National Defence | Défense nationale

B-GG-005-004/AF-010

CF INFORMATION OPERATIONS

Issued on Authority of the Chief of the Defence Staff

OPI: J6 Information Operations **1998-04-15**

Canada

PREFACE

1. SCOPE. This publication is the subordinate document to *Canadian Forces Operations Manual, B-GG-005-004/AF-000*, Chapter 32, Information Operations. This publication provides guidance for information operations (IO) by the CF throughout the full range of military operations. It addresses IO principles relating to both offensive and defensive IO and describes responsibilities for planning, coordinating, integrating, and deconflicting CF IO. Guidance concerning intelligence support to IO, Defence and interagency relationships, and IO in training and exercises also is provided.

2. PURPOSE. This publication has been prepared under the direction of Defence Planning Guidance and by the authority of the Chief of Defence Staff. It sets forth doctrine to govern the activities and performance of the Canadian Forces in joint operations as well as the doctrinal basis for Canadian military involvement in combined and interdepartmental or interagency operations. It provides military guidance for the exercise of authority by Commanders and prescribes doctrine for joint operations and training. It provides military guidance for use by the Environments in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the Commander from organizing the force and executing the mission in a manner the Commander deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. APPLICATION. This publication is authoritative but not directive. Commanders will need to exercise judgement in applying the guidance it provides to accomplish their missions. If conflicts arise between the contents of this publication and the contents of Environmental publications, this publication will take precedence for the activities of joint forces unless the Chief of Defence Staff, normally in coordination with the Environmental Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and guidance ratified by DND and the CF. For doctrine and procedures not ratified by Canada, Commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and not in direct conflict with DND/CF policies or directives. Where conflicts arise between multinational and DND/CF doctrine and procedures, Commanders should petition higher level authorities for guidance as required.

This Page Intentionally Left Blank

TABLE OF CONTENTS

PAGE

LIST OF FIGURES

PAGE

CHAPTER 1

INTRODUCTION

> ***"Generally, in battle, use the normal force [direct approach] to engage; use the extraordinary [indirect approach] to win"***
>
> **Sun Tzu, *The Art of War*, tr. Griffith**

101. POLICY

1. NDHQ Policy Directive for Information Operations outlines IO policy within DND/CF and delineates specific IO authorities, operating principals and responsibilities.

a. General

(1) The strategic aims of IO are to secure peacetime national security objectives, deter conflict, protect the DND and CF information and information systems, and to shape the information environment. If deterrence fails, IO seeks to achieve Canadian information superiority to attain its objectives against potential adversaries in times of crisis and/or conflict. IO seeks to persuade decisionmakers at all levels to peacefully, or with the least amount of resistance, accept an outcome beneficial to Canadian interests through the use of information. IO can be used to influence decision-makers at all levels, from the heads of state, to troops in contact on the front lines or the general populace on either or both sides of a dispute. Information is the means; decisionmakers are the objective.

(2) The IO paradigm, which applies to all who engage in Defence decision making, from the strategic to the tactical levels, is shown at figure 1-1.

