to respect the law of armed conflict, particularly with respect to non-combatants. Canada, however, is committed to these obligations. Within the guidelines provided to the CF, this responsibility has been expressed as follows:

> The obligations binding on Canada in accordance with Customary International Law and Treaties to which Canada is a party are binding not only upon the Government and the CF, but also upon every individual. Members of the CF are obliged to comply and ensure compliance with all International Treaties and Customary International Law binding on Canada.[68]

Thus, the CF must ensure that its current and future means of warfare do not violate these principles either through their methods, or in their effects.

Turning away from the conduct of warfare itself, the *jus ad bellum* principles of international law are relevant in examining the management of conflict, armed or not, between states. In ratifying the United Nations Charter in 1945, Canada and the other signatories agreed under Article 2(4) to refrain from "the threat or use of force against the territorial integrity or political independence of any state."[69] The inclusion of this article in the UN Charter was a significant step forward in managing conflict as it is tantamount to agreeing not to threaten or initiate war with any other state. Recognizing that this statement alone will not eliminate interstate conflicts, the UN Charter provides under Article 39 that

> The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.[70]

The UN Charter also acknowledges, in Article 51, that nations have "the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to

maintain international peace and security."[71] This provision for self-defence has since been taken one step further with the development of the concept of "anticipatory" self-defence. The scope of this concept was well defined in a letter drafted in 1842 by then-US Secretary of State Daniel Webster, when he iterated that anticipatory self-defence should "be confined to cases in which the necessity of that self-defense is instant, overwhelming and leaving no moment for deliberation."[72]

It is interesting to note the differences in the language used in articles 2(4), 39 and 51 of the UN Charter. In particular, Article 2(4) discusses a "threat of force", while Article 39 addresses the broader "threat to peace" assessment that may face the Security Council. However, in Article 51, the language is much more constraining, recognizing the right to self-defence only in cases of "armed attack". It is evident that this "reflects the Charter's preference for community responses (e.g., even threats to peace) over individual ones."[73] The nature of this inconsistent language has caused much discussion about whether particular state actions constitute violations of international law, whether they can be construed as threats or use of force, or whether they equate to armed attacks. How these actions are interpreted, of course, determines how other states legally respond to them.

There are no set formulae to address all circumstances. Volumes of research have been devoted to analysing what the drafters of the UN Charter were or were not considering as "threats" or "use" of force. Does political or economic coercion constitute a use of force? It is clear that economic sanctions and trade restrictions are well used by governments to protect their own national interests. But at what point do these actions constitute threats to others or a use (albeit unarmed) of force? If such actions are deemed as being threats of force, the initiating state would certainly be violating Article 2(4) of the UN Charter. Would there be a point at which a state suffering under this coercion would be considered "authorized" to resort to armed self-defence, to respond to an unarmed use of force?

While a strict interpretation of the UN Charter can provide a narrow set of answers to these questions, states have not let these language restrictions hobble their actions in international relations.

> On the contrary, in many cases states have responded to situations, either individually or in concert, in which community interests were served by taking coercive measures not specifically provided for in the Charter. Such incidents combine to map out a complex operational code as to those coercive acts the international community, or at least the politically relevant members thereof, accepts as lawful.[74]

In the management of conflict, therefore, it is evident that existing international law is to some extent "qualified" with regards to what states consider to be acceptable practice or behaviour. The development of the operational code, referred to above, is perhaps analogous to the development of customary international practices that will modify the guidelines of the UN Charter. What impact, then, do the guidelines of the original charter and the developing operational code have on the introduction and use of CNE and CNA?

CNE and International Law

The collection of intelligence information is not illegal under international law. "No serious proposal ever has been made within the international community to prohibit intelligence collection as a violation of

international law because of the tacit acknowledgment by nations that it is important to all, and practiced by each."[75] It is a customary practice of nations and is acknowledged as being a function that supports a state's inherent right to self-defence, a right recognized in Article 51 of the UN Charter.[76]

Espionage, the use of spies to collect information not publicly available, is normally a violation of domestic law. In wartime, spying is still considered legal under interna-tional law, although the punishments under domestic laws, if apprehended, are usually capital in nature. However, international law provides that "soldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies."[77] In the realm of CNE, can these phy-sical conditions be translated into cybernetic equivalents? Is there a cybernetic zone of op-erations that encompasses the computer sys-tem being targeted for information? Will CNE activities need to be attributable to a particular military force, to ensure prisoner of war protections?

As CNE is generally conducted from outside enemy territory, US Department of Defense legal counsellors consider that these questions will likely not become significant legal issues to ponder, as

(1) If an individual is not physically behind enemy lines he or she is not subject to capture during the mission; and

(2) There will be no issue of acting under false pretenses by abusing protected civilian stat-us or by wearing the enemy's uniform.

> This will exclude most information operations activities from being considered espionage during wartime. Nevertheless, behind-the-lines missions to collect information, or to install devices that enable the collection of information, may well raise wartime spying issues.[78]

This statement implies to some degree that espionage is not espionage unless one is caught. A more realistic statement might be that as espionage is considered a legal activity under international law, the domestic legal consequences of espionage are not likely to be faced in the use of CNE during armed conflict.

In the peacetime challenge of conflict management, acts of real or suspected espionage have resulted in the use of force by the targeted state. This response has not been well supported internationally. For example, international law holds that states have the complete and exclusive sovereignty of the airspace over their territory, including their territorial waters.[79] Aircraft, unlike naval vessels, thus do not have a right of innocent passage. On 1 May 1960, the Soviet Union shot down a U-2 reconnaissance aircraft over Soviet territory claiming that the flight constituted an act of aggression on the part of the US, in that it might either contain a deadly payload or be indicative of a further attack, to which an armed response in self-defence would be required.[80] The UN Security Council disagreed with this assertion, and characterized the U-2 flight not as a use of force, as outlined in article 2(4) of the UN Charter, but rather as a violation of Soviet airspace. This ruling proposes that "a degree of reasonableness attend any response — in essence that any response must be proportional to the act of self-defence against a threat, whether real…or perceived or alleged …."[81] Since the "9/11" attacks on the Unit-ed States, the dispatching of fighter aircraft to confront and possibly shoot down unresponsive commercial aircraft has

indicated that the criterion for reasonableness has broadened.

As discussed previously, the use of CNE as a required precursor to CNA can pose problems for states in accurately determining the intent of the CNE being conducted in their networks.

