AN HOLISTIC APPROACH TO INFORMATION OPERATIONS:
The Canadian Experience

Tiit T. Romet
Ibis Research Inc. and Private Consultant,
Formerly Defence Scientist, DND, Canada

ABSTRACT

This paper will initially describe the elements of the broad conceptual framework that was employed. It will then describe the specific concept developed within the CF and an outline of the structures that have been put into place. The paper will conclude with observations on lessons learned, and the difficulties experienced in following the holistic approach towards developing the Information Operations program, both within the military and the government at large.

BACKGROUND

Five years ago, the Canadian Forces (CF) were faced with decisions on how to integrate information based operations into its military routine. With the rapid evolution of computer and communication technologies, information was recognized at the outset as a strategic resource that must be effectively managed. Canada was already integrally networked with the United States in numerous related areas such as telecommunications and banking. Coupled with the overall global growth of commerce and information exchange via ever expanding communications networks, it was necessary to understand that the traditional view of borders no longer existed.

The expectations were being created not only in the military, but also in government and private sectors that information can be instantaneously gathered, analyzed and exchanged. The Internet had become the network by which personal (private), business and even (sensitive) military information could be exchanged. Both our economic and military effectiveness was increasingly dependent upon automated information systems and networks. Furthermore, as cost cutting and the creating of new efficiencies emerged, the military was integrating more and more civilian technologies into their military systems. We described these phenomena as the “civilianization of the military.”

With the United States military moving forward rapidly in this new domain, which they initially called “Information Warfare”, Canada needed to address the many issues that faced them. The CF understood that it did not have the human or fiscal resources to take the US approach and needed to develop a conceptual framework within which its own requirements could be analyzed and implemented.

DEVELOPING THE FRAMEWORK

The Advancement and Employment of Technology

It is generally accepted that the emergence of information based activity is directly linked to the technological advances occurring over the past decades and their application. The key technology areas, which are the underlying elements, include **communications, sensors** and **computers.**

The breadth and variety of **communications** that have developed vastly improves the options, complexity and criticality of the information that it carries. With the means of transmission offering greater choices, ranging from wireless, to wideband copper cables to optical fibers, the progressively increased availability of the number of channels, bandwidths and types of circuits (eg. satellite relay, cable television etc.) has extended the range, and shortened the time over which information can be exchanged.

Information is now available through a greater number of sources, and in particular from the military perspective, non-human **sensors.** The whole electro-magnetic spectra can be exploited passively or actively through the various collection means such as radio, radar, infrared/electro-optics, and synthetic aperture radar. In parallel though, the countermeasures have also evolved to better mask, deceive or hide objects of interest.

The constant evolution of **computer** hardware and software through increasing size, power and applicability while decreasing in size and cost is a daily reminder of the difficulty in staying at the lead-edge of information technology.

Not only has the technological basis for the information-based society evolved, so have the systems and organizations which utilize the technology increased in number and complexity. **News media** now cover global activity on a 24-hour, 7-day a week basis and increasingly, it is being made equally available to greater numbers of the world's population.

The **Internet** has become underlying conduit for much of the exchange of information and communication. It has evolved dramatically from its beginnings, a proposal by the RAND Corporation as nuclear-survival network using individually unreliable or vulnerable elements interconnected so that system capability and functionality would be survivable. Today, the demand for information via the Internet overrides the concerns for security and integrity of the information, or the reliability of the source. Consequently, even today, information can be exposed to interception, distortion or theft.

Electronic commerce is the most rapidly growing economic area. Legal tender in the form of money, stocks and bonds, and many other transactions now occur electronically or are only an electronic entry in a databank. The commerce of Canada (and thus that of the CF) is heavily dependent on the privacy and accuracy of the Internet and its commercial equivalents.

