INFORMATION WARFARE
AND THE CANADIAN FORCES

Document No. 1350-004-D001
Ver: 1, 9 May 1996

Public Works and Government Services Canada
Contract No. W2213-4-4723/04-QE
Requisition No. 846495RAB93

Prepared for:
LCdr R Garigue
SITS/ADM(DIS)

Mr. T Romet
DGInt/J2 Scientific and Technical

National Defence Headquarters
MGen George R. Pearkes Building
Ottawa, Ontario
K1A 0K2
EXECUTIVE SUMMARY

“Information Warfare” (IW) - defined in this paper as the preservation of one’s own information and information system while exploiting, disrupting or denying use of an adversary’s information and/or information system - represents a new entry on the spectrum of conflict that spans economic, political, social and military dimensions of war.

New operational concepts embodying Information Technology (IT) have introduced new terms and changed the meanings of existing terms. The potential for misunderstanding IW concepts and their implications is very real. The term “Information Warfare” originated in the US military environment and initially conveyed a precise meaning to the military persons using it. Unfortunately, popularized usage of the term now conveys a broad range of meanings to a world audience of military and business professionals now dependent on IT. The situation is made more complex by historical and current use of terminology in the Electronic Warfare (EW) and Command and Control (C2) domains of allied military forces.

IW that targets an enemy's military command, control, communications and intelligence (C3I) capabilities and protects one’s own C3I is called “Command and Control Warfare” (C2W). C2W is a key military component of Information Warfare, but to apply current C2W doctrine fully requires a review of its implications on Policy, Doctrine, Concept of Operations, Organization, Personnel, and Technology and Tools.

Policy
There are IW implications on Policy at the national level that involve DND and also implications internal to DND/CF that need to be examined and clarified.

Doctrine
The current C2W Doctrine needs to be re-examined as a result of the new dimensions that IW brings to the battlefield. Current doctrine does not address a number of critical issues.

Concept of Operations
A new and perhaps a radical change will be required in terms of a Concept of Operations that includes both offensive and defensive C2W.

Organization
The Organization required to support C2W can evolve from existing organizational units but will require a change in the current scope of their organizational mandate.

Personnel
The availability of suitably qualified Personnel to take on the challenges of C2W operations in an IW context is perhaps the most challenging aspect for the CF. The skills are not readily available either in the military or in industry and no recognized training is available to address the shortfall.

Technology and Tools
Finally, the Technology and Tools are for the most part available, at least conceptually. What is missing are the domain experts who can develop and tailor the
applications for CF operations.

The challenges identified in this paper for the C2W community are just the beginning. There are potentially even greater ramifications for organizations that interact with the C2W community.
**TABLE OF CONTENTS**

LIST OF FIGURES............................................................................................................. iv

1 INTRODUCTION..................................................................................................1

1.1 PURPOSE.............................................................................................................. 1

1.2 SCOPE................................................................................................................... 1

1.3 DOCUMENT ORGANIZATION........................................................................... 1

1.4 BACKGROUND....................................................................................................1

2 HISTORICAL PERSPECTIVE.............................................................................. 4

2.1 GENERAL............................................................................................................. 4

2.2 ADVANCE OF TECHNOLOGY........................................................................... 4

2.3 EMPLOYMENT OF TECHNOLOGY................................................................... 5

2.4 CONVERGENCE..................................................................................................6

3 THE INFORMATION SOCIETY.......................................................................... 8

3.1 GENERAL............................................................................................................. 8

3.2 THE INFORMATION WORLD............................................................................. 8

3.3 GENERIC DECISION-MAKING PROCESS....................................................... 14

3.4 MILITARY DECISIONS IN THE INFORMATION WORLD......................... 27

3.5 VULNERABILITIES, THREATS AND RISKS................................................... 33

3.6 JURISDICTIONAL AND LEGAL ISSUES......................................................... 37
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>MILITARY OPERATIONS IN THE INFORMATION SOCIETY</td>
<td>42</td>
</tr>
<tr>
<td>4.1</td>
<td>GENERAL</td>
<td>42</td>
</tr>
<tr>
<td>4.2</td>
<td>TYPES OF INFORMATION WARFARE</td>
<td>42</td>
</tr>
<tr>
<td>4.3</td>
<td>INFORMATION WARFARE CONCEPTS</td>
<td>43</td>
</tr>
<tr>
<td>4.4</td>
<td>COMMAND AND CONTROL WARFARE</td>
<td>45</td>
</tr>
<tr>
<td>5</td>
<td>IMPACT ON THE CANADIAN FORCES</td>
<td>51</td>
</tr>
<tr>
<td>5.1</td>
<td>GENERAL</td>
<td>51</td>
</tr>
<tr>
<td>5.2</td>
<td>POLICY</td>
<td>51</td>
</tr>
<tr>
<td>5.3</td>
<td>DOCTRINE</td>
<td>52</td>
</tr>
<tr>
<td>5.4</td>
<td>CONCEPT OF OPERATIONS</td>
<td>53</td>
</tr>
<tr>
<td>5.5</td>
<td>ORGANIZATION AND FACILITIES</td>
<td>54</td>
</tr>
<tr>
<td>5.6</td>
<td>PERSONNEL</td>
<td>55</td>
</tr>
<tr>
<td>5.7</td>
<td>TECHNOLOGY AND TOOLS</td>
<td>55</td>
</tr>
<tr>
<td>6</td>
<td>RECOMMENDATIONS</td>
<td>58</td>
</tr>
<tr>
<td>6.1</td>
<td>GENERAL</td>
<td>58</td>
</tr>
<tr>
<td>6.2</td>
<td>POLICY</td>
<td>58</td>
</tr>
<tr>
<td>6.3</td>
<td>DOCTRINE</td>
<td>59</td>
</tr>
<tr>
<td>6.4</td>
<td>CONCEPT OF OPERATIONS</td>
<td>60</td>
</tr>
<tr>
<td>6.5</td>
<td>ORGANIZATION</td>
<td>61</td>
</tr>
<tr>
<td>6.6</td>
<td>PERSONNEL</td>
<td>62</td>
</tr>
</tbody>
</table>
6.7 TECHNOLOGY AND TOOLS................................................................. 62
ANNEXES

A  Acronyms
B  Glossary
C  Bibliography
D  Individuals with Input to Report
LIST OF FIGURES

Figure 1 - Convergence in the Information World................................................................. 7
Figure 2 - Information Environments (GIE and MIE).......................................................... 10
Figure 3 - Integrated Information Environment.................................................................. 12
Figure 4 - Simple Decision Process..................................................................................... 15
Figure 5 - The OODA Loop................................................................................................. 17
Figure 6 - Information Domain [TAFIM].......................................................................... 18
Figure 7 - Decision System Layers..................................................................................... 23
Figure 8 - Physical Layer as a Network............................................................................. 24
Figure 9 - Logical Layer Virtual Network......................................................................... 25
Figure 10 - Threats to Information Systems..................................................................... 35
Figure 11 - National and Economic Security Infrastructure Components..................... 44
INFORMATION WARFARE
AND THE CANADIAN FORCES

1 INTRODUCTION

1.1 PURPOSE

The purpose of this report is to initiate discussion and further study of the subject of Information Warfare (IW) in the context of the Canadian Forces (CF) and the Department of National Defence (DND). This paper is also intended to provide initial direction and identify reference materials for the development of IW policies, procedures and doctrine.

1.2 SCOPE

The discussion in this report has been limited to the impact of IW on the CF with respect to Joint Operations. It is not intended to address IW interoperability among government departments, except as it may affect CF activities. It offers an initial functional analysis and recommendations, but does not attempt to extend this review into a complete analysis of organizational requirements.

1.3 DOCUMENT ORGANIZATION

In addition to this Introduction section, this report is arranged into the following sections and annexes:

2 Historical Perspective
3 The Information Society
4 Operations in the Information Society
5 Impact on the CF
6 Recommendations
Annexes:
A - Acronyms and Abbreviations
B - Glossary
C - Bibliography
D - Individuals with Input to the Report

1.4 BACKGROUND

1.4.1 Canadian Context
On 27 September 1995 the Information Highway Advisory Council presented its final report [RELEASE, KNECHT] (References are listed in Annex C) to Industry, Trade and Commerce Minister John Manley. The document contains more than 300 recommendations to assist the Government in development of a Canadian strategy for the Information Highway. Its recommendations deal with issues ranging from access to competition, and from privacy to support for Canadian content and culture in the information age.

The report identifies nine themes which capture the substance of the Council’s recommendations:

a. fair and sustainable competition as the driving force behind the Information Highway;
b. the urgency of building Canada's connections to the Highway;
c. the importance of promoting Canadian culture and content;
d. the enabling effect of the Highway throughout the economy;
e. research and development as the key to innovation, productivity and growth;
f. the importance of making essential Highway services as accessible as telephones and televisions are today;
g. the need to create a learning culture;
h. the requirement for strategic investments in Information Highway applications in the health and education sectors; and
i. the need to protect the rights of individuals in the information society, especially in the areas of privacy and security.

The Information Highway is a portent of social transformation. The Council believes that IT must enable Canadians, as individuals and as a society, to use technology for their individual and collective benefit. To do so, Canadians must become the agents of change.

The government of Canada is therefore setting the stage and the expectations of Canadians. The Internet, as now supported by national policy, has created an unprecedented demand for instantaneous information exchange in the military, government and private sectors. Information networks and computers connected to the Internet are routinely processing private (personal), proprietary (business) and sensitive (military) information. Our economic base and our military effectiveness may be more dependent on automated information systems than those of almost every other country in the world. However, the very technology that promises so much potential has resulted in an infrastructure that is fundamentally insecure to attacks from individuals, groups or nation-states which could easily deny service to or compromise integrity of military command and control systems.

Information should be recognized as a strategic resource which must be effectively managed
to maintain a competitive advantage. Timely and adequate information expands the range of options available to the planner or decision maker. Because of the critical role information plays in reducing uncertainty, structuring complexity and generating greater situational awareness, any action taken in the information domain can exert considerable leverage in the physical domains (e.g., resources such as material, personnel and finance) and the abstract domains (e.g., belief systems) [GARIGUE95].

Raw data in electronic format is becoming more available, driving the development of increasingly powerful computational systems and processes to handle the data and create from it useful information. In turn, these powerful new Information Technologies (IT) permit completely new forms of military endeavours that will require new organizations, activities, skills and mandates.

1.4.2 Military Context

New operational concepts embodying IT have introduced new terms as well as given new meanings to existing terms. The term "Information Warfare" originated in the US military environment and initially conveyed a very precise meaning to the small group of military professionals who were using it. Unfortunately, the popularized usage of the term now conveys a broad range of real and imagined scenarios to a worldwide audience of military and business professionals now dependent on IT. The situation is made more complex by the historical and current use of terminology in the Electronic Warfare (EW) and Command and Control (C2) domains of allied military forces. There is real potential for misunderstanding fundamental IW concepts and their implications.

The CF needs to address IW issues, originally identified by the US military, within the Canadian context. The initial step in such a process is to define the terminology to be used and the conceptual framework within which CF requirements may be analyzed.
2 HISTORICAL PERSPECTIVE

2.1 GENERAL

The conditions that brought about the emergence of IW are generally the result of technological advances since the middle of the last century, and their employment. They and their uses are discussed in this section.

2.2 ADVANCE OF TECHNOLOGY

2.2.1 Communications

Electronic communications have extended the range over which timely information can be exchanged far beyond the "earshot" and "eyesight" limits which constrained previous activities. First wire, and more recently wireless, wideband copper cables and optical fibres have progressively increased the number of channels, the bandwidths of media and their channels, and the types of circuits (eg, satellite relay, cable television and direct broadcast television). The world of communications has in consequence greatly expanded in terms of options, complexity, importance and criticality.

2.2.2 Sensors

Information is now derived in large part from non-human sensors. Radio, radar, infrared/electro-optics (IR/EO), video and synthetic-aperture radar exploit both active and passive technologies throughout the acoustic and electromagnetic spectra and their time domains. Resolution of data is now very fine-grained, pushing data rates up, and physical phenomena are digitally represented in real time. At the same time countermeasures have been developed to mask, deceive and hide objects of interest, increasing the complexity of data acquisition.

2.2.3 Computers

Hardware and software developments have advanced generally in parallel. Hardware power has been increased, while size and cost have gone down: the computing capacity that once occupied a large room and larger budget is now available on the desktop at consumer prices, software capabilities have increased, large scale databases (terabytes - $10^{12}$ bytes) are available, and the field of artificial intelligence has emerged. These developments have enabled the integration of knowledge-based systems with everyday information-system environments. Intelligent component systems (eg, routers, gateways, and financial and stock trading systems) are building on communication technology (eg, local-, metropolitan- and
wide-area networks (LANs, MANs and WANs)).
2.3 EMPLOYMENT OF TECHNOLOGY

2.3.1 News Media

News agencies now cover the globe on a 24-hour-a-day, seven-days-a-week basis, and are equally accessible by the world’s population. Live video imagery was provided to the world’s television audiences, for example, during the Gulf War in 1991.