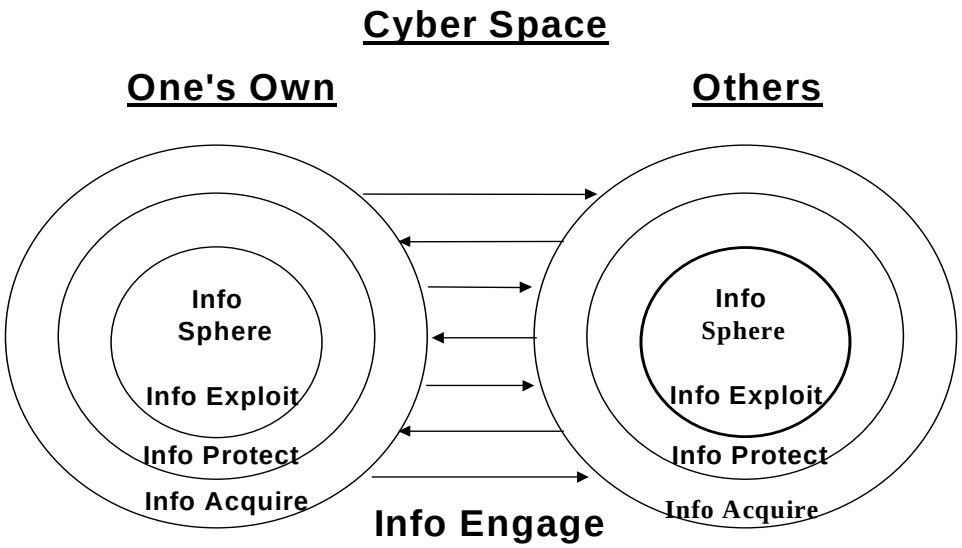

Figure 1-1. An Information Operations Paradigm

Information, which has always been key to decision making, is portrayed as an information sphere (critical resource or asset) and represents the sum total of available information from all sources (media, meteorological, open source, etc.). Information acquisition is the process by which our 'info sphere' will be populated with both friendly and adversary information. Information protection is the process by which this environment will be secured from our adversaries and ourselves (unintentional manipulation, destruction, etc). Information exploitation is the process by which information is presented to the decision maker for his use in a quantity, quality, form, location and time of his choosing. Finally, information engagement is the process by which any adversary's decision cycle can be adversely affected through denying him the ability to acquire information, nullifying his protection measures, neutralizing his exploitation tools, corrupting his information or destroying his C2 systems. The change being thrust on the world by the information revolution is driving the above IO paradigm.

(3) Information itself is becoming a strategic resource vital to national security. Information and its flow is fundamental to the sovereignty of a nation. Modern societies are dependent on a sophisticated civil/military information infrastructure that underpins every aspect of society in most developed countries. Defence, commerce, transportation and communications are just a few examples of key sectors which now depend heavily on information technology to function effectively. However, this dependency and its ensuing vulnerability has created a double-edged sword. Armed with an effective means of acquiring, exploiting and affecting another nation's information, advantages can be gained ranging from political, industrial, commercial, to defence. As demonstrated in the Gulf War, military commanders can minimize casualties on both sides by employing "soft kill" techniques which interdict and disrupt vital civil and military information networks, thus incapacitating opposition. The side which is able to achieve a degree of Information Superiority by protecting its own capabilities, while exploiting those of an actual or potential adversary, will have the greatest chance of survival and success. Moreover, the vulnerability of information systems, combined with the potential for far-reaching damage, also makes this an attractive target for smaller groups or individuals (e.g. terrorists). It is therefore implicit that the protection of one's own information capabilities and the exploitation of any potential adversary's information capabilities have become a fundamental principle of a nation's security.

(4) Throughout the continuum of conflict, the DND/CF must be capable of maximizing the capabilities and safety of our own forces through the effective use of IO, while safeguarding against any adversarial IO effort directed toward us or our Allies. The goal of IO is to influence decision-makers by affecting adversary information while exploiting and protecting one's own information. Proactive IO doctrine and procedures must be implemented throughout the entire span of the command decision-making cycle and not limited solely to those areas involving automated systems. This will force fundamental reviews of how information is handled and by whom, where and when that information is disseminated and through what means. As a result, the impact of IO will inevitably be far-reaching and profound.

(5) Information Operations are defined as actions taken in support of political and military objectives which influence decision makers by affecting other's information while exploiting (fully utilizing) and protecting one's own information. This also includes IO conducted throughout the continuum of operations to achieve or promote specific military objectives over a specific adversary or adversaries. Defensive IO activities are conducted on a continuous basis, in both peacetime and war, and are an inherent part of force employment across the full range of military operations. IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval.

(6) As an integrating strategy, IO focuses on the vulnerabilities and opportunities presented by the increasing dependence on information and information systems by the armed forces of Canada, our allies, as well as any potential adversary. For this reason, employment of IO has become essential to achieving our military objectives in support of the Commander's plan. In the DND, the ultimate strategic goal of offensive IO is to affect a human decision-maker to the degree that an adversary will cease actions threatening to Canadian national security interests. At the tactical and operational levels, IO target and protect information, information transfer links, information

gathering and processing nodes, and human decisional interaction with information systems. IO may have their greatest impact in peace and the initial stages of crisis. Ultimately, IO is not only essential to achieving goals and securing national interests, but is also a key means by which forces may be used with greater effect and suffer fewer losses. See Figure 1-2.