Information Environments and Infrastructures

While the United States began its exploration and activity in Information Operations from within the military, Canada chose its starting point the **global information environment (GIE).** The GIE was defined as individuals, organizations or systems outside the sphere of military control, and while separate and distinct, encompasses the **military information environment (MIE).** It was considered that all "operations" take place within the GIE and because of the technological advances, military operations can be viewed, analyzed and disseminated to a global audience in near-real time. In fact, in can be shown that information could be distributed quicker via commercial linkages than by government or military means.

To support the GIE, there exists a **global information infrastructure (GII)** that is an interconnection of communication networks, computers, data bases and consumer electronics that allows for the access of information to a wide audience. It is linked globally and characterized by a merging of civilian and military information networks and technologies. There exists within the GII, **national information infrastructure (NII),** which consists of a series of components that include public (governmental) and private information networks and support national visions, activities and organizations. There are no discreet boundaries between the GII and NII; in fact, global access to information becomes increasingly critical with the globalization of markets, resources and economies. The **defence information infrastructure** is embedded within the above two infrastructures provides mission support, command and control and intelligence networks to the military.

Information and Decision Architecture Overview

Within the broad conceptual framework, an architectural framework was established which could address such concerns as privacy, confidentiality and the decision making process. While many different models and systems have been developed to describe decision making, they all have the same basic common elements:

a. acquisition of data
b. processing of raw data into useful information which leads to understanding
c. comparison with the existing or current state
d. decision on implementation, direction etc.

It was important to understand that within the decision making cycle there were two distinct yet interrelated entities that ultimately contribute to a final decision. There exists an *information domain* that is comprised of three elements:

i. a specific set of information assets
ii. authorized uses of the information
iii. a security policy governing the use of the information assets.

As an example, the information assets could include all the medical records and information on an individual within a government health plan. The authorized users would be the selected government employees, the medical doctors and the patient. The security policy would specify how information is protected, who has access, how the information is stored, processed etc.

The other entity is the actual *information systems*, which comprises of the processing and communication components that must incorporate the security features and policies outlined in the information domain.
Layers of Vulnerability

The actual structure of the information system can be separated into three layers which overlay each other and are based on their function: physical, logical and semantic. This categorization has been useful in understanding the vulnerabilities of information within any information infrastructure. At the base is the **physical layer** that can be described as the hardware elements of the information system. These would include buildings, computers, communication equipment and even personnel. This view naturally leads to the concept of carrying out "links and nodes" analysis. The middle strata is the **logical layer** which consists of how the structure is operated, the software, the systems, the processing of data into information and ultimately knowledge, and the distribution of the information and the operating procedures. The third and highest level we called the **semantic level** and represent the content and interpretation of the information contained within the information system.

The **physical layer** is vulnerable to physical destruction and the object of traditional military weapon systems. As civilian and military infrastructures become more and more integrated, greater emphasis must be put into links and nodes analysis to ensure effective targeting. The goal of disrupting the **logical layer** is to interfere with system functions. Attacks could include delaying of the execution of procedures, misdirecting information or infection by software viruses. In the ideal disruption, the attacker does not need to destroy the information or system but rather control it. At the highest echelon, the **semantic level**, the objective of the attack is to affect and/or exploit the trust users have in the information system, the network and in their ability to interpret and make decisions about the information. Our broad framework emphasizes that what the military had called Psychological Operations may have a much broader context if describing global or national information infrastructures.

Implications to the Military

The broad framework that was being outlined was attempting to show that a society's ability to wage war depends on every component of the technological infrastructure that now exists. The ever increasing interdependencies between civilian and military infrastructures demands changes in how conflict is to be carried out, challenges the design of traditional institutions and hierarchies and redraws our concept of borders and national security. As stated by the Tofflers, societies wage war by their means of producing wealth, and we are, or have moved, into the information era.