2.3.2 Quasi-News/Telemarketing

Many news media have carried reporting to the editorial level, offering their versions of the news and propagandizing their consumers. The film “Forrest Gump” demonstrated the art of news manipulation by juxtaposing the adult actor Tom Hanks with notables such as US President JF Kennedy, who died when Hanks was seven years old.

2.3.3 Internet

Some thirty years ago the RAND Corporation proposed a nuclear-survival network using individually unreliable or vulnerable elements interconnected so that system capability and functionality would be survivable. All nodes would communicate in peer-to-peer fashion, each having the right to originate, pass and receive messages, without central control. Messages would be divided into packets, each separately addressed, each beginning at a source node and ending at a destination node, and each wending its way through the network on an individual basis, with the total message being reconstructed in sequence at the end of the trip. If a node failed, the remaining nodes in the network would find another route, bypassing the failed node. This structure became the foundation of the Defense Advanced Research Projects Agency (DARPA, later ARPA) net (DARPAnet), which over time became the Internet.

The Internet has become a very popular information source and communication channel (eg, electronic mail (E-mail), USENET, WWW) for all manner of users. It has proved difficult, if not impossible, to exercise control over the information. The content of print and television is much easier to control - there are relatively few producers and the audience is passive - whereas on the Internet everyone is both a producer and a consumer.

The thirst for information on the Internet overrides concern for security and integrity of the information and reliability of the source. Reasonable precautions are not taken by users anxious to explore and exploit this novel resource. Consequently, personal and business information and even sensitive Defence data are opened to interception, distortion and theft, and the integrity of the information must be regarded as questionable.
2.3.4 **Electronic Commerce**

IT has invaded the field of commerce. Banks make their profits not by storing money but by storing and moving information about money, and they need IT to do so. Their automated teller machines serve the needs of banks and bank depositors so well that the few (expensive) errors are considered acceptable. Shoppers are able to satisfy retailers with electronic "tender" rather than legal (paper) tender. Funds are transferred electronically, replacing paper instruments such as cheques and vouchers. Stocks and bonds are no longer actually "held;" ownership is represented only by an entry in an electronic accounting system. The commerce of Canada (and of DND) is now heavily dependent on the privacy and accuracy of the Internet and its commercial equivalents.

2.3.5 **Government Usage**

The governments of Canada (federal, provincial and municipal) and their agencies (eg, Canadian Police Information System) also rely on IT and electronic data communication. Some official applications are protected, but the majority are unguarded from deliberate and accidental compromise. For example, the CF order of battle may be sensitive in certain respects, but logistic supply orders could reveal the existence and locations of units through unclassified (and unprotected) transactions. In addition, many government authorities have access to domestic and foreign print, radio and television media, and could inadvertently reveal sensitive data to distribution systems having worldwide access.

2.4 **CONVERGENCE**

The following diagram [STEWART95] displays succinctly what is happening in the information world as communication and information technologies advance. The transport media (communications), IT (processes) and data content (knowledge) are converging and their interfaces are evolving. The mail services of the past are rapidly becoming mostly networks, and are progressing to become agents of intelligence networks. The paper medium - the interface of data and communications - is yielding to “twisted pair” and, ultimately, cable as data exchange converts to the electronic media. File cabinet storage space has to a large extent yielded prominence to magnetically stored databases, which will inevitably be supplanted by “knowledge bases” - a drastically new form of information storage that could enfold computers, audio data and video information in compact discs, hard discs and tapes. IW must take cognizance of these developments for both protection and exploitation purposes.
3 THE INFORMATION SOCIETY

3.1 GENERAL

This section addresses IT terminology, considers IW doctrine as it is evolving in the US and Canada, and describes the environment in which the CF must apply joint C2W.

3.2 THE INFORMATION WORLD

3.2.1 General

Concerted study of the field of Information Warfare has only relatively recently begun, and different models and opinions abound. The terms and definitions needed to discuss the issues are not yet stable. A study of the IW world must therefore begin by defining some of the current terminology concerning various information environments and their supporting information infrastructures. For a fuller discussion, please refer to [INFO OPS 95], [NDIMP95] and [BROWN95].

Because Canadian and US military forces endeavour to cooperate in their doctrines and strive for commonality, their terminologies must be compared. Where appropriate, comments are provided on the application of the US definitions in the Canadian context. While US terminology seems generally applicable, there is important Canadian IT terminology - not specifically directed at IW - that is addressed here in keeping with the purpose of this report.

3.2.2 Information Environments

3.2.2.1 Global Information Environment

The Global Information Environment (GIE) is defined as:

Individuals, organizations or systems outside the sphere of military or National Command Authority control that gather, process and disseminate information to national and international audiences [INFO OPS 95]. The GIE neither controls, nor is controlled by, the Military Information Environment (MIE - see below) and is separate and distinct from it, but it encompasses the MIE and frequently provides the media for military communications, deception, etc.

All operations take place within this GIE. It is interactive and pervasive in its presence and influence. Current technology allows any aspect of military operations to be made known to a global audience in near-real time. In some cases this information can be distributed...
commercially faster than by government or military means (e.g., “live” audio and video reports of the Gulf War operation Desert Storm).

Currently, the most influential players in the GIE are the news media, both objective and editorial, which may or may not be pursuing their own agendas. The number of news organizations and their ability to gather, process and disseminate information is increasing exponentially. The effect of media coverage, both domestic and international, can influence strategic direction and the range of operations of a military force. Some of the other players in the GIE are:

- Other Government Departments (OGDs) or Agencies;
- Non-government Organizations (NGOs);
- Private Volunteer Organizations (PVOs);
- International agencies that coordinate international efforts such as the Red Cross, World Health Organization (WHO), etc;
- International agencies or consortiums providing commercial services or products such as the European Space Agency (ESA);
- Cultural organizations and influences such as religious movements and leaders;
- Allied and adversary military and intelligence services; and
- Individuals with appropriate hardware and software to communicate with a worldwide audience, through the Internet for example.

3.2.2.2 Military Information Environment

Within the GIE exists the Military Information Environment (MIE), which includes those players important to military operations.

The Military Information Environment (MIE) is defined as:

> The military environment contained within the GIE, consisting of information systems and organizations - friendly and adversary, military and non-military - that support, enable or influence military operations [INFO OPS 95].

The MIE extends:

a. in space, from home station to the Area of Operation (OA);
b. in time, from alert through redeployment;
c. in purpose, from tactical missions to economic or social end-states; and
d. in people, from deployed soldiers and families at home to local or regional...
populations and global audiences [INFO OPS 95].

Similarly, one could define other, “special interest” sub-environments within the GIE (eg, a Financial IE (FIE) that would be concentrated on banks, stock markets, the flow of investments.

The GIE and MIE can be visualized as shown in Figure 2 (adapted from [INFO OPS 95]).

![Diagram of the Global and Military Information Environments](image)

3.2.2.3 Integrated Information Environment

The Integrated Information Environment (IIE) may be defined as:

a seamless, robust, multimedia infrastructure, enabling users to access, acquire, process and exchange information from anywhere, at any time and in whatever required form, according to need and authority. The baseline structure is hierarchical on the principle that a user’s information requirements build from his local realm, and spread and extend beyond local and regional boundaries to national and international horizons [NDIMP95] [BROWN95].

The major elements comprising the IIE (shown in Figure 3) are:

---

Doc No: 1350-004-D001     Ver: 1     Date: 9 May 1996     Page 11 of 63
a. **Environment Shaping Instruments.** Policies, doctrine, architecture, standards models, repositories, configuration management utilities and information management (IM) tools that permit the flexible development, administration and enhancement of elements within the IIE without violating the IIE’s overall integrity.

b. **The Information Universe.** The totality of all information existing in various information domains such as operations, intelligence, finance, materiel, etc., which may be held in a variety of holdings internal and external to DND/CF, part or all of which can be made available to commanders, managers and their staff.

c. **Information Holdings.** A subset of the information universe. Information can be held in and drawn from a variety of holdings which can be controlled by individuals, organizations, processes or systems.

d. **Information Technology Infrastructure (ITI).** The set of tools that support automation of IM. (See the next section for amplification.)

e. **The User’s Infosphere.** The personal subsets of the IIE that Defence users will need to create and manage in order to accomplish their missions and tasks in the assigned area of operations or management domain. Conceptually it can be thought of as a virtual, single window into the universe of information which provides the user with a real-time, integrated picture of the information required by the user, whether the user is in the office or on the battlefield [NDIMP95] and [BROWN95].
A few comments are necessary to compare and contrast the three Information Environments just described. The IIE, in keeping with [NDIMP95] objectives for IM, includes an underlying theme of *information that is needed or wanted*, and concepts for providing and organizing that information. On the other hand, the GIE and MIE in the context of IW, include all information and players. The IIE, as a *support* tool for DND/CF, would possibly be subject to *attack* from an IW perspective. Continued development of the IIE should be carried out with a heightened awareness of the threats and risks of various types of attack activities that may be encountered.
3.2.3 Information Infrastructures

Information Infrastructures provide the procedural and technical support to the information environments needed to ensure delivery and dissemination of the information.

3.2.3.1 Global Information Infrastructure

To support the GIE, there exists a Global Information Infrastructure (GII):

an interconnection of communications networks, computers, data bases and consumer electronics that puts vast amounts of information at the user’s fingertips. The GII includes more than just the physical facilities used to store, process and display voice, data and images. It encompasses a wide array of ever-expanding capabilities including cameras, scanners, keyboards, fax machines and much more [INFO OPS 95].

In short, the GII electronically links organizations and individuals around the globe, and is characterized by a merging of civilian and military information networks and technologies.

3.2.3.2 National Information Infrastructure

Within the GII, each nation has access to a National Information Infrastructure (NII):

a series of components, including the collection of public and private high-speed, interactive, narrow and broadband networks. It is the satellite, terrestrial and wireless technologies that deliver content to home, businesses and other public and private institutions. It is the information and content that flows over the infrastructure in the form of databases, the written word, television, computer software, etc. It is the computers, televisions and other products that people employ to access the infrastructure. It is the people who will provide, manage and generate new information, and those that help others to do the same. The NII is a term that encompasses all these components and captures the vision of a nationwide, invisible, seamless, dynamic web of transmission mechanisms, information appliances, content and people. The global accessibility and use of information in the NII is especially critical given the increasing globalization of markets, resources and economies [INFO OPS 95].

In practice, the GII and NII labels are misleading, as there are no discrete boundaries in the information environment. Note, however, that all elements of the NII need not necessarily be controlled nationally. For example, the communication requirements of far-flung diplomatic
or commercial operations may be carried by systems (communication satellites, trans-oceanic telecommunication cables, etc.) belonging to other nations or commercial organizations.

The NII and GII are all inextricably intertwined, and this trend will only intensify with the continuous application of rapidly advancing technology. This worldwide telecommunication web transcends industry, media and the military, and includes both government and non-government entities.

Although it uses much of the GII, the NII may be more easily considered to consist of those GII elements of national importance when viewed from the national perspective.

### 3.2.3.3 Defence Information Infrastructure

The Defence Information Infrastructure (DII) encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval and display. Under ideal conditions, the DII provides defence mission support, command and control, and intelligence computers to users through voice, data imagery, video and multimedia services [INFO OPS 95].

### 3.3 GENERIC DECISION-MAKING PROCESS

### 3.3.1 General

The ultimate role of information is to provide a basis on which judgements and decisions can be made. We discuss a model for the process by which decisions are made, and a general structural view applicable to systems supporting the process.

### 3.3.2 A Decision Process Model

A decision system is analogous to a simple closed-loop control system, wherein the desired state is compared to the current state and the resulting "error" is used to apply some form of correction to the controlled system, ideally bringing it into closer alignment with the desired state. Such a control system would normally continually monitor the current state and apply correction until (if a stable control system) the error between the desired and actual states is zero.

In terms related to a decision system, the current state is sensed through the acquisition of data describing the state. Various types of processing may be applied to the data in order to create information, knowledge and understanding upon which plans and options can be based. Ultimately a decision is made to carry out some action (which may be no action) designed to
move the "controlled" system from the current state toward the desired state. Figure 4 [INFO OPS 95] shows the "data" relationship used in this paper, from data to understanding and decision, called the Creation of Situational Awareness.

Many different models and representations have been developed to describe decision systems, but all such models include these basic elements:

a. acquire (raw) data;
b. process raw data into increasingly useful information which allows understanding;
c. compare the current state (as understood) to the desired state; and
d. decide on a course of action and implement it.

The data may be acquired through any number of "sensor" technologies (eg, radar, satellite, intelligence assets, news). The process may range from an individual observing a radar display to a complex system of computer and human "nodes" communicating over a global network to analyze large amounts of disparate data in order to provide information to a decision maker. The decision may be to change a range scale setting, commit forces to a military operation or, in a commercial arena, market a product in a particular manner.
Figure 4 also illustrates a number of important concepts related to any decision process.