> [O]nce a state has penetrated another state's information infrastructure to conduct espionage, it is only one keystroke away from the capability of engaging in hostile and potentially destructive ac-tivities that are unlawful under inter-national law.… If a trespassing state is simply looking around and copying files, for example, it may likely be engaging in nothing other than espionage. If those files, however, contained orders of battle and rules of engagement, then the trespassing state may be engaging in a pre-attack exploration of the battlefield. Similarly if the trespassing state were installing trapdoors to facilitate future penetrations, then it may be engaged in pre-attack penetrations. Finally, the planting of cyber-tools may be indicative of an attack that has not yet manifested itself. Short of an actual destructive attack, howev-er, it is very difficult for a state to be sure of the intent of a trespassing state — albeit at the minimum such a trespassing state is engaged in espionage.[82]

If Canada deems it politically acceptable to engage in CNE during peacetime, the activity is certainly considered legal under international law. However, we must be aware of the possible responses this activity may elicit under Article 51 if the target nation perceives that activity as a precursor to armed attack. The anonymity that typifies CNE provides some protection from a target nation's self-defence actions. However, an examination of that nation's likely responses, based on the function of the targeted network, the nation's past history and other international precedents, will be required to form an accurate risk assessment for the CNE activity. The integration of legal counsel into planning the activities for all CNE missions will be essential. These risks must be carefully assessed and managed if CNE is to provide peacetime intelligence and in wartime the necessary information to conduct CNA.

CNA and International Law

CNA, by its very definition, constitutes a use of force, as its objective is to "disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[83] While in the strictest sense CNA does not constitute a use of armed force, its effects can produce the same destruction as the use of armed force and thus, in practical terms, it is likely that the international community will be more concerned with the results of the attack than the methods.

> [I]f a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial system and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack. Even if the systems attacked were unclassified military logistics systems, an attack on such systems might seriously threaten a nation's security. For example, corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop

> mobilization or medical supplies may seriously interfere with its ability to conduct military operations. In short, the consequences are likely to be more important than the means used.[84]

In adopting a CNA military capability, therefore, it must be clearly understood that its use will be considered as a use of force, the consequence of which may result in enemy use of similar or conventional military means.

As a use of force, the CNA activity must also conform to the laws of armed conflict. Targets must be assessed for military value and proportionality, or likely civilian collateral damage. Further, the methods used in conducting the attack must not violate any existing Hague or Geneva conventions. Summarizing public discussions on this topic, Thomas Wingfield provides examples of two very similar CNA scenarios, one of which is illegal under the laws of armed conflict, and another that is not.

> In a recent article, an author states: "analogy strongly weighs against sending a logic bomb disguised as e-mail from the International Committee of the Red Cross (ICRC) or even from 'Microsoft Software Support' — where such a message might be permissible without perfidious labels."[footnote omitted] The flaw in this statement is that it incorrectly equates two information attacks that are quite different under international law. The first, a false message from the ICRC, is clearly perfidious, in that it delivers a weapon under the protection of the Red Cross symbol — an action directly analogous to delivering a car bomb in an ambulance. The second, however, is just as clearly lawful, in that Microsoft Corporation enjoys no protected status under international law. A message from Microsoft would be no different from a message from any other firm with which a belligerent is doing business. The analogy here would be a comman-do team emplacing a bomb in enemy headquarters while disguised in the ov-eralls of a local plumbing company.[85]

Thus, in acquiring a CNA capability, one must understand that its employment can be considered as a use of armed force, for which the methods of delivery and effects must respect the laws of armed conflict.

Final Assessment

While Canada's historical involvement in the intelligence field has concentrated on signals intelligence and code breaking, the recent changes introduced in Bill C-36 set the stage for CSE and the CF to engage in intelligence collection by exploiting the global information infrastructure. Canada's current contribution to allied intelligence secures ac-cess to the information needed to develop meaningful foreign and national security policies. The desire to access intelligence related to transnational issues can be well supported by exploiting those systems that interconnect the global community. CNE can certainly provide this capability and should be developed for this purpose.

The use of espionage is considered legal under international law, and CNE, with its characteristic trait of anonymity, is well suited to intelligence collection. The political will to enter into the realm of CNE is evident in CSE's new mandate. However, it must be carefully planned and implemented as its discovery could, in certain circumstances, be construed by a target nation as a precursor to the use of armed force, to which they would be legally entitled to respond. Any such response, while requiring a sense of reasonableness to be considered legal,

could potentially include the use of conventional armed forces.

CF use of CNA capabilities could legally be considered a use of force. Thus, Canada's use of CNA must comply with the exigencies of international law. The ability to execute this capability in times of hostilities, however, is dependent upon the execution of CNE functions during times of both peace and conflict. As a military capability that is highly desirable for its effectiveness in the information-dependent global environment, CNA operations can be implemented in a manner that respects both *jus ad bellum* and *jus in bello* international laws.

There are, therefore, no legal impediments to Canada's establishing CNE and CNA capabilities. Based on military strategic priorities, the CF should work to define both types of CNE/CNA missions: those that support the overall intelligence picture; and those that will conduct the reconnaissance work necessary for the use of CNA in neutralizing adversaries' military capabilities. As is the case for other military capabilities, international codes of conduct and the law of armed conflict will regulate their use. The requirement for CNE/CNA to be used in a deliberate and measured way must be reflect-ed in the manner in which these capabilities are developed.

ESTABLISHING THE CAPABILITY

While the use of CNE and CNA must comply with the legal and political considerations discussed in the previous chapter, the establishment of these capabilities must also address the unconventional nature of these operations. The need for this capability to be well developed before times of crisis, conducted in secrecy and precise in effect, requires a high level of training which must be reflected in the way it is developed, used and controlled. In this chapter, it is proposed that the best model to be used in establishing this capability is that for Special Operations Forces (SOF).

To examine the appropriateness of this model, the role and purpose of SOF, including Canada's JTF2, will be discussed. A comparison of the CNE/CNA missions with SOF missions will also be conducted. After examination of the similarities between SOF and CNE/CNA capabilities, methods and objectives, analogies will be drawn between the SOF training requirements, and those of CNE/CNA. Finally, the SOF comparison will lead to the recommendation of an appropriate command and control model for CNE/CNA capabilities, based on existing CF structures and SOF best practices. To begin this evaluation, an understanding of SOF characteristics and missions is required.

Role of Special Operations Forces

Special Operations Forces (SOF) are a military capability found in many nations. One 1997 summary identified 287 special force units within 66 nations or states.[86] The term 'special operations' is defined variably around the world; however, US Joint Special Operations Doctrine provides a broadly accepted definition as

> …operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or informational objectives by unconventional military means in hostile, denied, or politically sensitive areas.[87]

While the range of operations can vary significantly, special operations missions can be usefully divided into nine different categories:[88]

- **Direct Action** — short-duration strikes and other small-scale offensive actions

including, for example, raids, ambushes, direct assault, standoff attacks and recovery operations.