THE CANADIAN FORCES CONCEPT

Based on the initial broad concept development, and then through follow-up visits, meetings, and discussions, the Canadian Forces formulated their vision of Information Operations. For the CF, IO went beyond simply information systems and processes, but rather, **IO should be viewed as a STRATEGY, NOT a capability unto itself.** If viewed as a strategy, then the objective of IO became the decision-maker, whether they be a president, prime minister, commander or individual service member, sailor, soldier or airman. Therefore, IO became a strategy that integrates various capabilities to achieve political or military objectives. It followed then that IO includes a wide range of capabilities that could encompass traditional military activities such as destruction, deception, OPSEC, EW, PSYOPS (C2W) to technologically based activities such as computer network attacks, or civil affairs, public affairs and even legal affairs.

Definition

For the CF, the definition became:
"Actions taken in support of political and military objectives which influence decision makers by affecting other's information and/or information systems while exploiting and protecting one's own information and/or information systems."

The CF definition for IO shows that information is the means, and the decision maker is the end. The definition intentionally downplayed the technical aspects of IO and focuses on all measures that could be used to influence the decision maker. While many debates have gone on in Canada, as well as throughout the world on defining IO, the CF definition was intended to be broad. As such, it could be applied to national, international, civil or military activities and applies equally to peace, crisis or war.

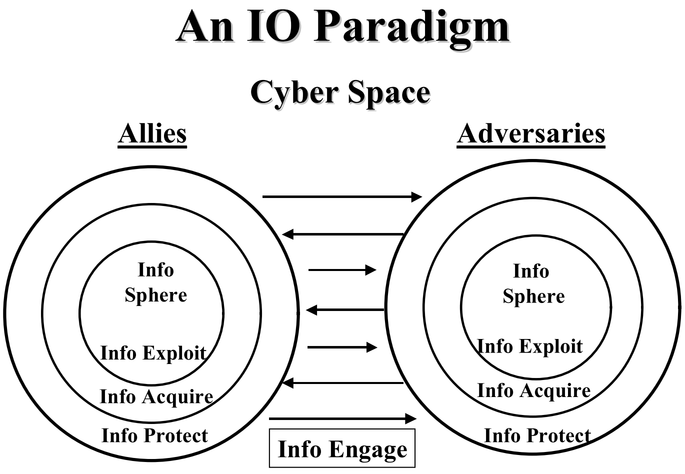

Figure 1: The IO Paradigm

The IO paradigm that was developed to portray the CF message and that became the basis for the development of the CF structure was a series of information "spheres" as shown in the above figure.

This environment, that was called for lack of any better words **cyber space,** contains the sum total of all information, both adversarial and friendly. There are four basic processes that can be carried out in this cyberspace: information exploitation, acquisition, protection and engagement with the understanding that the same activities will be carried out simultaneously by any adversary.

The CF wants to be able to **exploit** the information it possesses. This implies having a system established that will provide the appropriate information to the appropriate user at the appropriate time. The CF will need to **acquire** information, both that pertaining to our potential adversaries through various intelligence and other means, and that of our allies and friends to ensure compatibility. Whenever one collects or exploits information, it also needs to **protect** the information and the processes by which it collects and exploits. This process will include both protection from our adversaries through computer/system intrusion detection and reaction; and from ourselves, such as the disgruntled employee or viruses. The protection aspect also includes the ability to recover and operate after intrusions or disruptions. Finally, the CF needs to **engage** our adversaries (or our own internal "enemies") by trying to prevent or blind their ability to acquire information, break through their protective mechanisms and acquire or gain control of their information and/or processes.

IMPLEMENTATION INTO THE CANADIAN FORCES

It was from these four basic processes and functions, exploit, acquire, protect and engage, that the CF evolved its IO Group structure and activities to be able to carry out its responsibilities and mandates. Parallel to this effort, the Defence Department was also engaging the other government departments and Privy Council Office (central government activities) both at the Executive and Staff Working levels, to establish a co-ordinated government response to the threats and vulnerabilities. DND saw itself has having an important role to play but one as a partner in the larger Government of Canada process. This view integrated well with the overall concept of Global and National Information Infrastructures, their protection and Canada's role within these processes.