A Decision Maker's *understanding of his environment* is limited by the quantity and quality of the information available to him at the time a decision is made and *his perception* of the extent of the effect of any action he may decide to have carried out. Note that this does not limit the actual extent of effects from such a decision or action.

*One’s reach may well exceed one’s grasp, even if his sight does not attain his view.*

Implicit in the "definition" provided by Figure 4 is the hierarchical nature of decision processes and the data they manipulate. As the scope of the decision to be made expands (e.g., from platoon commander to corps commander), the input to the process contains less raw data and more interpreted/processed information. For example, the knowledge that an enemy tank is in the forest ahead is of great importance to the platoon commander and will have a significant impact on any decision he may make, but it is of much less significance to the Corps commander. Alternatively, this can be stated as the following principle:

*One man's INFORMATION is another man's DATA.*

An important concept touched on previously is the speed or timeliness with which the processed data makes its way through the processing both horizontally to a local decision maker and vertically up the hierarchy to a remote decision maker. Simply stated:

*Information is perishable.*

Finally, due to the impracticality of collecting complete data describing the current state, the actual processing required to create understanding from the data and the "distance" of the decision maker from the raw environment data, there can be a significant difference between the actual current state and the current state as understood by the decision maker. In addition, if the underlying data is incorrect any conclusion or understanding reached is questionable, if not entirely suspect.

*Just because you believe it, doesn't make it so.*

All of these concepts are important to the discussion as they highlight areas that are susceptible to disruption by properly applied actions in the IW domain — actions which it will be necessary to exploit and against which to defend.

3.3.3 The *OODA Loop*
One model of the *Decision Cycle* features an Observation-Orientation-Decision-Action (OODA) Loop, shown in Figure 5 and described as follows:

a. **OBSERVATION:** The beginning of the OODA Loop and the view of the battlefield. This is the raw intelligence received by the commander’s staff. Observation is only as good as the collectors (the eyes of the commander).

b. **ORIENTATION:** By intelligence analysis of past Observations and biases, the commander knows where he and his adversary are in time and space. The commander then develops a prediction of where the battle is heading, like a boxer positioning himself against his foe.

c. **DECISION:** Based on Observation and Orientation, plans are made based on the decisions of the commander.

d. **ACTION:** In this step the Decisions made by the commander are turned into action. Units are tasked by Decisions. The Action happens when the unit executes the Decision [JC2W SOC 95].

3.3.4 **Generic Information System Structures and Vulnerabilities**

3.3.4.1 **Architecture Overview**

In this Report, the architectural framework for achieving confidentiality and privacy is
separated into two conceptually distinct entities:

a. a concept that segregates information into Information Domains; and
b. a physical implementation of communications and processing components making up an information system that facilitates both local and remote access to the information contained in the domains.

3.3.4.2 Information Domains

Information Domains are comprised of three elements as shown in Figure 6:

a. a specific set of information assets;
b. authorized users of the information; and
c. a security policy governing the use of the information assets.

As an example, the information assets in a domain might be all the tax information the government has collected on a corporation. The authorized users would include specific members of Revenue Canada and the financial officer of the corporation. The security policy specifies how the information will be protected within the government information collection, storage, access, processing, distribution, update and dissolution processes.

3.3.4.3 Information Systems

The extensive array of processing and communications components that will be used in information systems must incorporate security features that satisfy the security policies of the Information Domains. To address this need, the components are divided into two general groups:

a. The Local Subscriber Environment (LSE) is comprised of those technological elements over which an authorized agent of the user community has unambiguous,
direct control both in configuration and use.

b. The Communication Network (CN), in contrast, includes elements upon which the system relies but are not directly or completely controlled by the user or his/her agent. The agent may have partial or shared control, but not full control. Such elements include commercial telephone lines and the Internet. Dedicated telephone lines are considered to be uncontrolled since the actual routing of the communication between the source and destination is not under the user's or his agent's direct and total control.

3.3.4.4 Relationship of Information Domains to Information Systems

Information Domains are distinct from Information Systems. Information Systems are made up of communication equipment, processing equipment and networks; Information Domains are not. Information Domains are not bounded by networks, but rather by the presence of their assigned information assets and specifically authorized users. They may be supported by any information system that can meet the protection and delivery requirements of the Information Domain security policy. Three Information Domains, for example, can be supported by three LSEs on a single communication network, one Information Domain accessible by all three LSEs while the other two could each be accessible by two LSEs.

Information is managed by individuals and groups who create, collect, process, categorize, store, use, exchange and despatch particular information. The value and required protection of that information is determined by the individual or group, likely in accordance with certain laws or policies that apply to the information. Three elements are necessary for this concept to be employed.

a. An individual or group must have a defined membership.
b. Information assets must be uniquely defined within the domain of the group.
c. The security policy regarding protection of and access to the information assets must be known and agreed to by the membership.

3.3.4.5 Information Domain Characteristics

An Information Domain is a set of users, their information assets and a security policy. The Information Domain security policy is a statement of the criteria for membership in an Information Domain and the required protection of the information assets.

Each Information Domain is uniquely identified. The unique identification indicates the sensitivity of all the information assets in the domain. Any security attributes must be the same for all information assets in the domain. However, members of an Information Domain
may have different security-related attributes: some members, for example, may have read and write privileges while others may only have read privileges. Since the security attributes of all assets within a domain must be the same, a user who has read and write privileges will have them for all assets in the domain.

Information Domains may have security policies with unrelated protection requirements. Information systems that support multiple Information Domains must adopt a protection strategy that satisfies all of them. One such strategy, termed strict isolation, is to isolate one domain from another except where an explicit relationship is established. Information systems must provide mechanisms to maintain separation of information in ways that are satisfactory to any domain using the system.

Some operating requirements will necessitate the sharing or transfer of information assets among domains. Inter-domain transfers must be in accordance with the security policies of both domains. The simplest method of sharing information is to accept new members into an existing Information Domain. Where only some information from one or more domains is needed, a new Information Domain may be created to contain the shared information.

When information is copied or moved from one domain to another, audit and traceability trails may have to be implemented - if required by the security policies of the Information Domains involved.

3.3.4.6 Information Domain Security Policy

The security policy of an Information Domain defines the following five areas:

a. Membership requirements.
b. Definition of the Information Assets.
c. Security Services and Strengths required.
d. Interdomain transfer requirements.
e. Security Management requirements.

These policies are used to implement the required level of protection for the information assets of the domain. They can be used to determine what constraints must be placed on information systems that will handle the information assets.

3.3.4.7 Threats

3.3.4.7.1 General
The threats that may be brought to bear on information systems take many forms, few of which are physical. The harm caused by an attack can vary from temporary injection of a hacker’s message into a computer display to total destruction of all data or electronic circuits. The effect therefore ranges from a temporary program delay to loss of all data and the use of an information system. The attacking mechanism can extend its effects to other information systems via data transactions on disc, Internet, etc. Some examples are described below.

3.3.4.7.2 Computer Virus
A computer “virus” is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces.

Viruses include "cruise" viruses that seek and destroy particular data sets, "stealth" viruses that hide themselves from detectors, file infectors and boot-sector viruses. Using operating system software and different utilities, viruses can make a system act upon data in unintended ways (such as clandestinely placing a call with a computer's modem and transmitting data), or they can simply waste processor time. Although viruses can be built which will cause physical damage (eg. commanding a hard disk to thrash itself to destruction), for simplicity all viral attacks are gathered into the Logical category by virtue of the manner in which they are introduced.

3.3.4.7.3 Worm
A “worm” is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually does not modify other programs.

3.3.4.7.4 Trojan Horse
A “Trojan horse” is a code fragment that hides inside a program and performs a disguised function. It could be camouflaged as a security-related tool. SATAN, which is available on the Internet and checks UNIX systems for security holes, but can be modified to help an external hacker obtain unauthorized entry to information systems on which it has been tested.

3.3.4.7.5 Logic Bomb
A “logic bomb” is a type of Trojan Horse, used to release a virus, worm, etc. It could be an independent program or a piece of code, commonly planted within system software by a system developer or programmer.
3.3.4.7.6 Trap Door

A “trap (or back) door” is a mechanism built into a system software by the designer to give him clandestine access into the system, circumventing normal protection and detection techniques such as audit trails.

3.3.4.7.7 Chipping

Computer “chips” (integrated circuits) can be configured by the manufacturer to include some unexpected functions: delayed failure, physical self-destruction, unauthorized emission of detectable signals, etc.

3.3.4.7.8 Nano Machines

Nano machines are robots smaller than ants that, scattered in a target area, find computers and crawl into the hardware, where they shut down electronic circuits.

3.3.4.7.9 Microbes

Microbes have been developed that will consume oil pollutants. They could conceivably be created with an appetite for silicon devices (which comprise most of the active components of a computer), and distributed in computer-occupied areas.

3.3.4.8 Layers of Vulnerability

We can separate the actual structure of an information system into Physical, Logical and Semantic layers based on their functions. This categorization has been useful in collecting, analysing and presenting the ideas contained in this report. The following sections define these layers and give some brief examples of how they may be attacked.

Figure 7 shows the different layers of an Information System structure. On the left is a representation of normal (intended) operation; on the right is a representation of the type of effect that might be experienced after an attack upon each layer.
3.3.4.9 Attacks on the Physical Layer

The Physical Layer represents the physical manifestation of the Information System Structure. The physical manifestations consist of buildings, computers, communication equipment (telephone lines, switches, communications satellites, ground stations, etc.), power distribution systems and supporting personnel. The Physical Layer can be characterized as the "hardware" elements of the Information System.

Figure 8 is a simple representation of the Physical Layer as a *Network*, where the numbered *nodes* in the diagram represent buildings, personnel or computers, and the lettered *links* represent the communication equipment connecting the nodes.
This view of the Physical Layer naturally leads to the concept of analyzing the processing Nodes and communication Links in an Information System Structure.

As a set of hardware, components of the Physical Layer are vulnerable to physical destruction using traditional weapon systems such as missiles, bombs, sabotage, etc. Physical destruction of any such information structure element ensures complete denial of its services.

Included in the class of weapons providing physical destruction, from the Information System point of view, will be new Radio Frequency Weapons, which exploit the susceptibility of electronic components to destruction by high energy Electromagnetic Pulse (EMP) radiation. Such weapons are important because they provide mission-kill without the use of lethal force. An EMP weapon would have handicapped operations at the New York World Trade Center more than the bomb attack.

The fact that an attack has been made against the Physical Layer, and the results of the attack, are normally apparent from a loss of services. This effect is achieved by traditional weapons such as missiles, bombs, sabotage etc. Targetting a network (such as an electrical or telephone grid) for destruction is easy, but a node and net evaluation must be done to cripple the network effectively.

3.3.4.10 Attacks on the Logical Layer

Up one level of abstraction from the Physical Layer is the Logical Layer (also referred to as the Syntactic Layer) (See Figure 9), which represents how the Structure is operated. It generally consists of the software and operating systems of the computers and telecommunication equipment that determine what data are collected, how they are processed into information and (ultimately) knowledge, and how they are distributed throughout the Information System. Included in this layer are the operating procedures followed by system users.

A distinction can also be made between the total system (or installed plant) and those portions necessary for a particular application or providing support to particular functions. For example, it may be appropriate to consider those elements of the Logical Layer used to support departmental Financial Management, the Intelligence function in a headquarters staff, or simply those elements that represent the ITI support for a single user’s infosphere. That naturally leads to the notion of the Logical Layer as Virtual Networks supporting different functions overlaid on the Physical Network (Layer), as shown in Figure.
It is apparent that some nodes and links in the network are used to support more than one function, or represent a possible single point of failure for the functions in question. For example, Node 5 appears in all three functions and Link G appears in two functions; if Link H were severed, the virtual network for Function 2 would be disconnected. Depending on the nature of the functions and the reconfiguration capability of the underlying network, loss of these links and nodes may cause significant disruption to the functions.

Attacks against the Logical Layer seek to interfere with system functions. Such attacks might involve delaying the execution of procedures, misdirecting information, overloading an externally accessible node so it cannot carry out its Information System support activities, or infecting by software viruses.

Externally accessible nodes in the Information System Structure can also be attacked by
"crackers" searching for information, attempting to contaminate the information held by the system or trying to take control of the system. A central theme of IW is that by controlling an adversary's network you can control his awareness and understanding of events, and ultimately his decision-making process. **There is no need to destroy an adversary's systems or data if they are under your control.** In fact, it is to the advantage of the hacker/cracker if the system continues to operate; otherwise he would derive no benefit.

Attacks against the Logical Layer can be more difficult to detect since the system still operates, but not properly. PC users are somewhat used to occasional bouts of erratic behaviour from their systems; so if the Logical Layer attack is carried out in a "non-disturbing" or "non-disruptive" manner it may remain undiscovered for quite some time. In addition, users may not understand what is happening when their systems are operating normally, let alone recognize that "odd" behaviour could be caused by some sort of attack.