- **Special Reconnaissance** — obtaining or verifying, by visual or other collection methods, information concerning the capabilities, intentions and activities of real or potential enemies, or to secure data regarding meteorological, hydrographic or geographic characteristics of a particular area;

- **Foreign Internal Defence** — organization, training, advising and assisting Host Nation military and paramilitary forces, with a goal to enabling these forces to maintain the Host Nation's internal stability.

- **Unconventional Warfare** — advising, assisting, organizing, training and equipping indigenous forces and resistance movements; guerrilla warfare; sabotage.

- **Combating Terrorism** — defensive measures to reduce vulnerability to terrorist acts, such as evaluation of existing physical security systems and training and offensive measures to prevent, deter and respond to terrorism, including hostage or sensitive material recovery and attack of terrorist infrastructure.

- **Psychological Operations** — inducing or reinforcing foreign attitudes and behaviours that are favourable to a command-er, including safety warnings, surrender appeals or instructions or appeals for pub-lic support.

- **Civil Affairs** — establishing, maintaining, influencing or exploiting relations be-tween military forces and civil authorities, to ensure that civilians do not interfere with operations and that they are protect-ed.

- **Counterproliferation of Weapons of Mass Destruction** — actions to seize, destroy, render safe, capture or recover Weapons of Mass Destruction (WMD).

- **Information Operations** — actions to affect adversary information and information systems while defending one's own information and information systems.

Special operations missions differ from conventional military operations in a number of ways. The missions are usually clandestine in nature[89] and have high military or political value. They can be executed to create favourable conditions by influencing the political will of a foreign nation or by setting the conditions for further military action, as has been seen in Afghanistan. The forces carrying out these missions are usually small in size and often operate far from bases. This requires insertion into hostile or politically sensitive areas, as well as support and extraction capabilities. Rigorous training and mission-specific rehearsals are usually required to increase the likelihood of success.[90]

Currently in the Canadian Forces, the only Special Operations capability resides in the Joint Task Force Two (JTF2) organization, responsible for federal counter-terrorism and hostage rescue.[91] Formal Canadian doc-trine for special operations, if it exists, is not publicly available; indeed, the full mandate for the JTF2 is known to be published only in Canadian Government Cabinet documents.[92] Outside of its known counter-terrorism man-date, however, its employment has been un-officially characterized to also include Direct Action, Special Reconnaissance and Foreign Internal Defence.[93]

While the JTF2 capability brings to mind the more offensive types of special operations, doctrinally the less destructive activities such as elements of Information Op-

erations (IO) can also be considered as special operations. Within the broad IO strategy, missions for SOF focus on targeting an adversary's "nodes, links, human factors, weapons systems and data"[94] and can be em-ployed either destructively in war or to deter or control crisis escalation. These definitions of SOF missions clearly encompass the broad purposes of CNE/CNA, which are established IO capabilities. Thus, the CNE/CNA functions should be considered as SOF missions. A more in-depth comparison of the CNE and CNA missions and special operations charac-teristics also reveals a clear association.

CNE and CNA as Special Operations Missions

While IO is recognized as an independent special operations activity, there is also great similarity between Special Reconnaissance and CNE missions. The difference is the operating environment in which the missions are conducted: for the first, it is a physical space, while for the latter, it is cyberspace. The desired output from each activity is the same: the collection of information that can be interpreted to provide target and threat assessment. This information may not be readily available on open systems, and like the Special Reconnaissance mission require-ment to get in and out of hostile or denied areas to gain information,[95] CNE activities involve the undetected penetration past an adversary's guarded information systems and databases. Finally, the CNE information gathering capability can focus on determining an adversary's strategic and operational capabilities and intent, depending on the tar-geted information system. This parallels the Special Reconnaissance role of focusing on operational and strategic targets beyond the reach of conventional reconnaissance forces.[96]

While CNE mirrors the Special Reconnaissance function, CNA parallels the Direct Action mission. In conventional warfare, lines of communication (LOC) are defined as "a route, either land, water, and/or air, which connects an operating military force with a base of operations and [along which] supplies and military forces move."[97] Direct Action missions can "involve an attack on critical targets such as the interdiction of lines of communications (LOCs) or other target systems."[98] For CNA operations, the LOC are the information systems that support the command, control and sustainment of fighting forces. CNA affects these LOC through system disruption, denial or destruc-tion, or via data destruction or manipulation. If adversaries cannot use or trust their infor-mation systems, their ability to conduct and sustain conventional warfare will be significantly impeded.

Direct Action missions can also involve the "the seizure, destruction, or neutralization of enemy facilities in support of conventional forces or in advance of their ar-rival."[99] A CNA example of this type of mission would be the conducting of a Denial-of-Service (DoS)[100] computer attack against net-worked air defence systems, or the manipulation of target recognition data to preclude the automated targeting of incoming air assets. For CNA missions, such as Direct Action missions, Special Reconnaissance, or CNE in advance of the attack, is required.

While there are many similarities between traditional special operations and CNE/CNA, there is one significant difference: the degree of physical danger and exertion required of the special operations forces themselves. Many special operations missions are designed to be clandestine; if the traditional SOF are discovered, combat forces will be required to extract the teams from the area of operations. For CNE and

CNA, however, the fact that the operation would normally be conducted from within the home state, well outside the area of operations, eliminates this requirement. Thus, the nature of the training and physical requirements for the two types of special operations forces will have significant differences. If the CF is to develop a CNE/CNA capability, it is important to consider these necessary training requirements.

Training Development for Special Operations

Special Operations forces, by definition, require specialized, highly focused capabilities for which conventional forces do not train. To incorporate the training needed for special operations into larger convention-al forces would "restrict their ability to respond to a broad range of threats,"[101] and risk making them jacks-of-all-trades and masters of none. This is not to imply that the skills necessary for conventional forces are not im-portant for special operations. In fact, the op-posite is true. The personnel that work in special operations are generally mature, experienced military members who have performed well within one or more military specialties.[102] Colonel Charlie Beckwith, the first commander of the modern Delta Force, was certainly a believer in this philosophy, stating that

> …before a soldier could become a good unconventional soldier he'd first have to be a good conventional soldier. He had to understand what a rifle squad was all about, what a platoon could do, what a rifle company could do. To break the rules you have to know what the rules are. You can't be unconventional until you are conventional first.[103]

This postulation holds true for the skills required to execute CNE and CNA special operations missions. Before one can learn to exploit computer networks and information systems, a comprehensive understanding of networking principles, operations and system administration is necessary. Once these concepts have been mastered, detailed experience in the protection of information and information systems is important as it is through experience in defending networks that one learns the most common and most dangerous vulnerabilities. With this knowledge and experience in hand, the next stage is to develop the necessary skills and experience to create and exploit technical and procedural information system and network vul-nerabilities.