IO Working Group

Initially, the CF established an IO Working Group to address many of the issues that needed to be investigated for the military to become proficient in IO, including concepts, doctrine, policy, R&D requirements and training. The Group encompassed all the major components of DND including J3 Operations, intelligence, the three services, legal, policy, Chief Information Officer, R&D community and public affairs.

Since its inception, the CF has re-structured to form the CF Information Operations Group (CFIOG). This effort integrated and consolidated many functions that relate to IO activities to form a single voice to represent IO activities. New activities were established based on the IO paradigm that was described earlier. A National Vulnerability Assessment Team (NVAT) was initially established to begin the role of protection of the CF's information resources. This activity has now been joined by a Computer Incident Response Team (CIRT) and is currently establishing the mechanisms to detect, report and investigate intrusion attempts of military information systems.

Parallel to these efforts, CF Doctrine has been written, approved and disseminated. Individual service doctrines have been prepared and integrate with the broader CF Doctrine. While this aspect was completed without major delays, the CF Policy development was more difficult. Among the largest issues included concerns about the role and activity of PSYOPS, its relationship with Public Affairs, and legal aspects of offensive and defensive IO activities.

Some of the key features that the recently approved policy contains include:

a) IO is an integrating strategy that focuses on all aspects of influencing decision makers
b) IO is not simply a technical issue, but includes things such as publics affairs, PSYOPS, government infrastructure vulnerability
c) Commanders are responsible to implement defensive IO at all times
d) Co-ordination of IO will be carried out by an Information Operations Co-ordination Cell (IOCC)

Information Operations Coordination Cell

The IOCC concept has been designed to provide IO inputs to operational plans developed by the National military staff. The composition is seen to be flexible, customized to meet the needs of specific requirements. While the concept has been accepted, it has yet to be activated consistently for exercises or operations. The inclusion of IO requires major re-thinking by staff and re-alignment of planning processes by all concerned. It will undoubtedly be some time before consideration of IO becomes second nature to our planners and staff.

Role of Research and Development

From the earliest stages of IO concept development, it was clearly stated that the R&D community needs to be engaged in supporting the CF IO process. Each of the IO processes defined in the IO paradigm, protection, exploitation, acquisition and engagement need a significant R&D contribution for the CF to fully carry out its role. This role becomes a particular challenge with the evolving relationship between civilian and military technologies and requirements.

J6 Coordination Role

Within the CF, the J6 have been given the role of coordinating the IO development. A small IO staff forms the permanent nucleus of the IO coordination role and provides the constant IO visibility required to implement the change. This role includes not only CF and Government of Canada functions but our international relationships as well. They have the advantage of having implemented the IO concepts and establishing the structures to accommodate the requirements.

LESSONS LEARNED, BEING LEARNED, TO BE LEARNED

With the National Government

The basic concept that was initially established and maintained throughout the IO developmental process was that IO was a strategy and that it encompasses an information environment that exceeds that of the military alone. This holistic approach therefore requires contributions from the whole to function effectively, otherwise the Department of National

Defence (DND) would operate in a vacuum. The greatest difficulty DND has encountered is probably the reluctance of the Government of Canada to accept the leading role that is necessary in the holistic approach; and a role that all participants engaged in the area have expressed as necessary. National Defence sees itself as a significant but wholly cooperative member integrated into a larger national role.

Another difficulty that arises in Canada's situation has been its reliance on incorporating IO developments and studies originating abroad into a Canadian position. This will diminish Canada's role as an innovator in IO, both in civilian and military fields. However, it can argued that by taking the cautious approach, Canada will avoid repeating earlier mistakes; but at the cost of losing its uniqueness which it could have established. In this process however, DND is left to forge ahead in the IO arena without the benefit of strong central leadership.