3.3.4.11 Attacks on the Semantic Layer

At the highest level of abstraction sits the Semantic Layer, representing the content and interpretation of the information contained within the Information System. It is characterized by the awareness provided to the decision maker, the "trust" accorded to the products of the system and the mental models applied by the users at all levels of the decision-making hierarchy.

The objective of attack on the Semantic Layer is to affect and exploit the trust users have in the information system and the network, and to influence their interpretation of the information it contains. Semantic attacks focus on manipulating, modifying or destroying the mental models - the awareness and representations - that are developed through the use of an information system. Spoofing other peoples’ identities, selective “spamming,” broadcasting specific arguments, discourses, misinformation and slogans, and causing information overload can influence decision makers so they misinterpret what is happening. The attack is quite a challenge; it is the new dimension of what was once termed Psychological Operations (PSYOP) or Deception.

The best way to think about these weapons are as “Memes” or virus of the minds that can be created via the information systems. Trying to recreate a close representation of what exactly is happening in the real world is the most difficult part of conflict management and warfare, but this type of consideration will become more and more central to the Information Warfare debate as Social User Interfaces (SUI) start populating systems.

3.4 MILITARY DECISIONS IN THE INFORMATION WORLD
3.4.1 General

The doctrine and technology described above is considered next in the context of a military environment and the command and control of military forces.

3.4.2 Technology and Organizations

The technology of war does not consist just of instruments intended primarily for waging war. A society's ability to wage war depends on every facet of its technology: its roads, transport vehicles, agriculture, industry and methods of organizing its technology. Behind military hardware is hardware in general; behind that is technology as a certain kind of know-how, of looking at the world and coping with its problems [RAND].

Advanced information and communication systems, properly applied, can improve the efficiency of many kinds of activities, but the new technology is also having a transforming effect for it disrupts old ways of thinking and operating, provides capability to do things differently and suggests how to do things better.

The information revolution challenges the design of institutions. It erodes hierarchies, diffuses and redistributes power (often to the benefit of smaller elements), crosses borders, redraws boundaries of responsible agents and expands space and time horizons; thus it generally forces the opening of systems. But institutions remain essential to organizations. Responsive, capable institutions will adapt their structures and processes to the information age, and evolve from traditional, hierarchical forms to flexible, networked models of organizations.

The information revolution is strengthening the importance of networks (eg, social and communication networks). The information revolution makes it possible for diverse, dispersed agents to communicate, consult, coordinate and operate together across greater distances and with better information than before.

The information revolution will cause shifts, both in how societies may come into conflict and in how their armed forces may wage war - societal-level conflicts (waged in part through internetted nodes of communication) and C2W at the military level. While both revolve around information and communication matters, at a more fundamental level they are forms of war about a society’s or a military’s knowledge of itself and its adversaries.

Combining new technology with old processes may create new inefficiencies while some activities become more efficient. The activity itself, both operationally and organizationally, will need revision in order to realize the full potential of the technology. The accompanying organizational and operational changes may allow for reductions in the overall size of a force.
Benefits of decentralization may be enhanced if, to balance a possible loss of centralization, the high command gains topsight - ie, the view of the overall conflict. This term carries with it an implication that temptations to micro-manage will be resisted.

3.4.3 Command and Control

3.4.3.1 Definition

The term “command and control” (C2) is defined as:

the process by which commanders plan, direct, control and monitor any operation for which they are responsible [JOINT95].

C2 includes decision-making from sparse or conflicting information and acting upon those decisions in a way that best represents the decision-maker’s estimate of the situation and the alternatives [ELLIOT95]. To capitalize on this capability, command, control, communications, computers and intelligence system designers have two approaches from which to choose.

a. They can attack the information-availability problem head-on and try to capture and process as much information as possible; or
b. They can reconcile themselves to information that is incomplete, and orient the system and the decision-maker to coping with uncertainty.

3.4.3.2 The C2 Knowledge Process

The process for developing knowledge can be conceived in several distinct stages.

a. Acquisition, filtering and conditioning of input information to ensure that it represents significant changes or verifications of the real world and not unnecessary or irrelevant information, and also to present it in a form that is suitable for rapid application.

b. Combining information with the user’s knowledge of the situation to clarify, update or confirm knowledge. The information must be projected into a perception model that the user employs to represent his environment or situation. The decision maker will have several alternative perception models, especially when uncertainty is large.

c. As knowledge improves the decision-maker can exercise judgement or intuition with more confidence. He uses the knowledge to enhance his perception.

3.4.3.3 Reasons for Change in C2
The real drivers for C2 decision-making are:

a. the operational situation demands it;
b. an opportunity presents itself along with supporting information for the decision; and

procedure calls for a decision.

Forces in modern warfare move and re-form too quickly for the decision-making processes of the past. Information is provided by many more sensors and in much more detail, arriving over communication systems that are more responsive. Consequently, decisions must be made faster and are required more urgently.

The true measure of effectiveness of a military command and control system is its contribution in enabling the efficient and effective delivery of combat power to bring about a desired end. Data is important, but only if it is accurate, timely and relevant to some decision a commander will make. Data does not equate to knowledge; communication flow does not guarantee effective decision making; hierarchy cannot guarantee effective coordination.

3.4.3.4 Methods of Improving C2

We must decrease the degree to which the commander is in a reactive mode - making obligatory decisions before choosing to do so voluntarily. Major improvements are possible if technology is implemented with a view toward the real decision drivers, and if doctrine, organization, facilities, concepts, procedures and training are adapted to address them.

One way of improving delivery of information and knowledge of the decision-maker is to disseminate information in a form that is easily managed, presented and understood. In many cases the best medium is visual and the best presentation is an image or graphic. Movement away from "information push" toward "user pull" and "smart push" is a significant aspect of the emerging way to improve information exchange.

Current systems are geared to procedures from the past, in which specific types of information are isolated ("stovepiped") into different parts of the staff. Information such as force status, intelligence, weather and logistics are handled as separate "knowledge domains;" it must be integrated either in the decision-maker’s mind or with multiple presentations ("windows"). Emerging technology will enable the decision maker to assemble information from multiple knowledge domains to clarify a situation or problem.

Force deployment and movement plans can be integrated into a situation display. Critical elements of hostile forces can be identified for possible engagement and examined from several perspectives. Analysis simulations can be accomplished faster and integrated more
thoroughly into the overall C2 decision making context.

Commanders require practice to develop the expertise, judgement and intuition for quick and precise decision-making even in the face of uncertainty. The major cognitive abilities are recognition of patterns of knowledge, and correlation of those patterns with judgemental or intuitive understanding of the situation and alternative courses of action. IT can provide the means for that practice.

3.4.4 Factors in Reviewing Military Decision Systems

Today’s “information revolution” offers the potential to form a powerful partnership between information and combat power. Just as three ordinary technologies - the telephone, the television and the computer - are being combined, the critical elements of combat power can be combined so the whole is greater than the sum of the parts. No one completely understands the impact on society of the merger of telephone, television and computer; so it is with the military. It seems, however, that the military potential of the information revolution is on the scale of changes like the invention of gunpowder and the advent of mechanization [KELLY].

The pressure to pursue state-of-the-art information technologies is driven, in part, by the accelerated pace and enlarged scope of military operations. What has changed are the dimensions, sophistication and consequences of warfare.

Achieving a complete revolution in military affairs requires complementary changes in organizational structures, operational strategy and service doctrine.

Information technology is improving so rapidly that perceiving its impact on the more fundamental elements of military command and control is difficult. Technological change is occurring faster than military organizations and doctrine can accommodate it.

The constant flow of new tools for information collection, processing, display and distribution provides the illusion that technology will ultimately alleviate the complexity and uncertainty in operational information that have plagued commanders for hundreds of years. This illusion has heightened expectations and fuelled demand for technical solutions to all problems of command. The reality is that information technology may magnify complexity and uncertainty in operational information.

3.4.5 System Requirements for Military Command and Control

3.4.5.1 The Requirement
Decision-makers must sense the environment, process and evaluate data, choose a course of action, and direct that action. In earlier ages, four of the five steps were entirely sensory and usually embodied in a single person. As the scope and sophistication of combat increased, the number and variety of situations addressed by a commander increased at a much greater rate, eventually exceeding the ability of a single individual to deal with them. The commander could no longer see far enough or exercise his decision cycle fast enough to cope with the increasing size and speed of the battlefield. Instead, he had to rely on input from subordinates operating in parallel, across multiple echelons of command and with several decision cycles other than his own. His effectiveness became dependent on the shared understanding of several commanders, each with different perceptions of the battlefield and the ends to be achieved.

The new view of C2 should acknowledge the dynamic and stochastic nature of warfare rather than emphasize the formal structure of command. The emphasis should be on function, understanding and decision making. This view seems more appropriate given the dramatic increase in the scope, pace, sophistication, lethality and unpredictability of modern warfare.

Military command and control systems must, therefore:

a. support human decision making;
b. reduce uncertainty while acknowledging that uncertainty cannot be eliminated;
c. decrease the complexity of coordinating, integrating and applying cbcm resources;
d. bridge time, space and purpose; and
e. possess flexibility to respond to combat dynamics.

3.4.5.2 Support for Decision Making

Transforming data into information, and ultimately into knowledge and understanding, is a cognitive process performed by human beings.

Decision-making, not information flow, is at the core of the command and control process. Data is not useful until it is aggregated into information and placed in the context of the commander or decision maker.

3.4.5.3 Reduction of Uncertainty

Combat is not a deterministic process - decisions will be made under conditions of stress, fatigue, fear and confusion, and in response to seemingly random events. Any tool that fails to reduce uncertainty in an acceptable amount of time will be useless. Striving to eliminate
uncertainty slows the decision cycle, and history demonstrates seizing the initiative regardless of uncertainty usually provides military advantage that outweighs waiting for perfect information.

3.4.5.4 Decrease of Complexity

Warfare in the future involves numerous objectives and many simultaneous actions conducted over large areas. Emerging information technologies offer powerful abilities to help commanders cope, but are bound to introduce unforeseen vulnerabilities and limitations. From an engineering perspective, each generation’s command and control systems are more complex than its predecessors. Users must understand and tolerate the complexity, but require devices that are simple to understand and operate. Commanders should be comfortable in deriving their perceptions from data collected, interpreted and displayed primarily by electronic means.

Complexity in command and control manifests itself in various ways; one is “information overload” or “saturation.” In addition to saturating human decision makers, the increased volume of data may overload communication and electronic circuits and subsystems, resulting in preemption, delays and lost data. Communication bandwidth has increased exponentially, but the demand for bandwidth has increased faster. Some of the data that consumes capacity is of questionable value. Systems should be designed to serve the decision-maker’s needs and capacity to accept it. Command and control doctrine should be revised to prevent data and information from flowing through systems unnecessarily.

The historic response to information overload has been a growth of staffs; yet information can become more complex as the number of hands it must pass through increases, grows to coordinate their actions and increases uncertainty in the minds of the decision-makers. While formalization and standardization may yield certain advantages of efficiency and compliance, they can also centralize error and bind decision-makers to fixed procedures.

Information saturation adds to the exponential growth in complexity of C2. Complexity, in an engineering sense, is acceptable as long as it is managed and designed to appear transparent to users. Complexity breeds uncertainty, which undermines decision-making. In new designs, interfaces need to be minimal and simple, mechanisms transparent and information flow restricted to essentials.

3.4.5.5 Bridging Time, Space and Purpose

Human decision-makers will continue to play a crucial role despite decreasing response times and the corresponding reduction in decision-making time.
Effective C2 demands mastery of time and space relationships, recognizing the decisive point and bringing combat power to bear at the right place and time. Theoretically, systems that provide sensor-to-shooter information are desired; in practice, sensor-to-shooter connectivity is difficult to achieve. Information rarely moves directly from one to the other; instead, it travels through a variety of data links, command centres and reporting systems. Along the way, the data is processed, filtered, manipulated, correlated, fused and analysed. With each stop, the potential for delay, misunderstanding, misperception and miscommunication increases.

With new technology, data and information can be shared laterally and vertically, across service boundaries, over vast distances, securely and in real time, allowing forces to synchronize actions operationally and tactically. Synchronization at the operational level has always been important because it supports unity of purpose. At the tactical level, synchronization has posed problems. Lacking means of real-time coordination, synchronization has amounted to placing limits on forces by establishing restrictive zones and coordination lines. The practice of limiting movement is driven by a lack, rather than possession, of information.

3.4.5.6 Flexibility

Flexibility is the capacity to adapt to rapidly changing conditions. The goal is to react faster than the enemy, to concentrate strength against his vulnerabilities, and to identify and eliminate own weaknesses before the enemy can exploit them. Flexibility implies more than speed of movement. Battlefield information, placed in the hands of the forces in contact in time to identify key points of decision, enhances their agility and flexibility. Information processing and decision support systems should be placed in the hands of all forces that can make a difference on the battlefield.