Acquiring detailed knowledge about the adversary's environment, such as the military structure, command and control relationships, and intra-organizational relationships, is as important in CNE/CNA as in any other special operations mission. It allows for an element of predictability in the adversary's behaviour, as well as acting as a trigger when the routine is disturbed. This may require training that focuses on operations of specific adversarial groups. In addition, as discussed in the previous chapter, use of force constraints also require that the CNE/CNA special operations forces act within predeter-mined Rules of Engagement for their missions. As a result, knowledge of the Laws of Armed Conflict must also form part of the overall training requirement. Thus, training for CNE/CNA skill sets will call upon exist-ing core military skills and the technical skills that are developed for the CND information protection mission. Upon this foundation, advanced skills specializing in network reconnaissance and infiltration, vulner-ability analysis, system dependence analysis,[104] weapons/sensor information systems analysis and exploitation development will all be essential. To properly develop these skill sets, a systematic, structured

approach to identify training requirements is required. A model such as that provided in the Canadian Forces Individual Training and Education System (CFITES) should be considered as a possible option for this training development.[105]

The sensitivity of the CNE/CNA tasks to be performed, and the possibility for lethal effects require a rigid approach to training development that will ensure that the correct skills are being provided to effectively conduct the required tasks. As has already been identified, the training requirements for CND, CNE and CNA tasks should be treated as a group of interdependent capabilities, building from the defensive to the offensive.

In addition to defining the training requirements, it is essential that personnel are appropriately selected to undergo this training, as the training investment time is not insignificant. Current experience in the CND mission has identified that a minimum of 18 months is required before personnel are properly trained to conduct certain tasks without direct supervision. It is essential, therefore, that the personnel selected for CNE/CNA training be well suited to the tasks. An analysis of the desired characteristics and possible benefits of selecting from established military occupations will have to be considered. This has not been the case in the past, as is evidenced by the selection of personnel for the CND mission.

Military Occupations in Special Operations

When the CND mission was initially mandated, a Network Vulnerability Analysis Team (NVAT) and DND Computer Incident Response Team (DND CIRT) were established within the CF. While it is considered that all members of the CF are responsible to protect the information in their environment,[106] it was recognized that a centre of expertise was also required to provide CF-wide infor-mation protection advice and direction. To conduct this mission, a detailed level of education, training and skill is required to execute the NVAT and DND CIRT functions. These teams were initially established using personnel from the Communications Research (Comm Rsch) and Communications and El-ectronics Engineering (CELE) occupations. The rationale for the selection of these personnel was two-fold. First, the Commander of CFIOG, who initially mandated the estab-lishment of this capability, had personnel re-sources from these occupations available for employment. Second, while most of the personnel did not initially possess the skill sets to conduct the CND mission, the characteris-tics and training in the Comm Rsch and CELE occupations were intuitively felt to be relevant to the tasks that needed to be performed.

Since the initial establishment of these CND capabilities, personnel from other mili-tary occupations have also been incorporated into the organization, again requiring signifi-cant additional training. What has not been done for the CND mission, and what needs to be done for the CNE and CNA missions, is to formally determine if there is/are one or more existing occupations that already train to meet some of the CND, CNE and CNA functions. If this is found to be the case, consideration should be given to select personnel from within these groups. However, should this not be the case, personnel selection for the CND, CNE and CNA missions should not be restricted to a predetermined set of military occupations.

This type of non-restrictive personnel selection policy appears to have been considered in the JTF2 recruiting process. Their model for personnel selection does not discriminate on the grounds of military occupation. As in any organization, the need for

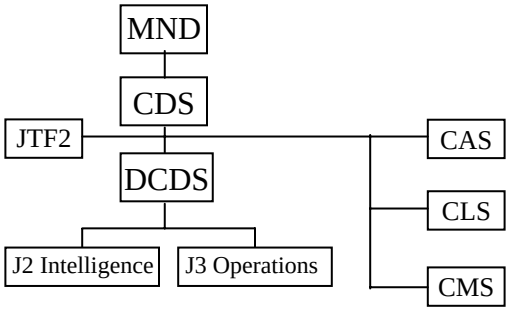
day-to-day support functions dictates a requirement for personnel with specific traditional support skills and occupations, such as financial and logistics support. However, for the Category A, Special Operations Assaulters, and Category B, Technical Specialists, the "open call" for personnel selection[107] indicates that no existing military occupation provides the type or level of training necessary to meet the required tasks. While experienced and highly fit military personnel with a combat arms background are desired, it would appear that limiting the personnel selection pool to combat arms occupations does not advance the training needed to meet the performance objectives and levels required for JTF2 tasks.

Thus, as in the case of JTF2, it is important to keep the special nature of CNE/CNA operations in mind as the task identification and training necessary for these capabilities are developed. It is equally important that an effective command and control structure be developed for these capabilities.

Command and Control for Special Operations

Special operations missions can be undertaken either unilaterally, as in a Hostage Rescue; independently from a larger military campaign, as in a Special Reconnaissance mission; or in support of a conventional commander, as in pre-assault cover and diversionary operations.[108] To ensure effective management of this capability, given its possible impact across strategic-, operational- and tactical-level operations, it is important that a robust command and control structure be implemented to support the varying nature of these operations. United States doctrine addresses this requirement by ensuring that despite its many different geographic and component commands, SOF missions are always executed through a SOF chain of command.[109] In a military as large as that of the United States, this has been accomplished through the establishment of various levels of SOF task force and component commanders, who ensure that mission tasks are appropriate and well supported. Within the CF, it is equally important to have this SOF–focused command and control structure in place.

Currently, the JTF2 organization is responsive directly to the Chief of Defence Staff (CDS)[110] for its counter-terrorism taskings and force generation, much like the Chiefs of the Air, Maritime and Land Staffs. As illustrated in a simplified diagram at Figure 4.1, the Deputy Chief of the Defence Staff (DCDS) is responsible for all deployed and domestic CF Operations, as well as the joint intelligence function. JTF2's direct tasking and reporting relationship to the CDS bypasses the normal structure for military operations and reflects the strategic political function of the counter-terrorism role.