It is therefore not surprising, that Canada remains the only Western/technologically advanced nation without a government sponsored computer incident response team. With the holistic approach taken by DND, the concept of information as a national asset is a fundamental premise, and as a result requires appropriate national security to be considered as well.

With the Department of National Defence

Certainly an advantage of the holistic approach has been the relatively smooth development of DND policy and doctrine. In particular, the integration of individual service policy and doctrine has been made easier. Trying to achieve a departmental consensus, let alone a national consensus, is much more difficult if it is being driven from the bottom up.

The introduction of IO into the Department has created the opportunity for new roles to be established, especially in some traditional areas. For example, the J6 that has traditionally been responsible for communications and electronic support finds itself potentially controlling "operational weapons" in the form of computers and networks. While the J6 in Canada has firmly believed in the lead role of the operational elements of the department when it comes to IO, it has been given greater responsibilities in areas that have not been traditionally within their mandate.

As the slow transition to the IO Group took place, it was obvious that a number of traditional roles and structures were going to be changed. It has been a characteristic of many organizations, not only within DND but elsewhere as well, that there is the tendency to consolidate and protect the existing structures and functions. Yet with a holistic approach to IO, and in organizational development in general, rather than becoming more inward and protective, it is far more beneficial to leverage skills and functions. This is a difficult lesson to learn.

With the new IO concept, it is also necessary to develop personnel with new skill sets, and to be placed into new, non-traditional roles. It follows that new opportunities have to be made for training, and within the personnel system, recognition for the new roles and responsibilities that are associated with carrying out IO related functions. The holistic approach has made these opportunities slower in evolving as traditional roles and training still receive the greatest attention and support. No longer can military personnel be expected to be posted into a new position for three years and then move on. The training and demands of working within IO requires a longer commitment and ongoing training to remain at the lead edge. These issues still need further refinement within the CF to fully benefit from an IO program.

Research and Development

The military R&D community finds itself in a particularly difficult position. First, it must compete forever diminishing resources within government. Second, and more importantly, it must compete against the civilian/commercial competitors that have been at the technological lead edge for a number of years. This also means that the traditional R&D role needs to change or adapt to one of being a leading edge integrator rather than innovator. This is particularly relevant in the Canadian situation where Canada seldom produces complete systems, but rather provides components or produces hybrid systems that have integrated numerous technologies and concepts. As well, to maintain pace with the civilian and commercial sectors, the former concepts of long, medium and short-term research need to be re-thought. Because of the increased integration required, it is almost a necessity for the R&D scientist to work hand-in-hand with the operator to be fully integrated into the IO operational strategy.

General Comment

From the initial IO working groups, it was made abundantly clear that no new financial allocations could be expected for IO activities. It was expected that existing funds be re-allocated to meet the needs. In a holistic approach, the opportunities to find re-allocated funds are much fewer since every organization and manager will be trying to protect their limited resources. Even the US approach of working up from the individual service elements eventually reaches a point where there is no further opportunity to re-allocate or adjust funding. Since IO has been introduced as a new concept with its own set of threats and vulnerabilities, it does become necessary to inject new funding and personnel into the area.

ACKNOWLEDGEMENTS

There have been many individuals that have contributed to the IO development within the Department of National Defence and without which, I would not have had the opportunity to prepare the accompanying paper. Among the many individuals that need mentioning are: Robert Garigue, currently Chief of IT Security/CIO office for the Province of Manitoba; Dr. Leroy Pearce, Scientific Technical Advisor to the CIO, DND; Col Randy Alward, Commander IO Group, DND; LCol Alan Smith, J6 IO, SqLeader Barry Horne, Majors Alan McGreer and Randy Colmar, exchange officers in J6IO; Maj Doug Smith; Dr. Brian Harrison; Capt Luc Dandurand and WO Bruce Fraser of the IO NVAT team; Dr. Brian Eatock H/IO and Mr. Gordon Marwood, Chief Scientist, Defence Research Establishment Ottawa.