In addition, modern C2 systems permit large hierarchical organizations to be streamlined and serial processes to be modified to support parallel and simultaneous operations. Wherever possible, processes and systems should support sensor-to-shooter information flow. While battle management and planning support should be available to field commanders, the process cannot become a pre-condition to action. Time permitting, field commanders will request intelligence and planning support, but C2 systems should not be constrained by inflexible processes or practices. C2 doctrine, procedures and training are needed to ensure C2IS systems and practices do not inhibit the agility and flexibility of forces to respond to rapidly changing circumstances.

3.5 VULNERABILITIES, THREATS AND RISKS
3.5.1 General

As the vulnerabilities of the information infrastructure are identified, those with the tools, and the intent to use the tools, become the threat that must be countered.

Every day, all over the world, computer networks and hosts are being broken into. The level of sophistication of these attacks varies widely; while it is generally believed that most break-ins succeed due to weak passwords, a large number of intrusions use more advanced techniques. Less is known about the latter types of break-ins, because they are much harder to detect.

Russian-organized crime gangs are quickly outpacing the Italian Mafia as the most feared criminals. Unless something is done by law enforcement and private security agencies on a global scale to deter them, they will loot banks, corporations and government agencies of billions of dollars - without using guns or traditional methods. Their modus operandi will be to rely solely on computer keyboards and the Internet. It has been stated [TIMES] that “cyberspace detectives” reports of financial thefts by Russian organized-crime hackers on the Internet last year exceeded $5 billion in the US alone. Furthermore, $300 million in untraceable computer transfers have vanished during the past two months from banks and security firms based on the East and West coasts of the US. Transnational crime gangs operating on several continents are now the main computer security problem. The FBI has identified about 220 gangs that now operate in 17 US cities in 14 states, while approximately 5700 crime gangs have been identified in the former USSR employing about 100,000 full-time members and an estimated three million part-timers, according to the Russian Ministry of Internal Affairs. According to the FBI, Russian gangs are also entrenched in 29 foreign countries and maintain contacts with nearly 100,000 criminal enterprises worldwide. The crackers are also stealing and selling proprietary designs, pending merger and acquisition secrets, new products coming out of R&D laboratories and confidential information about corporate litigation.

3.5.2 Threats to Information Infrastructure

3.5.2.1 General

The threats to the information infrastructure are genuine, worldwide in origin, technically multifaceted and growing. They come from individuals and groups motivated by military, political, social, cultural, ethnic, religious, personal and industrial gain. An additional threat comes from information vandals who invade information systems for thrill and to demonstrate their ability. The globalization of networked communications increase access to our information infrastructure from points around the world. Threats against computers,
computer systems and networks vary by level of hostility (peacetime, conflict or war), technical abilities and motivation (Figure 10). The bottom line is that threats to tactical forces exist from a variety of new and different sources, and they on a continuing basis, even in peacetime.

### 3.5.2.2 Types of Threats

Adversaries have several options to influence or oppose information systems. Attacks can be designed with a delayed effect, such as corrupting a database or controlling program as well as direct actions to degrade or physically destroy. Options are listed below.

a. Unauthorized access, either to gain information or insert data.
b. Inserting malicious software to cause a computer to act in a manner other than that intended by its users. This category includes computer viruses, logic bombs and programs designed to bypass protective programs.
c. Corrupting data through malicious software, altering data or electronic attack.
d. Collecting signals intelligence - communication, electronic, radiation or data.
e. Conducting electronic attacks such as jamming, broadcasting false signals or electromagnetic pulse (EMP).

f. Psychological operations (PSYOP) and deception can be used to influence or oppose information systems.

g. Physical attack to destroy, degrade or disrupt communications and control networks. Weapons range from terrorist bombs through artillery, cruise missiles and air attack.

3.5.2.3 Sources of Threats

Threats come from a range of sources, from the unstructured (unauthorized users or insiders), to structured (foreign intelligence services and adversary militaries). Boundaries between these groups are indistinct: for example, actions that appear to be the work of hackers may actually be the work of a foreign intelligence services. Some sources are listed below.

a. Unauthorized users, such as hackers, conduct most of the attacks against information systems in peacetime. To date, they have targeted mainly personal computers, but the threat they pose to networks and mainframe computers is growing.

b. Insiders, individuals with legitimate access to the system, pose one of the most difficult threats against which to guard. Whether recruited or hostile, the insider has access to systems normally protected against attack. The insider can attack a system at almost any time during its lifetime; times of increased system vulnerability include design, production, transport and maintenance periods.

c. Terrorists are increasing their use of commercial information systems. Their actions range from those of the hacker through destructive actions against the infrastructure, such as bombing. Terrorist groups have been identified using computer bulletin boards to pass intelligence and technical data across international borders.

d. Non-state groups - the "New Warrior Class" - is taking advantage of the possibilities offered by the Information Age. They can acquire, at low cost, the capability to strike at their foes' commercial, security and communication infrastructures, and from a safe distance. Besides attacking opponents outside the battlefield, these groups make use of the international news media to influence global public opinion and shape perceptions of a conflict - or to create conflict where none exists.

e. Foreign intelligence services have been active in peacetime information operations. Taking advantage of the anonymity offered by computer bulletin boards, they often hide organized collection or disruption activities behind the facade of unorganized hackers. Much of their efforts do not directly target the military; instead, they attempt to penetrate commercial and scientific networks.

f. Adversary activities are more traditionally associated with open conflict or war, but their manipulation of the news media during peacetime may frame the situation for
an onset of hostilities.

3.5.3 Nodes and Links as Targets

A distributed information system consists of nodes (switches, command centres, etc) and links (media connecting the nodes). Both can be attacked; sometimes it is easier, safer or surer to attack one than the other; sometimes a node or link not directly associated with the target of interest constitutes a more attractive target for purposes of attacking the intended victim than the latter.

As shown in Section 3.3.4 (Information System Structure Models), the Logical and Semantic Layers of an Information System are often more vulnerable than the Physical Layer, leading to the possibility that a remote node or link has indirect influence over an designated target and therefore can affect it adversely. A heavily defended military formation’s tactical command post, for example, that is dangerous to attack by air may rely totally on data and information from a much weaker main command post at a separate site, and is connected to it by a radio or similar link vulnerable to certain attack such as jamming or deception. Target analysis would reveal the vulnerability of the weaker post and the dependence of the stronger post on its data; logic would indicate the desirability of attacking the weaker target, and suggest the means and timing. Generally speaking, a node or link that affects more than one other node or link is a more desirable target than one whose loss has minimal effect on surrounding system elements.

Similarly, Arab nations hostile to the US have found it easier, cheaper and (in theory) safer to attack non-military targets within the US borders than to confront its military forces in the Middle East. The US has discovered that it is far more vulnerable to attack in its NII than in its DII and (in particular) its tactical C2 systems, which expect and continually prepare for attacks.

The nature of hostilities conducted at Virtual and Semantic Layers of an information system requires the attacker to carry out very careful analysis of the targets and possible alternates, and to collect precise data about the whole target organization (military forces, NII, DII, locations, technical parameters, etc) before executing an operation against it. Such analysis pays dividends by contributing to the certainty of the attack’s success, effectiveness and cost.

3.5.4 Confidentiality and Assurance

Information systems, and C2 elements reliant thereon, are vulnerable to data theft and distortion, as well as to destruction. To prevent theft it is customary to employ some form of
encryption or similar security. Encryption can also provide assurance of the accuracy and completeness of the material. Military forces in general, and the CF in particular, have established encryption routines, but the NII and GII are only just addressing those requirements. In addition, there is a need in the civilian world to send signatures electronically, for contracts, money transfers, etc; the Canadian Government is addressing those requirements.

3.6 JURISDICTIONAL AND LEGAL ISSUES

3.6.1 General

In past military conflicts jurisdictional or legal issues related to information have probably not been considered to any great extent; however today, and in the future, the military use of information comes under increased scrutiny in operations other than war and in combined operations with our allies and other government departments. As we become more reliant on IT systems we also become more vulnerable to attacks on our IT systems. The department must consider the potential for loss or compromise of information in all areas of conflict and the potential for litigation and/or loss of credibility when it comes to protection of IT assets.

The departmental and interdepartmental jurisdictional responsibilities related to information security are provided in [SECURITY], which outlines Canadian policy and its application to government departments. The security policy states in part that:

a. Information is to be classified and designated according to the appropriate provisions of the Access to Information Act and Privacy Act.

b. Materiel and information technology assets are to be classified and designated according to their confidentiality, integrity, availability and value.

c. Sensitive information and assets are to be safeguarded according to minimum standards and as assessment of related threats and risks.

This policy applies to the CF, Royal Canadian Mounted Police (RCMP), Canadian Security Intelligence Service (CSIS) and other government departments. Appendix B of [SECURITY] outlines departmental responsibilities, including a number of items related to Information Warfare, as follows:

a. CSIS:

   establishing guidelines for declassification or downgrading of classified information pertaining to security intelligence activities, as defined by the CSIS Act, as well as that relating to security intelligence sources or methods;
b. Communications Security Establishment (CSE):

(1) negotiating international SIGINT agreements, including those for exchange of SIGINT with foreign governments and organizations;
(2) approving the release of SIGINT to departments and contractors;
(3) classifying, downgrading, sanitizing and declassifying of SIGINT and approval of action taken on the basis of SIGINT;
(4) providing cryptographic support for the federal Government;
(5) promoting and evaluating trusted software;
(6) providing advice on threat and risk assessments and system accreditations;

c. Department of Foreign Affairs and International Trade (DFAIT):

(1) all measures to protect sensitive information or assets under its control in Canada and at and between Canadian diplomatic and consular missions abroad;
(2) providing advice on threats to sensitive information and assets outside of Canada, when requested;

d. DND:

(1) inspecting and evaluating measures to safeguard its own electronic data processing assets;
(2) conducting counter-intrusion and counter-intelligence programs within the department in accordance with approved security standards and agreements;

e. Public Works and Government Services Canada (PWGSC):

ensuring the confidentiality, integrity and availability of common service telecommunications in government.

3.6.2 Classification and Protection of Information

The military has responsibilities and obligations for classification and protection of operational data, and the confidentiality and privacy of individuals and corporations. When information is shared with other departments, agencies and allies there is the additional burden to ensure that shared data is handled in the appropriate manner.

In the first instance all departments are responsible for classifying all information that is reasonably likely to be exempt from access under the Access to Information Act and Privacy
Act, specifically:

a. where compromise could reasonably be expected to be injurious to the Government of Canada (GOC), international affairs and defence, including the detection, prevention or suppression of subversive and hostile activities; and
b. where the information is obtained or prepared by an investigative body during lawful investigations into activities suspected of being threats to the security of Canada within the meaning of the CSIS Act.

Departments are also responsible for designating information that is likely to be exempted or excluded from access under the Access to Information or the Privacy Act. This includes information related to:

a. law enforcement and investigations;
b. safety of individuals;
c. medical records [SECURITY, Chapter 2-1, Appendix C]; and
d. Privacy of individuals (eg, Income Tax data).

3.6.3 Confidentiality and Privacy of Individuals and Corporations

The delivery of federal programs and services in Canada and abroad requires that agencies respect all relevant provincial laws and international agreements, including those of privacy and access. Government departments are required by law to protect information gathered from private citizens and corporations. (While the Acts do not specify what is to be done or the required level of protection, they do require the Government and Departments to "Protect the Privacy of citizens and persons" (including corporations which, within the meaning of the act, are considered persons)). The acts range from those specific to a particular department, such as the Tax Act, to those applicable to all departments, notably the Privacy Act and the Access to Information Act.

The federal government also has a number of policies and directives that specify requirements for achieving security of personal information. These include the GOC Security Policy (GSP), and Data Matching Policy and Guidelines for Federal Information Exchange Agreements.

The Organization for Economic Cooperation and Development (OECD) adopted “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” in 1980, to which Canada has adhered. The federal Privacy Act, and several provincial and territorial acts, were based on the OECD Guidelines. The Guidelines include principles of international application, covering free flow and legitimate restrictions. Other countries and international organisations have legislation and directives that need to be taken into account. Most notable in this regard is the European Union (EU) Data and Privacy Protection Directive. In situations where the
Federal Government and its Departments are sharing or exchanging information with other countries, this legislation will have to be taken into account.

Within the public sector a recent development is the Canadian Standards Association (CSA) Model Privacy Code. Although still in draft form, this document is already gaining considerable support. The Privacy Commissioner in his recent report recommended that the GSP be modified and updated to reflect the provisions of the CSA Model Privacy Code. In an analysis of privacy legislation needs for Canada, Professor Colin Bennett pointed out that Canada was one of the very few nations without privacy legislation affecting both the public and private sectors, and that while, in his opinion, the CSA Model Privacy Code was on a par with or slightly ahead of that in other countries, it would need enabling legislation to be considered equivalent to the EU Directive.