CAS — Chief of the Air Staff
CDS — Chief of the Defence Staff
CLS — Chief of the Land Staff
CMS — Chief of the Marine Staff
DCDS — Deputy Chief of the Defence Staff
MND — Minister of National Defence

Fig. 4.1 — JTF2 Relationship to Normal C^2 Structure

An expansion of the CF SOF capability to include the CNE/CNA requires a revised command and control structure. The structure proposed in Figure 4.2 reflects the direct relationship of SOF to the CDS for force generation requirements and counter-terrorism, and a coordinating relationship with the DCDS for SOF capabilities used in

support of military operations. In addition, this diagram proposes the requirement for an information fusion capability to integrate the information generated by various sources, including SOF, to produce intelligence products that support existing and future conventional and special operations. Given the current relatively small size of the Canadian Forces' SOF capability,[111] the inclusion of CNE/CNA operations in a high-level, centralized SOF command and control structure would ensure that these capabilities are clearly and precisely exercised.

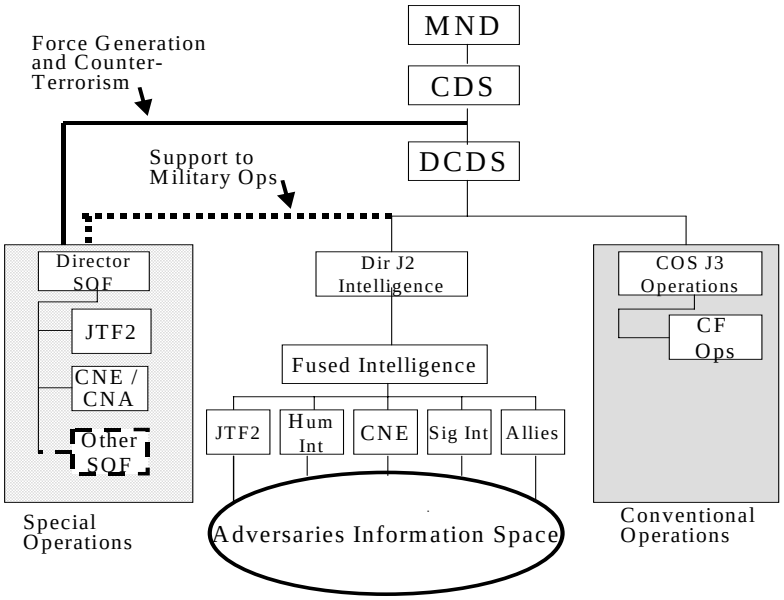


Figure 4.2 — Proposed SOF Command and Control Structure including CNE/CNA

Final Assessment

It is evident that CNE and CNA should be recognized as special operations capabilities. Not only are they offensive ele-ments of information operations, which is recognized as being a SOF mission, but their methods and objectives also closely parallel other recognized SOF capabilities, such as surveillance and reconnaissance and direct action. Accordingly, the doctrine for developing, commanding and tasking SOF forces should be used as a baseline in the development of the CNE/CNA capability.

The development of CNE/CNA capabilities requires unique training; comprehensive technical skills, familiarity with military operations, detailed target study, and an understanding of the Laws of Armed Conflict are all required elements. The impact of CNE/CNA operations thus requires a robust training model to ensure that forces are well trained to carry out precise and deliberate op-erations. In developing the training require-ments, the tasks and requirements necessary for the defensive CND mission should also be considered. In addition, the selection of the proper personnel is a vital element of building the capability.

Finally, the command and control of CNE/CNA capabilities must be retained within a simple and responsive structure, that recognizes and is accountable for missions that can be politically and strategically sensitive. In addition, the value that CNE missions can add to the overall intelligence picture can be significant. The integration of

CNE taskings and information into the larger intelligence gathering and dissemination function is vital if this is to occur. To meet these requirements, CNE/CNA should be integrated into a new SOF organizational structure that conducts the necessary force generation activities and coordinates with the DCDS in support of military operations.

CONCLUSIONS AND RECOMMENDATIONS

To determine whether the CF should adopt CNE and CNA as military capabilities, it has been necessary to consider the applica-bility and legality of these operations and ex-amine the necessary operational/organization-al structures. For a nation that must judicious-ly manage its resources, the development of CNE and CNA capabilities must fall in line with the Strategic Capability Planning model that has been developed for the CF. It has been shown that CNE/CNA do indeed provide capabilities that not only meet the required goals, but can do so across a broad segment of the conflict spectrum. CNE/CNA operations strongly contribute towards the re-quirement for strategic intelligence and com-mand, while the remote nature of their operations also support the requirements for mobil-ity, force protection, sustainment and force generation.

Public discussion about the use of CNE and CNA, however, has been limited by both the secrecy that has traditionally sur-rounded intelligence operations in Canada, and the general indifference that is shown to-wards military capabilities. In examining the legal framework in which CNE and CNA must operate, it is evident that despite their similarities, CNE and CNA are capabilities that are relevant at different places across the spectrum of conflict. As a result, there are different legal considerations for the use of each.

CNE is analogous to intelligence gathering, and as such is legal under international law. However, the use of CNE, if discovered by the target and attributable, may result in a variety of responses, depending on how the action is interpreted. Given the lack of existing customary law in defining threat and use of force guidelines for cybernetic activity, it can be difficult to accurately determine how a target may respond to discovering CNE operations. Thus, the integration of legal counsel into the planning activities for all CNE missions will be essential to best estimate what actions would be considered as armed attack or use of force. Ongoing analysis of state practices as international cybernetic activities and terrorism continue will be essential to accurately assess the impact of CNE activities.

As an intelligence gathering capabili-ty, CNE is applicable across a wide segment of the conflict spectrum. From a strategic in-telligence perspective, Canada gets access to allied intelligence sources based primarily upon its contributions in the signals intelligence realm. Access to this intelligence pro-vides Canada with the information it needs to develop meaningful foreign and national security policies. In a world that is quickly becoming more interconnected, CNE is an effective capability to provide this type of in-formation. Bill C-36 clearly recognizes this, providing CSE, the CF or both a mandate to exploit the global information infrastructure in support of Canada's security interests.

CNE is also an effective capability for military operations. In peace support operations, the non-lethal nature of IO has been used to influence adversaries to conform to a desired behaviour. CNE/CNA can be, and has been, used in a similar matter, exploiting the information and information systems upon which a belligerent relies to force or dis-

suade him from an undesirable course of action. While some adversaries may use asymmetric attack methods that do not rely on information systems, CNE is still an effective means of collecting intelligence about these activities. Few state or non-state adversaries can accomplish the planning and coordination of these activities without the use of common information systems. Based on military strategic priorities, the CF should work to define both types of missions: those that support the overall intelligence picture; and those that will conduct the reconnaissance work necessary for the use of CNA in neutralizing adversaries' military capabilities.

CNA is, by definition, a use of force and as such can be considered as lawful only in the exercise of one's inherent right to self-defence, under Article 2(4) of the UN Charter, or unless it is authorized by the Security Council under its Chapter VII authority. This is true for the use of any military force and, therefore, should not be a matter for significant public concern. The CF would have to carry out CNA operations within the constraints of *jus in bello* international law, regarding the means and methods of warfare, and the protection of victims of war.