In summary, there exist numerous pieces of legislation and directives which establish requirements for confidentiality and privacy protection of information. It can be anticipated that in the next several years the amount of legislation and the stringency of requirements will increase.
3.6.4 Regulation of Information

Canadian legislation governing IT and information is still undergoing development. (In one case the value a court assigned to stolen business documents was the cost of the paper on which they were printed.) It should not be surprising, therefore, that international legislation is in a more primitive state. There are no international procedures or laws governing theft from one country of data stored in another, and computer hackers who steal, degrade or destroy data in the computers of another nation must be prosecuted (if legislation exists) in their home state - assuming that the host state is on agreeable terms with the victim nation.

Fierce resistance has met attempts to establish restrictions over obscene material on the Internet (although recently the German government imposed conditions on one US provider of Internet access, who promptly established obscenity controls). The objection is that obscenity controls over an essentially international resource could lead to politically-inspired and other controls to limit the information available to subscribers.

Such legal issues are reflected and enlarged with respect to national security. No international law determines when a computer attack by one national government on another nation’s information resources can be regarded as an act of war; yet a deliberate, well-planned attack could seriously degrade - and perhaps destroy - vital records such as financial transactions.

Charged with the military defence of Canadian interests, the CF require internationally-accepted (or, at least, GOC-accepted) IT regulations (ie, IW rules of engagement) if they are to develop strict protective measures for their, and Canadian, information and information systems.
4 MILITARY OPERATIONS IN THE INFORMATION SOCIETY

4.1 GENERAL

The history of warfare has paralleled the history of technology. Recent advances in IT present the military theorist and strategist with new challenges. The need to acquire data, process and assimilate information, and disseminate decisions is inextricably linked with the pace and intensity of modern warfare.

The concept of lines of communication was developed in a time when communications and information travelled along the same land or sea routes as supplies, trade and military forces. Satellites, computer networks, microwaves and wireless communications have freed the information flow from following parallel paths. Unfortunately, many of our concepts such as "interdicting lines of communications" are based on technologies from a more restrictive age. In the age of information operations we must consider information functions, flows and values to appreciate fully the potential consequences of "interdicting lines of communication". In today's high technology world, control of information is a critical component of the success of any employment of military forces.

4.2 TYPES OF INFORMATION WARFARE

4.2.1 The Difficulties of Definition

Defining information warfare (IW) is more than academic quibbling. Too broad a definition prevents finding a possible conceptual thread when a tighter definition might reveal it. Warfare's definition is sensitive to the milieu of its user. The American concept of war, for instance, is unique to a particular way of thinking: it results, as might an accident, from a breakdown of norms designed to maintain peace. Competition, however - regardless of how desperately waged - is not war. Consider, too, the traditional criteria for prosecution of war: to destroy the opponent’s strategic core, and - what is often quite difficult - to disarm the enemy. How reliably can IW do either?

Consider, too, the difficulty faced by a joint staff in assigning precise responsibilities even for those forms of IW that are specifically military (as opposed to, say, defending national financial systems against hackers). C2W is assigned to operations staff. Design of C2 systems for security and protection is assigned to an engineering staff; aspects of information warfare that involve the establishment and maintenance of battlefield intelligence, reconnaissance and surveillance systems fall under an intelligence directorate; because most of the interesting issues in IW assume a future information architecture different from the present, it is logical to assume that this realm is associated with a long-term planning
The defining aspect of information warfare is denial (or at least disruption), and its counterpart, protection. Into this definition must fit C2, EW, hacker war and information blockade. Information-based warfare may also be included insofar as attacks on the instruments and integrity of collection systems will become increasingly important to conventional operations. Similarly, psychological warfare is about denial in that most people cannot entertain two diametrically opposed notions in their heads at the same time. Cyberwar is a milieu where warfare and information intersect, but it too fits.

Seven forms of information warfare - ie, conflicts involving information protection, degradations and denial - are defined by [LIBICKI94]:

a. C2W - strikes against the enemy head and neck (nodes and links);

b. Information-based warfare - the design, denial and protection of systems that seek to dominate battlefield awareness;

c. Electronic warfare - warfare in the electromagnetic spectrum;

d. Psychological warfare - information used to change opposing wills;
   (1) operations against the national will;
   (2) operations against the opposing commanders;
   (3) operations against troops; and
   (4) cultural conflict;

e. Hacker warfare - software based attacks on computer systems;

f. Information blockade - a form of economic warfare; and

g. Cyberwar - futuristic scenarios of information terrorism and semantic attacks.

In the context of the US military, it is far from clear that these seven forms combine to form a coherent medium of conflict, much less a rationale for a coherent IW class.

4.3 INFORMATION WARFARE CONCEPTS

4.3.1 Social Infrastructure Components at Risk
IW refers to information-related conflict at a grand strategy level between nations or societies. It may focus on public and/or elite opinion. It may involve diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of information networks and databases, and promotion of dissident or opposition movements across computer networks.

The prime targets would be those social and economic areas that would offer the easiest access. Figure 11 shows the main national infrastructure components available for attack. The heavy links that exist between these areas would permit maximum disruption to the social fabric. For example, attacking the financial component would inflict more severe havoc than an attack on the military component. Furthermore, that attack could be performed without even setting foot into that country, which brings to light the problem of defining the battlefield’s location.

In other words, IW represents a new entry to the spectrum of conflict that spans economic, political, social and military forms of war. IW could be largely non-military, but would have dimensions that overlap into military war.

IW may be waged by government against illicit groups and organizations involved in terrorism, proliferation of weapons of mass destruction or drug smuggling. Or to the contrary, it may be waged against the policies of specific governments by advocacy groups and movements, involving, for example, environmental, human-rights, or religious issues. The non-state actors may or may not be associated with nations, and in some cases they may be organized into vast transnational networks and coalitions. Some movements are increasingly
organizing into cross-border networked and coalitions, identifying more with the development of civil society (even global civil society) than with nation-states and using advanced information and communications technologies to strengthen their activities. This may well turn out to be the next great frontier for ideological conflict, and IW may be a prime characteristic.

Some IW will involve military issues. Possible issue areas include nuclear proliferation, drug smuggling, and anti-terrorism because of the potential threats they pose to international order and national security interests. Moreover, broader societal trends (e.g. the redefinition of security concepts, the new roles of advocacy groups, the blurring of traditional boundaries between what is military and what is non-military, between what is public and what is private, and between what pertains to the state and what pertains to society) may engage the interests or at least some military offices in some IW related activities. IW might be developed into an instrument for trying, early on, to prevent a real war from arising. Deterrence in a chaotic world may become as much a function of one cyber posture and presence as of one's military force posture and presence.

4.3.2 Information Warfare as Strategy

The concept of Information Warfare (IW) may be considered as an overarching view of how modern warfare must be approached. It is a conceptual framework which not only assists in the development of military plans, projects and capabilities, but also determines how all government agencies involved in crisis management and conflict resolution interact. It also helps in the design, development and implementation of Command and Control Information Systems (C2IS).

Information Warfare (IW) can be defined as:

Actions taken to achieve a goal by influencing and controlling adversary information, computer processes and information systems, while protecting one’s own information, computer processes and information systems.

4.4 COMMAND AND CONTROL WARFARE

4.4.1 General

C2W is the military aspect of IW. The CF doctrine definition proposed in [CHAP26] is:

C2W is the integrated use of all military capabilities including operations security (OPSEC), deception, psychological operations (PSYOP), electronic warfare (EW)
and physical destruction; supported by all-source intelligence, communications and information systems; to deny information to, influence, degrade or destroy an adversary’s C2 capabilities while protecting our own against similar actions [CHAP 26].

4.4.2 Concept of C2W Operation

An attack on a command centre or information system node, particularly if properly timed, can be very disruptive to operations. Despite the known disadvantages of single-point vulnerabilities, most traffic in messages tends to circulate within very small spaces known as command centres.

Attacks on command centres can disrupt operations beyond their mere destructive effect. Iron bombs are not the only way to attack command centres. Systems can be disabled by cutting off their power, introducing enough electromagnetic interference to make them unreliable, injecting viruses, etc. Precisely how the other side is hurt depends on back-up architectures, which nodes supply information and how such information is required to inform battlefield decisions. Resources may be dispersed as a countermeasure, but not until:

a. the threat is demonstrated or recognized;
b. the technological sophistication of current command centres permits it;
c. the extent to which authority is vested in personal contact; and
d. present organizational and cultural factors have been transcended.

What is new is the sheer size of the C2 communication load in the information age. The extent to which operations depend on this load determines the value of efforts to cut communications. An attack on electronic communication channels can disable C2 systems.

Attacking communication links requires a good sense of how the other side communicates. Key aspects are, for example:

a. A cable architecture may make nodes easy to identify and disable.
b. In an electromagnetic architecture, key nodes are often visible (eg, microwave towers).
c. Satellite lines of communication can be jammed, blinded or killed.
d. A communication grid of many small elements radiates little and offers great redundancy, and compounds the targeting problem of the enemy.
e. Key traffic can be made redundant at the cost of reducing the capacity of the system.
f. Extra robustness can be provided by new technologies.
The influence of C2W on the outcome of a conflict is predicated on the target’s command architecture. A rigid structure is one extreme of organizational structure, and highly vulnerable to communication failure. Conceivably, an attack on central authority could mandate field commanders to demonstrate initiative that more than compensates for lack of central coordination. Conversely, if the central authority can be induced to surrender, the last thing one wants is for the peripheral forces to fight on.
4.4.3 C2W Disciplines

4.4.3.1 General

C2W is an integrated capability that supports military operations. The two disciplines that make up this strategy are C2-Attack and C2-Protect. C2-Attack and C2-Protect denote the synchronized and coordinated application of C2W using combinations of OPSEC, Deception, PSYOP, EW and Physical Destruction in offensive and defensive ways. The terms are defined in Annex B (Glossary).

4.4.3.2 C2-Attack

4.4.3.2.1 Principles

The principles of C2-Attack are:

a. plan based on the unit's mission, commander's intent and concept of operations;
b. synchronize with and support the commander's plan;
c. take and hold the initiative by degrading the adversary's information system; and
d. force the adversary to be reactive. "Reactive" means that C2-Attack will slow the adversary's tempo, disrupt the adversary's planning and decision cycles, disrupt the adversary commander's ability to generate combat power, and degrade the adversary commander's means for executing mission orders and controlling subordinate unit operations.

4.4.3.2.2 Effects

In general terms, C2-Attack has four effects.

a. The adversary is denied information by disrupting his observation, degrading his orientation and decision formulation, and degrading information collection. Information collection can be degraded by destroying collection means, influencing the information the adversary acquires or causing the adversary not to collect at all.
b. The adversary commander is influenced by manipulating perception and causing disorientation of his decision cycle.
c. Adversary information operations are degraded by selectively disrupting the C2 communications, computer capabilities and intelligence systems.
d. The adversary's information capabilities can be neutralized or destroyed by physical destruction of nodes and links.
C2-Attack is most effective when timed to occur just before the adversary needs a C2 function, and when focused on a target that is resource-intensive and hard to reconstitute.

4.4.3.3 C2-Protect

4.4.3.3.1 Principles

The principles of C2-Protect are:

a. gain command and control superiority - unimpeded friendly processing of information, accurate development of courses of action, valid decision making and efficient communication with subordinates;
b. stay inside the adversary’s decision cycle by denying information to, influencing, degrading and destroying his C2W resources;
c. reduce the adversary’s ability to conduct C2-Attack;
d. reduce friendly C2 vulnerabilities using C2-Protect measures; and
e. reduce friendly interference to our C2 systems throughout the electromagnetic spectrum (de-confliction and coordination).

4.4.3.3.2 Effects

The effects of C2-Protect mirror those of C2-Attack.

a. It denies the adversary information he needs to take effective action.
b. It persuades the adversary not to take action, take the wrong action or take action at the wrong time.
c. It degrades or destroys his capabilities to perform C2-Attack against friendly forces.

4.4.3.4 C2W ANALYSIS

C2-Attack analysis identifies adversary C2 systems of C2W interest and determines the critical C2 and C2-Attack nodes, links and processes in those systems. The C2-Attack focus has the purpose of increasing payoff by identifying key target vulnerabilities for offensive action.

C2-Protect analysis focuses on the adversary’s ability to detect, locate and attack critical friendly C2 nodes and his decision-making process. As with C2-Attack, intelligence plays a major role by providing information on adversary sensors, target selection and attack means. Analysis considers physical destruction, EW, OPSEC, deception and PSYOP means available to the adversary and how they might be applied to friendly C2 systems. The product is a list of critical nodes, links and processes that must be addressed by C2-Protect.
C2-Protect analysis examines technical and procedural modifications to friendly and adversarial systems, new technologies, and countermeasures that may degrade or defeat friendly systems relying upon signatures for targeting, recognition, identification and warning. Weapon systems having embedded target recognition must have current threat data for proper combat identification and optimum system performance.

4.4.3.5 Discussion

C2W may imply some institutional redesign for a military in both intra- and inter-service areas. Moving to networked structures may require some decentralization of command and control. The new technology may also provide greater "topsight" - a central understanding of the big picture that enhances the management of complexity.

C2W may also imply developing new doctrines.