The strategic impact that CNE/CNA can have, and their unique missions and functions, mirror the characteristics that make SOF missions different from conventional military forces. Elements of IO are doctrinally recognized as special operations missions. In addition, there are great similarities between Special Reconnaissance and CNE, and Direct Action and CNA. Hence, CNE/CNA capabilities should be considered as SOF activities. The development of CNE/CNA training and command and control structures should, therefore, parallel those processes that have been proven to work for SOF. The requirement for well-developed training programmes and robust command and control structures reflects the specialized training and political/strategic sensitivity requirements for CNE/CNA missions.

With respect to training, it is critical that the tasks to be performed be accurately assessed and translated into performance objectives to ensure that personnel are highly trained to conduct these sensitive missions. The development of personnel selection criteria and a study of existing military occupation structures will help to ensure that training is focused on the appropriate military personnel. The close relationship between CND and CNE/CNA also suggests that the training requirements for this complete suite of functions should be analysed together. Thus, a well-defined training development model, such as CFITES, should be used to formalize the CND and CNE/CNA needs analysis and training development process, and to implement a programme to establish personnel selection criteria.

A command and control structure for the CNE/CNA capability can be modelled on the existing JTF2 command and control struc-ture. Given the requirement for CNE/CNA to work closely with other military operations, a modified structure along the lines of that in Figure 4.2 is required. CNE/CNA should be integrated into a new SOF organization command and control structure that is responsible for its own force generation activities and coordinates with the DCDS in support of military operations.

Canada has a long history of military involvement in activities to promote international peace and security. This has included both intelligence gathering in a shared information environment, and the application of military force in war and peace support operations. The CF should adopt CNE and CNA as legitimate military capabilities that strength-en that commitment, providing new

tools to manage hostilities in an information age.

> In the field of observation, chance favors the prepared mind.
>
> — Louis Pasteur[112]

KEY TO ABBREVIATIONS

CAS	Chief of the Air Staff
CELE	Communications and Electronics Engineering
CERT CC	Computer Emergency Response Team Coordination Center
CF	Canadian Forces
CFIOG	Canadian Forces Information Operations Group
CFITES	Canadian Forces Individual Training and Education System
CJTL	Canadian Joint Task List
CLS	Chief of the Land Staff
CMS	Chief of the Maritime Staff
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
DND CIRT	Department of National Defence Computer Incident Response Team
DoS	Denial-of-Service
GOL	Government On-Line
ICRC	International Committee of the Red Cross
IFOR	Implementation Force
IO	Information Operations
IW	Information Warfare
LOC	Lines of Communication
MND	Minister of National Defence
NATO	North Atlantic Treaty Organization
NCW	Network Centric Warfare
NDA	National Defence Act
NGO(s)	Non-Governmental Organization(s)
NVAT	Network Vulnerability Analysis Team
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness
OGI	Other Government Initiatives
PLA	People's Liberation Army
RMA	Revolution in Military Affairs
SOF	Special Operations Forces
UN	United Nations
WMD	Weapons of Mass Destruction

NOTES

[1]Canada, Department of National Defence, Chief of the Defence Staff, *An Honour to Serve: 2000–2001 Annual Report of the Chief of the Defence Staff*, 2001, 24, <www.dnd.ca>, accessed 2 March 2002.

[2]Wayne M. Hall, "The Janus Paradox: The Army's Preparation for Conflicts of the 21st Century", *The Land Warfare Papers*, No 36, Oct 2000 (Arlington: The Institute of Land Warfare, 2000), 3.

[3]Within the United States, the National Infrastructure Protection Center (NIPC) provides this role; in Canada, it is the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

[4]W. Hays Parks, "The International Law of Intelligence Collection," *National Security Law*, edited by John Norton Moore, Frederick S. Tipson, and Robert F. Turner (Durham, NC: Carolina Academic Press, 1990), 433.

[5]Canada, Department of National Defence, Chief of the Defence Staff, B-GG-005-004/AF-010, *CF Information Operations*, 14 Apr 1998, 1-6.

[6]*Ibid.*, 1-7.

[7]*Ibid.*, 3-5–3-7.

[8]*Ibid.*, 1-7.

[9]United States, Department of Defense, *Joint Pub 3-13, — Joint Doctrine for Information Operations*, 9

October 1998, GL-5.

[10]Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Falls Church: Aegis Research Corporation, 2000), 29.

[11]Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) web site, "Who We Are," <http://www.ocipep.gc.ca/whoweare/indexe.html>, accessed 2 March 2002.

[12]OCIPEP places all products produced for the public on their web site. Based on an analysis of the 2001 and 2002 notices posted as of 2 March 2002, 31 of 33 Advisories, 8 of 9 Information Notes, 7 of 7 Alerts, and 0 of 1 Other Analytical Products were devoted to items related to cybernetic threats, vulnerabilities and activities.

[13]Judith Bax, "Office of Critical Infrastructure Protection and Emergency Preparedness Mandate and Responsibilities," National Security Studies Course, Canadian Forces College, Toronto, 17 Apr 2002.

[14]CEI Computer Economics web site, "Malicious Code Attacks Had $13.2 Billion Economic Impact in 2001," <http://www.computereconomics.com/article.cfm?id=133>, accessed 15 Mar 2002.

[15]The Government of Canada's Government On-Line (GOL) initiative is directed at providing Canadians with a more accessible, responsive service from Government organizations. While DND provides few services directly to Canadians, the need to adapt the Department's business services, such as financial information services for employees, contracting for goods and services, and e-commerce, requires the interconnectivity of our common unclassified information services to the Internet.

[16]'Script kiddies' is a term that refers to "people with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems," as defined in *The On-line Jargon File*, version 4.3.1, 29 Jun 2001, <http://www.tuxedo.org/~esr/jargon/html/entry/script-kiddies.html>, accessed 29 Mar 2002.

[17]'Hacktivism' is a term "that refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage." This definition is taken from the on-line paper by Dorothy E. Denning, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, <http://www.cs.georgetown.edu/~denning/infosec/nautilus.html>, accessed 29 Mar 2002.

[18]It was widely reported in the media in 1999 that the United States Department of Defense had been subjected to covert network attacks by Russian sources, dubbed operation "Moonlight Maze" during which unclassified though sensitive information had been accessed. The story, as originally reported in October 1999, can be found in the article "Yearlong Hacker Attack Nets Sensitive U.S. Data Technology" by Bob Drogin in the 7 October 1999 issue of the *Los Angeles Times*.