The post-modern battlefield stands to be fundamentally altered by the information technology revolution, at both the strategic and tactical levels. C2W is much broader idea than attacking an enemy' C3I systems while improving and defending one's own; it is characterized by the effort to turn knowledge into capability. Even though its full design and implementation requires advanced technology, C2W is not reliant upon advanced technology per se: the organizational and psychological dimensions may be as important as the technical, and may in some circumstances be waged with low technology.

4.4.3.6 Hierarchical versus Network Structures

Military forces depend heavily on hierarchy; yet the information revolution is likely to erode hierarchies and redraw the boundaries around which institutions and their offices are built. Moreover, the information revolution favours network designs for organizations.

Most adversaries the CF face in the realm of low-intensity conflict - international terrorists, guerrilla insurgents, drug smuggling cartels, ethnic factions and racial or tribal gangs - are all organized like networks. Perhaps a reason that military institutions have difficulty engaging in low-intensity conflicts is because they are not meant to be fought by institutions. It may take networks to counter networks.

Many techniques that could be essential to C2W may improve the cost-effectiveness of many military operations, no matter what overall strategy is being pursued. To benefit from this evolutionary approach, we need to:
a. enquire methodically how the information revolution might provide new technical capabilities for warfare;
b. analyse what kinds of operational and organizational innovations should be considered in light of such capabilities; and
c. examine new theory regarding the information and communication dimensions of war, and the role of "knowledge" in conflict environments.

The traditional emphasis on C2, a key strength of hierarchy, may have to yield to an emphasis on consultation and coordination, the crucial building blocks of network designs. This may raise transitional concerns about how to maintain institutional traditions, as parts of the military become networked with other parts (inside or outside the CF) in non-traditional ways.

The information revolution has already raised issues for inter- and intra-service links and, in the case of coalition warfare, inter-military linkages. C2W doctrine may require such links. It may call for particularly close coordination among officers responsible for strategy, plans, operations, C4I and field units.

Operational and tactical command in C2W may be exceptionally demanding. There may be little of the traditional chain of command to evaluate every move and issue each new order. Commanders may be required to operate with greater latitude but as part of integrated, joint forces. Topsight may have to be distributed to facilitate this change. The types and compositions of units may change. What have often been viewed as makeshift organizational adjustments in time of war should now be viewed as a peacetime goal of standing forces, to be achieved before the onset of war. Military organizations must become more agile so as to permit flexible yet efficient C2 activities.
5 IMPACT ON THE CANADIAN FORCES

5.1 GENERAL

The full impact of IW on the CF is potentially extensive and well beyond the scope of this paper; however, the critical issues from the C2W perspective can be described in terms of:

a. Policy;
b. Doctrine;
c. Concept of Operations;
d. Organization and Facilities;
e. Personnel; and
f. Technology and Tools.

5.2 POLICY

The Information Highway Advisory Council addressed the need for security but primarily from a confidentiality and privacy perspective. The implications on malicious or hostile actions taken against the elements of a national infrastructure is not given suitable attention. There needs to be a discussion of the potential threats to national security from disruption, corruption or compromise.

The DND/CF Integrated Information Environment (IIE) is not simply part of a defence infrastructure. It is rather a part of a global external information network whose internal connections are incredibly complex. The ability to cause a catastrophic breakdown of our information and telecommunications infrastructure exist and is not technically challenging. We must develop capabilities that will enable the protection of information enclaves within this global environment. The tension between protection and openness and balance between economy and effectiveness must be carefully addressed.

Economic pressures will force private industry to develop strategies for dealing with security and privacy in electronic commerce. Visa and Microsoft have recently announced that they have established joint ventures to establish standards for electronic commerce in their Secure Transaction technology. Microsoft and other software developers are including C2 (Trusted Computer System Evaluation Criteria rating) features in their standard product line (e.g. Windows NT and Novell Netware). The international security community is in the process of developing the common criteria that will define a set of security related protection profiles that can be used for stating and evaluating security functional and assurance requirements. However, even giants like Microsoft are not likely to develop the global protective and reactionary mechanisms needed to protect networks from concentrated attack. This will have
to come from government/military efforts.

We will need to evolve toward enclaves or domains of systems whose levels of protection will vary according to the utility of the information in commerce or warfare. The key to protecting the nations infrastructure is to provide the ability to:

a. protect the system from attack;
b. detect an event when it is occurring and be able to decide if it is an attack, failure mode or an isolated hacker;
c. React, to the event in a way that minimizes the impact and restores and maintains capability.

We must rethink our approach to relating threat and risk. In the military and government environment it has been the case that threat was paramount. One always needed to have a well defined threat in order to provide justification for protective measures. It was considered prudent to purchase countermeasures in proportion to the clearly defined threat in order to avoid spending more that the risk would warrant. These common business practices have not kept pace with the growth and dynamics of computer technology. Incidents of hacker penetration of networks is growing at an alarming rate. Hacker attacks on commercial information systems, if precisely orchestrated, can distract the political leadership from their national security duties. A cacophony of hacker attacks can rival terrorist attacks for their sheer annoyance value; indeed they can disrupt the lives of far more people.

5.3 DOCTRINE

Doctrine establishes a way of thinking about war, it provides the basis for harmonious actions and mutual understanding. Information warfare doctrine must provide for definition of the rules of engagement in the information domain.

Sharp increases in the power-price ratio of information technologies, concentrated, in particular, on distributed systems suggest radically new architectures of information gathering and distribution.

IW targets at the strategic and operational levels must be evaluated carefully. Attacking IW targets only at the tactical level and without joint oversight risks the loss of useful pathways to valuable operational and strategic targets.

Netted systems have become vulnerable, but successful attack requires prior study. A successful attack could either to cut off a source of data or to overload the target system with extraneous data. The wrong strategy could be self-defeating.
Equally difficult to predict are the defences that will have to be developed against being seen, or at very least, widening the distance between image and reality on the battlefield.

The evolution of information-based warfare may be understood as a shift from situational awareness to battlefield visibility.

Some of the Joint C2W doctrinal issues that need to be considered are:

a. victory can be attained without the need to destroy an opposing force;
b. post-industrial doctrine may be developed that differs from industrial -age traditions of attritional warfare;
c. in the best circumstances wars may be won by striking at the an opponents cyber structures, his systems of knowledge, information and communications;
d. a fully articulated doctrine might allow the development of a capability to use force not only in ways that minimize costs to oneself, but which allow victory to be achieved without the need to maximize the destruction of the enemy;
e. redefinition of “an act of war”;
f. extension to the domain of operations; and

g. clarification of DND’s role in projecting power and protecting national security in the IW domain.

5.4 CONCEPT OF OPERATIONS

One factor that unifies IW is the need for knowledge of a target system's architecture and parameters. The side that better understands its enemy’s motivation, structure and goals is better prepared for conflict. Understanding the enemy's culture and his use of information systems in his society remains important.

Architecture is about bit integrity. At the core physical level architecture incorporates the sensors themselves, their power, acuity, availability and reliability. At the network level, architecture encompasses their interconnection: do they feed the core processor directly, are they filtered through particular systems, or intermediate nodes. At a higher level lie the integrity systems: encoding and encryption, message prioritization, access, digital signatures and redundancy.

Architecture links information to decision. How are readings interpreted, what readings are correlated to each other, what constitutes recognition, where the boundaries are set to eliminate false positive and false negatives, under what circumstances are sensor bit-streams given higher relative priority and so on. Finally, information from heterogeneous streams are
melded to influence decisions or support it after the fact. The sensor-to-shooter complexes of tomorrow are but one channel others include political direction, rules of engagement, the status of own forces and so on.

Information warfare waged without due regard for the architecture of decision making is no better that the proverbial shot in the dark. To know the other side's system in wartime it may suffice to know the other side's system in peacetime.

In an integrated information infrastructure, a coordinated network control capacity is required to integrate the communications control function and the data control functions. This coordinated control requires the visibility of infrastructure operations from keyboard to keyboard. The issues are still; in a defensive context - protect, detect and react; and in an offensive context observe, orient, decide and act. We must be able to detect the signs of an attack early and to be able to distinguish attacks from other forms of failure or perturbations. The overall national information infrastructure needs to be monitored by an external security control centre with the responsibility for defensive information warfare and will have a robust computing and communications capability. It must be able to diagnose problems, conduct triage actions to limit proliferating attacks or cascading failure modes, and manage the restoration of operations without being dependent on the damaged network for this activity.

In the EW domain it is almost second nature to think of EW assets providing a self protection capability for environmental assets (such as aircraft and ships). This same approach applies to our C2W assets. A concept of operation in the information domain needs to be articulated and documented in an understandable manner. The concept needs to embody both offensive and defensive C2W and include the concept of information domains.

5.5 ORGANIZATION AND FACILITIES

5.5.1 Organization

The information revolution is bound to erode hierarchies and redraw the boundaries around which institutions and their offices are normally built. Moreover, the information revolution favours organizational network designs.

A major disruption in the Public Switched Network (PSN) would have a crippling effect on the nations business and financial institutions. Who then is responsible for protecting the information in these computers and networks? Domains of authority must be clearly defined so that when an attack occurs the appropriate agents may react.

It must be possible to determine if an event involving the nation’s networks is the result of an
accident, criminal attack, isolated terrorist attack or an act of war. The damage from an event may be the same but if the intent behind the event is malicious then the responsibility for response to the event falls under a different jurisdiction that is a function of intent, crime, terrorist or war. If we are unable to react promptly until the jurisdiction is established, it may be too late to react appropriately.

We must foster an interdepartmental climate of understanding and reason so that we can reach agreement on acceptable means to conduct status monitoring of the information infrastructure in such a way that will allow industry and government to detect and react to attacks through cyberspace without creating an electronic police state.

5.5.2 Facilities

We must not forget the physical plant that houses our information systems. Critical data must be backed up regularly, stored in locations that will not share common disasters. In addition, means for distributed computing that is inherently protected from local perturbations should be developed. Disaster recovery planning should be given more attention and exercised on a regular basis, to avoid the impact of incidents such as blackouts caused by fires at a downtown Ottawa Hydro sub-station in 1987 (which took 72 hours to restore full operation) and 1995 (which took only six working hours and some silent-hour activity).

5.6 PERSONNEL

Ultimately, many problems are the result of authorized individuals roaming and browsing in computers and computer files outside their specific responsibilities. In the business world the majority of crimes are committed by authorized users acting outside of their authorized duties. Even with the additional screening of military personnel we are not going to change human nature. It is possible however to be aware of such behaviour and to design systems and procedures that mandate accountability.

The techniques for protecting systems against insider threats are well-known. Training and awareness, strong identification and authentication, meaningful audit collection and reduction. Clearly we must focus resources on the passive and continuous identification and authentication of the users of information systems, auditing of user activities at both the technical tele-computing and application (workflow) levels (including audit reduction), and the design of personnel security programs for information workers.

Network managers must be equipped to know the status of the infrastructure on a global basis and be able to detect attacks or system failures. They must be prepared to react effectively and efficiently when a problem does occur to diagnose, control and recover capability.
5.7 TECHNOLOGY AND TOOLS

5.7.1 Defensive IW

The ability to cause a catastrophic breakdown of our information and telecommunications infrastructure exists and is not technically challenging. In the past, it required the resources of a nation to wage war. Today anyone with relatively inexpensive equipment and a modicum of technical understanding can cause disruption that could be significant and costly.

In spite of years of discussion about the need for security in computer systems and networks, most systems continue to be designed without the needed security features. The military continues to defer security requirements in favour of other operational needs when budgets are tight. Even where security is being included, the current process of development and security evaluation causes systems to be obsolete by the time they are fielded. Clearly to acquire military systems over a 5 to 10 year acquisition cycle is inconsistent with today's needs. A design approach is needed that is appropriate to the continued injection of security technology into existing and developmental information environments. This design approach should explicitly address the security design practices for the protection on information environments, the detection of malicious action and capability to react to such actions.

To achieve this we begin with a systematic examination of information security research and design criteria at the architectural level. We must find:

a. a means to know the current state of an information system environment at the technical computing level, the telecommunications level and the application level.
b. criteria to recognize when the current state of the environment is perturbed in order to provide for automated diagnostics and warning.
c. features at the technical level and application levels that will enable the ready restoration of a perturbed environment to a known desired state.
d. basic protection features that will limit well-known and low cost attacks on an information environment
e. network features that will automatically limit proliferating attacks or cascading failure modes.

The technical capacity and cost to attack information systems is now so insignificant in proportion to the value of the information that we must assume the threat is real. In order to conserve critical resources, we must balance protection with the value of the information. We need to develop design metrics that relate a specified degree of protection to cost. A normalized means of addressing the incremental cost of various information security
technologies and design features in relation to the anticipated risk is needed for informed design decisions.

5.7.2 Analysis Tools

The human being needs to be able to take the knowledge products and to use them to enhance his or her perception. This is where technology is starting to have significant impacts and where C2 doctrine, organizations, concepts and procedures must be re-engineered to exploit and leverage emerging technologies.