[19]The Canadian Forces Information Operations Group (CFIOG), formed in 1998, has, as one of its mandates, the prevention of and response to computer network attacks. <http://www.dnd.ca/img/info ops/info_ops_e.htm>, accessed 26 Feb 2002.

[20]*Communications Security Establishment* web site, "About CSE," <http://www.cse.dnd.ca/en/about cse/about_cse.html>, accessed 13 Mar 2002.

[21]*Canadian Security Intelligence Service* web site, "The CSIS Mandate," <http://www.csis-scrs.gc.ca/eng/backgrnd/back1_e.html>, accessed 26 Feb 2002.

[22]Canada, Department of National Defence, Minister of National Defence, *1994 White Paper on Defence*, 14.

[23]Canada, Department of National Defence, Director General Strategic Planning, *Strategic Capability Planning for the Canadian Forces*, 13 June 2000, 22.

[24]*Ibid*., 28.

[25]*Ibid*., 28.

[26]*Ibid*., 29.

[27]*Ibid*., 24.

[28]*Ibid*., 24.

[29]*Ibid*., 26.

[30]Vice Admiral Arthur K. Cebrowski, "Network-centric Warfare: An Emerging Military Response to the Information Age," Presentation at the 1999 Command and Control Research and Technology Symposium, 29 June, 1999, <http://www.nwc.navy.mil/pres/

speeches/ccrp2.htm>, accessed 2 March 2002.

[31]Network-Centric Warfare is defined as "an Information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization." In the on-line version of book by David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, <http://www.dodccrp.org/NCW/intro.htm>.

[32]Cebrowski, "Network-centric Warfare," no pagination.

[33]James Mulvenon and Thomas J. Bickford, "The PLA and the Telecommunications Industry in China," *The People's Liberation Army in the Information Age*, edited by James C. Mulvenon and Richard H. Yang (Washington: RAND, 1999), 256–257.

[34]*Ibid*, 183.

[35]Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, *Threat Analysis TAO1-001: Al-Qaida Cyber Capability*, 2 Nov 2001, <http://www.ocipep-bpiepc.gc.ca/emergencies/other/TA01-001_E.html>, accessed 15 Mar 2001.

[36]Chief of the Defence Staff, *An Honour to Serve: 2000–2001 Annual Report of the Chief of the Defence Staff*, 9.

[37]Pascale Combelles Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations*, (Washington: Institute for National Strategic Studies), 1998, 35.

[38]*Cyber War*, Host Steve Kroft, with Bill Triplett, Richard Clarke, Gen John Campbell, Adm Herbert Browne , "Sixty Minutes," CBS, 9 May 2000.

[39]William M. Arkin, "The Cyber Bomb in Yugoslavia", article at washingtonpost.com, 25 Oct 1999, <http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm>, accessed 28 Feb 2002.

[40]David A. Fulgham, "Yugoslavia Successfully Attacked by Computers," *Aviation Week & Space Technology*, 23 Aug 1999, 31–34 .

[41]United States Navy Fact File web site, <http://www.chinfo.navy.mil/navpalib/factfile/aircraft/air-fa18.html>, accessed 29 Mar 2002.

[42]Cost is calculated based on the price for a Category 9, Technical Power Group Unix workstation as quoted in cost estimates on the Public Works and Government Services National Master Standing Offer Computer Acquisition Guide, at <http://computer. pwgsc.gc.ca/unix/reynax/rey 9a-e.cfm>, accessed 4 May 2002.

[43]Chief of the Defence Staff, *An Honour to Serve: 2000–2001 Annual Report of the Chief of the Defence Staff*, 26.

[44]*Ibid.*, 26.

[45]Wesley K. Wark, "The Evolution of Military Intelligence in Canada," *Armed Forces and Society*, 16.1 (1989), 80.

[46]Scott Anderson, "The Evolution of the Canadian Intelligence Establishment, 1945–1950," *Intelligence and National Security*, 9 (1994), 450.

[47]Scott Anderson, in his article "The Evolution of the Canadian Intelligence Establishment, 1945–1950," refers to this facility as a location at which instructors from the British Special Operations Executive (SOE) trained American agents from the Office of Strategic Services (OSS) in espionage and sabotage techniques. Anderson refers readers to the work *Camp X* by David Stafford (Toronto, 1987) for further details.

[48]Wark, 86.

[49]Anderson, 457.

[50]General Charles Foulkes, Memorandum, "A Proposal for the Establishment of a National Intelligence Organization," 22 Dec 1945, RG24, Box 6178, File HQ 22-1-43, Vol 1.

[51]Wark, 92.

[52]On 5 Sep 1945, Igor Gouzenko, a cipher clerk in the Russian Embassy in Ottawa, defected, bringing with him documents that indicated the presence of a Soviet spy ring in Canada.

[53]Anderson, 461.

[54]Communications Security Establishment web site, "About CSE," <http://www.cse.dnd.ca/en/about cse/about_cse.html>, accessed 13 Mar 2002.

[55]Anderson, 466.

[56]Anderson, 465.

[57]Communications Security Establishment web site, "About CSE".

[58]Canada, House of Commons, *Bill C-36 Anti-Terrorism Act*, 37th Parliament, 1st Session 49–50 Elizabeth II (Ottawa: 28 Nov 2001), Art 273.64(1), <http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_3/C-36TOCE.html>, accessed 13 March 2002.

[59]*Bill C-36*, Art 273.61.

[60]*Bill C-36*, Art 273.65(6).

[61]Anderson, 450.

[62]Canada, Department of National Defence, Office of the Judge Advocate General, *B-GG-005-027/AF-021 — The Law of Armed Conflict at the Operational and Tactical Level*, 25 September 2000, 1-1.

[63]United States, Department of Defense, Office of General Council, *An Assessment of International Legal Issues in Information Operations*, 2nd edition, August 1999, 1.

[64]Wingfield, 57–58.

[65]Office of the Judge Advocate General, *B-GG-005-027/AF-021 — The Law of Armed Conflict at the Operational and Tactical Level*, 2-1.

[66]*Ibid*., 2-2.

[67]*Ibid*., 2-3.

[68]*Ibid*., i.

[69]United Nations, *1945 Charter of the United Nations*, Article 2(4), San Francisco, 1945.

[70]*Ibid.*, Article 39.

[71]*Ibid.*, Article 51.

[72]Letter from Daniel Webster to Lord Ashburton (6 Aug, 1842), quoted in the article by Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999), 885–937, p 22. This letter refers to the *Caroline* incident, in which during insurrections in Canada in 1837, the British crossed the Niagara River into Schlosser, New York, to sink the boat *Caroline* that was being used by insurgents to cross back and forth. This action was deemed as self-defence by the British, but Daniel Webster, in his response to the British, outlined the now accepted principles, quoted above, by which the concept of anticipatory self-defence could apply. After WW II, the Nuremberg Tribunals spoke approvingly of the *Caroline* standard proposed by Webster.