Emerging technology must be exploited while adapting it and applicable command and control processes to significantly improve the effectiveness of decisions at reduced costs.

We must apply technology to support reaching decisions as opportunities rather than demands.

A readily apparent way of improving the delivery of information and knowledge of the decision maker is to disseminate information in a form that is easily managed, presented and quickly understood. In many cases, the best medium is visual and the best presentation is an image or graphic. Movement away from "information push" toward "user pull" and "smart push" is a significant aspect of the emerging way to significant improvements in information exchange.

The challenge is to improve the speed with which "what if" analyses can be accomplished and to integrate the simulations more thoroughly into operational systems and the overall C2 decision making context, including the operators procedures.

Institutions such as CNN, and tomorrow's technologies such as DBS, make the dissemination of deception easier. If nothing else, the proliferation of media permit the promulgation of confusion. Viewers could maintain computer agents that could roam the Net extracting news and commentary to their interest and linking from recently archived and real-time material and putting it together into individual news broadcasts.

5.7.3 Databases

Database research and design requirements should be explored including such topics as:

a. how the integrity state of stored data can be known even if not being used to support active transactions; and

b. design features for rapid replication of data bases while under attack as a strategy for
single point failures.

While databases for EW parameters have been in existence for several decades, it has been only in the last few years that the benefits of relating platforms and weapons to emitters has become a necessity for providing operational reprogramming support to front line EW systems. A similar approach will be required in the area of C2W. Initially there will be the requirement to identify the parameters related to links and nodes. This data will be necessary for the reprogramming required for the current generation of reprogrammable land EW systems. The real value from a joint C2W perspective will come when we have a database that will allow relationships to be made among the physical architecture to the logical decision making architecture. There is also the additional requirement to overlay the temporal dimension on links and nodes analysis i.e. getting inside the adversary’s OODA Loop decision cycle.
6 RECOMMENDATIONS

6.1 GENERAL

In formulating these recommendations the five military actions (i.e. Deception, OPSEC, PSYOP, EW and Physical Destruction) have been considered as they relate to the Offensive C2W Planning Process (i.e. Support to Commanders objectives, Identify enemy C2 Nodes, Analyse Nodes, Prioritize nodes, Determine desired effect, Assign assets, Determine effectiveness) and the Defensive C2W Planning Process (i.e. Identify Critical C2 Nodes, Analyse C2W Nodes, and Recommend options) as they are currently defined in Chapter 26. The recommendations are consolidated under the broad headings of Policy, Doctrine, Concept of Operations, Organization, Personnel, and Technology and Tools.

6.2 POLICY

6.2.1 General

There are two IW policy areas that need to be clarified. First as it relates to IW activities at the national level and the role of DND within the national context, and second within the C2W context of operations there is the need to clarify and perhaps extend the mandate for IW operations to include the full range of potential military operations from peace to war, i.e. the current policy for Operations other than war needs to be re-examined from an IW perspective.

6.2.2 National Level IW Policy

Currently the roles of the various government departments are not defined for IW activities. This is understandable when there is no clearly defined threat. Yet the information revolution is bound to erode hierarchies and redraw the boundaries around institutions and their responsibilities. Moreover, the information revolution favours organizational network designs. An appropriate Canadian government response could evolve to an IW community of interest with domains of authority clearly defined so that when an attack occurs the appropriate agents may react. Although the damage from an event may be the same, if the intent behind the event is malicious then the responsibility for response to the event falls under a different jurisdiction that is a function of intent (i.e. crime, terrorist or war). Nonetheless, from a DND perspective guidelines are needed to identify what should be considered the onset of hostilities. Furthermore, DND relies so heavily on a civilian infrastructure for communications, power, banking etc. any threat and subsequent degradation in service can significantly impact DND capability. We must foster an inter-departmental climate of understanding and reason so that we can reach agreement on acceptable means to conduct status monitoring of the information infrastructure in such a way that will allow industry and
government to detect and react to attacks through cyberspace without creating an electronic police state.

As a minimum, DND needs a policy to:

a. identify the extent of its reliance on the civilian IT infrastructure;
b. understand and quantify the impact of collateral damage to the military by IW attacks on non military targets;
b. coordinate with other government departments the process of identifying and characterizing threat agents, threat events and threat capabilities that represent a danger to Canada (including PSYOP);
c. clarify and perhaps extend internal DND policy related to GOC IW operations.

6.2.3 C2W Policy Clarification

The current C2W policy is focused primarily on C2W operations in War; a war where there is a clearly defined enemy and enemy commander and support infrastructure. Conversely, in the normal conduct of military operations there will be targets that when destroyed will have an impact on the IW aspects of the overall conflict. The policy needs to be extended to include operations other than war where there may be no clearly defined commander and the support infrastructure is a dynamic, complex and highly adaptive system. The policy also needs to evolve to provide a capability to identify potential collateral damage to both friendly and enemy forces as part of their overall C2W planning process - i.e. even without a stated intent to conduct offensive IW the end result could be the same and we need to be prepared for the result. The policy needs to reflect the time sensitive nature of data and information and the need to examine information domains where a security policy can be defined and applied selectively and adaptively in response to the IW operational situation.

The C2W policy should be clarified to:

a. define the rules of engagement for a full range of C2W operations;
b. plan for potential operations that result in an offensive IW impact;
c. plan for an adaptive security policy for information domains engaged in IW operations.

6.3 DOCTRINE

Information Operations transcend the operational environment normally assigned to land, sea or air forces. Operations in this fourth (or cyberspace) environment must be based on a clearly defined policy as clarified by doctrine for joint operations.
The current Defensive C2W planning process appears to ignore the potential for PSYOP against friendly forces. All military personnel engaged in information operations (across the full spectrum of conflict) will have access to open source information, media and perhaps directed mis-information. The joint staff need to be advised by appropriate agencies when this occurs and be prepared to respond accordingly.

The defensive aspects of information operations also need to consider the fall-back actions and recovery/restoration of information assets that include DND and civilian infrastructure components. It is not clear what role the joint staffs play in planning for and responding to an attack on our information assets.

Specifically the doctrine needs to:

a. reflect the needs of an agile organizational structure - of both friends and enemies
b. be re-engineered to exploit and leverage emerging technologies;
c. be sensitive to the temporal aspects of the modern IW battlespace;
d. recognize a new range of threat agents, threat events, and threat capabilities;
e. be responsive to the rapid pace of change in technologies that is driving IW operations
f. recognize the complexity of coordination of offensive PSYOP and its impact on friendly forces;
g. include defensive PSYOP as part of the planning process
h. clarify with other government and civilian agencies roles for reacting to an attack on our information assets.

6.4 CONCEPT OF OPERATIONS

We must foster the concept of Information Domains that are not bounded by networks, but rather by the presence of their assigned information assets and specifically authorized users. They may be supported by any information system that can meet the protection and delivery requirements of the Information Domain security policy. To support the operational concept a design approach is needed that is appropriate to the continued injection of security technology into existing and developmental information environments. This design approach should explicitly address the security design practices for the protection of information environments, the detection of malicious actions and the capability to react to such actions.

The use of threat simulators and stimulators is a key concept that needs to be applied to the C2W domain. We need to test and probe the security features of our networks and information domains with realistic viruses and concerted attacks from knowledgable threat agents. The Joint Staff need to evolve a concept of operations that can take disparate
activities and recognize them as threat events. The operational concept must include an understanding of threat capabilities as well as employment of our C2W assets, both offensive and defensive. Disaster recovery planning should be given more attention and exercised on a regular basis.

Information operations need to focus on support to the Joint Staff. The services that need to be provided include:

a. C2W threat analysis
b. C2W threat change impact analysis
c. C2W vulnerability analysis
d. C2W databases
e. C2W modelling and simulation facilities

6.5 ORGANIZATION

IW operations include C2W in the military context, but also extend to Interdepartmental operations at the national level. The Joint Force Commanders will need input from National Operations staff (J3/G3), Intelligence, Security, Communications, EW and Environmental Commanders. There may be a role for other agencies such as CSE.

For C2W we must rethink our approach to relating threat and risk. The ability to cause a catastrophic breakdown of our information and telecommunications infrastructure exists and is not technically challenging. Within the military there needs to a single focal point for IW operational support.

The current Interim EWOSC is intended to provide that focal point for operational support to environmental EW systems. It provides a variety of threat analysis, database and core support services to all three environments and is a joint operations resource. The individual environments are represented within the EWOSC facility by Integrated Support Stations ISS's which provide the detailed reprogramming of environment specific EW systems.

The C2W operational, intelligence and engineering skills required for characterization of threat agents, threat events, and threat capabilities need to be combined in a single unit. Similarly, the real value of a C2W tailored database, from a joint C2W perspective, will come when we have a database that will allow relationships to be made among physical, logical and decision-making (semantic) architectures. There is also the additional requirement to overlay the temporal dimension on links and nodes analysis i.e. getting inside the opponents OODA loop decision cycle.
The Interim EWOSC is limited to the RF portion of the frequency spectrum, but the EWOSC project is intended to extend that support capability to include IR and communications systems. One of the fundamental tenets of EW operational support is the need to capture the synergism of operational (land, sea and air), intelligence and engineering staffs to affect a mission tailored EW capability. This unit is ideally suited to broaden its mandate and assume the role of the IW operational support centre - To achieve this requires:

a. personnel with skills in the IW operational domain;
b. extension of the threat analysis capability to include C2W;
c. extension of the database capability to include C2W systems;
d. development of the equivalent of a joint C2W ISS;
e. development of methods and acquisition of tools to support the joint staff's C2W simulation and modelling systems;
g. access to IW threat data provided by national/DND resources.

The current offensive C2W planning process includes the need to "determine desired effect, assign assets, and determine effectiveness". It is not clear from an organizational perspective who determines the desired effect, who owns the assets to be assigned and who determines effectiveness. Clearly, Joint staffs have as a minimum role coordination in all three areas. Also, it should be noted that IW assets required to test (stimulate and simulate) our own vulnerabilities also can be used in an offensive role.

6.6 PERSONNEL

A small, but very specialized, group of personnel will be required to fill IW positions within an IWOSC unit, Joint staffs and related Intelligence, Security and Communications organizations. The IW operational domain is subject to the rapid evolution of hardware, software and communications technologies and personnel will require up-to-date skills in each of these areas in order to be effective. Network managers must be equipped to know the status of the infrastructure on a global basis and be able to detect attacks or system failures. They must be prepared to react effectively and efficiently in order to diagnose, control and recover capability when a problem does occur.

The current military training system is not well suited to the acquisition or maintenance of skills in an area subject to continual and rapid change such as IW. It must be understood that, in order to stay current in the IW field, personnel will likely require periodic (every one or two years) training to update their skill and knowledge. Furthermore, the skills required are not necessarily unique to a specific trade or to the rank structure. Currently many of the required skills are easily found only within the popularized, but notorious, hacker community. Finally, progression and employment for such IW personnel will need to be addressed in order to
provide a meaningful career for the individual and an effective IW cadre for DND/CF.

The military actions related to PSYOP and deception in general require additional skills that need to be integrated in Joint planning and operational activities.

To provide personnel with the appropriate IO skills requires that:

a. the specific skills must be identified in detail;
b. a plan for staffing/manning/contracting needs to be developed;

6.7 TECHNOLOGY AND TOOLS

Many of the tools and techniques required for C2W support are extensions of those currently used in the EW domain. For example EW threat analysis and EW database support can, at least conceptually, be extended to include C2W requirements. New and unique areas include links and nodes analysis, coping with the sheer volume of information available and the time critical nature of Information Operations, i.e. the OODA loop.

The methodologies for documentation and analysis of information domains is conceptually an extension of techniques currently available but they need to be refined and tailored for C2W needs. Many of the tools required for C2W links and nodes analysis have both an offensive and defensive capability. Ideally a capability needs to evolve to provide an analysis and development environment to examine IW threats, potential countermeasures and related analytical tools.

An IW Battle Lab facility (patterned along the lines of an environmental ISS) could:

a. provide a focal point for IW technology demonstrations within DND;
b. host a variety of software - government-owned, contractor-furnished, demonstration copies and publicly-available shareware;
c. be made available for training and conducting IW related research;
d. be connected to the Internet so as to maintain cognizance of one aspect of the operational environment.

The potential IW battle Lab activities could include:

a. EW parametric data visualization, to investigate the application of visualization technologies to analysis of electronic warfare parametric data;
b. links and nodes analysis, to identify the process, methods and tools that can be used by joint staff to identify, analyse and determine critical links and nodes for planning
and conducting defensive and offensive IW (C2W) operations;
c. text visualization, to investigate the application of visualization of textual information to query document databases, browse the results of queries and perform visual analysis prior to selecting and reading documents;
d. defensive IW tools technology demonstrator, to analyse state-of-the-art IW threats and tools available to monitor, detect, counter and correct the results of their intrusion;
e. analysis of state-of-the-art electronic agents and pattern detectors (such as found on the Internet), to support intelligence analysis and providing user alerts; and
f. information system static and dynamic vulnerability analysis.