[73]Schmitt, 22.

[74]Schmitt, 8.

[75]Parks, 433–434.

[76]Parks, 433.

[77]*1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land*, Article 29, contained in the Department of National Defence collection *B-GG-005-027/AF-022 — Collection of Documents on the Law of Armed Conflict*, 25 September 2000, 5– 10, 8.

[78]Office of General Council, *An Assessment of International Legal Issues in Information Operations*, 43.

[79]1944 Convention on International Civil Aviation (61 Stat, T.I.A.S. 1591 15 U.N.T.S. 295, 3 Bevans 944), Articles 1 and 2, as quoted in Parks, 439.

[80]Wingfield, 96.

[81]Parks, 439.

[82]Wingfield, 354.

[83]Department of Defense, *Joint Pub 3-13, — Joint Doctrine for Information Operations*, GL-5. While discussion of CNA activity is contained within the CF IO doctrine, it is not formally defined. This will occur in the CF IO Policy document, due for formal release in the near future. It is expected that the definition will be very similar to this US Joint definition.

[84]Office of General Council, *An Assessment of International Legal Issues in Information Operations*, 16.

[85]Wingfield, 169. Note that the use of perfidy — killing, injuring or capturing an enemy — is considered illegal under Article 37 of the 1977 Protocol Ad-ditional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I).

[86]Robin Neillands, *In the Combat Zone: Special Forces Since 1945* (London: Orion, 1977), 320.

[87]United States, Joint Chiefs of Staff, *Joint Pub 3-05 — Doctrine for Joint Special Operations*, 17 April 1998, I-1.

[88]*Joint Pub 3-05 — Doctrine for Joint Special Operations*, II-3–II-11, contains nine principal missions for special operations forces. In addition, SOF can be tasked to participate in seven other collateral activities, normally performed by the regular military services, including Coalition Support, Combat Search and Rescue, Counterdrug Activities, Countermine Activities, Foreign Humanitarian Assistance, Security Assistance, and other Special Activities.

[89]As a point of note, clandestine operations are not synonymous with covert operations. In clandestine operations, the objective is to conceal the existence of an operation, while covert operations conceal the identity of the operation's sponsor. However, some special operations can be both clandestine and covert.

[90]*Joint Pub 3-05 — Doctrine for Joint Special Operations*, I-4.

[91]Canada, Deputy Chief of the Defence Staff, *CANFORGEN 013/02 DCDS 033*, Unclassified Recruiting Message, 191443Z FEB 02.

[92]Canada, Standing Committee on Procedure and House Affairs, Transcript *Committee Evidence*, 37th Parliament, 1st Session, Number 046, February 20, 2002. 1700–1705 hrs, Wednesday, February 20, 2002, 37th Parliament, 1st Session. <http://www.parl.gc.ca/InfoComDoc/37/1/HAFF/Meetings/Evidence/HAFFEV48-E.htm>, accessed 22 March 2002.

[93]David Pugliese, a journalist with the *Ottawa Citizen*, has written the book *Canada's Secret Commandos: The Unauthorized Story of Joint Task Force Two*, purported to be based on interviews with military personnel and previously classified documents. In this book he highlights JTF 2's Direct Action and Special Reconnaissance missions in Bosnia (pp 45–47), and Foreign Internal Defence Missions in Haiti (pp 59–60).

[94]*Joint Pub 3-05 — Doctrine for Joint Special Operations*, II-11.

[95]*Ibid.*, II-5.

[96]*Ibid.*, II-5.

[97]United States, Joint Chiefs of Staff, *Joint Publication 4-09 – Joint Doctrine for Global Distribution*, 14 Dec 2001, GL-12.

[98]*Joint Pub 3-05 — Doctrine for Joint Special Operations*, II-3.

[99]*Ibid.*, II-3.

[100]Denial of Service (DoS) attacks are numerous in method and approach. The Computer Emergency Response Team Coordination Center, a security monitoring organization from Carnegie Mellon University (CERT CC) generically describes them as "an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include attempts to 'flood' a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, and attempts to disrupt service to a specific system or person." <http://www.cert.org/tech_tips/denial_of_service.html#1>, accessed 29 Mar 2002.

[101]*Joint Pub 3-05 — Doctrine for Joint Special Operations*, II-1.

[102]*Ibid.*, II-2.

[103]Neillands, 7.

[104]System dependence analysis encompasses a very broad field of study that focuses on the analysis of the multitude of interrelationships between information system components. Dependence analysis research being conducted by Judith A. Stafford, Debra J. Richardson, and Alexander L. Wolf, for example, focuses on "dependence relationships at the architectural level [that] arise from the connections among components and the constraints on their interactions." Study of these methods for exploitation purposes will form an important part of developing CNA system exploitation. Further detail on the research of Stafford, Richardson and Wolf can be found in their paper *Architecture-level Dependence Analysis for Software Systems*, at <http://www.cs. colorado.edu/users/serl/papers/aladdin-rosatea.pdf>, accessed 29 Mar 2002.

[105]The CFITES model provides a structured management model that can assist in accurately and efficiently determining training needs and delivery methods. This model incorporates a Quality Control System to ensure that what individuals learn meets the requirements of the tasks and duties that need to be performed. In addition there is a Quantity Control System component to ensure that the training and education are provided to the right individuals at the right time, for the right cost. More information on CFITES is available in the CF publication *A-P9-000-*

001/PT-000 Manual of Individual Training and Education, Vol 1 — Canadian Forces Individual Training and Education System Introduction/Description, 31 May 1994.

[106]*Canadian Forces Information Operations Group*, Information Protection Centre, letter 1000-16 (IPC4-4), *Information Protection (IP) Training and Awareness Requirements Project — Requirement for Insertion of "IP Basic Principles" at CF Entry Level Training*, November 2001, 1.

[107]Canada, Department of National Defence, Assistant Deputy Minister (Human Resources — Military), Message 102/98 ADM(HR-Mil) 066, *Joint Task Force Two (JTF2) Personnel Selection 98/99*, 06 Oct 1998.

[108]*Joint Pub 3-05 — Doctrine for Joint Special Operations*, III-1.

[109]*Ibid.*, III-5.

[110]Transcript, *Committee Evidence*, 1640–1645 hrs.

[111]The US SOF number over 45,000 personnel.

[112]Quoted in H. Eves, *Return to Mathematical Circles*, edited by Prindle, Wever and Schmidt (Boston), 1988. <http://math.furman.edu/~mwoodard/ascquotp.html>, accessed 15 Mar 2002.