Figure 1-2. Information Operations as an Approach

(7) IO is not a concept which is exclusive to the military. Instead, it must be embraced as a government-wide strategy. However, a strong IO capability is one of the many components offered by the Canadian military. IO can support overall Canadian Government strategic engagement policy throughout a range of military operations. The effectiveness of deterrence, the projection of national influence, and other strategic concepts is greatly facilitated by the ability of Canada to affect the perceptions and decision making of others. In times of crisis, IO can help deter adversaries from initiating actions detrimental to the interests of Canada or its allies or to the conduct of friendly military operations. If carefully conceived, coordinated and executed, IO can make an important contribution to defusing crises; reducing the period of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts; and forestalling or eliminating the need to employ forces in a combat situation. Thus, IO in peacetime, crisis and conflict, at both the national-strategic and theatre-strategic levels, require close coordination among a wide variety of elements of the Canadian Government to include DND. See Figure 1-3.

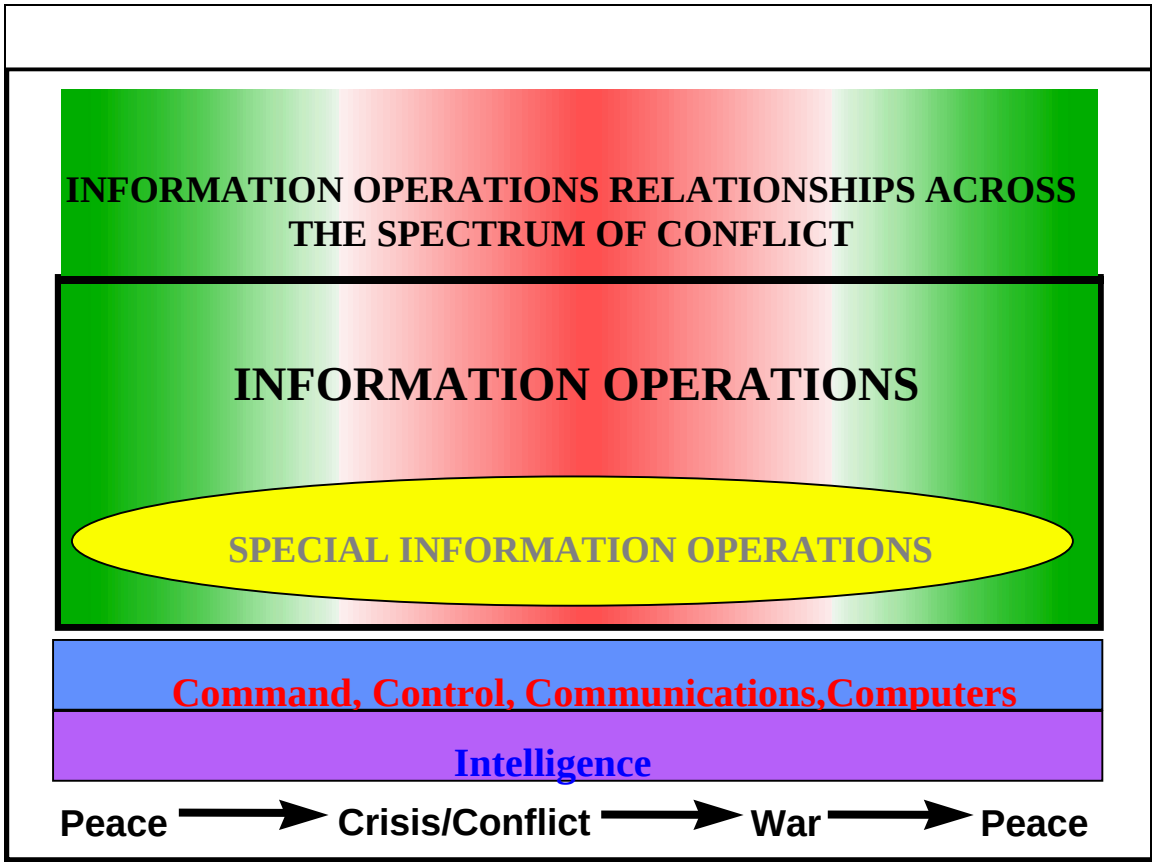

Figure 1-3. Information Operations Relationships Across Spectrum of Conflict

(8) IO can be waged in wartime within and beyond the traditional military battlefield. As a subset of IO, command and control warfare (C2W) is an application of IO in military operations that specifically attacks and defends the command and control (C2) target set. The C2 target set includes targets which affect the adversary's ability to exercise command and control over his military forces. However, the capabilities and disciplines employed in C2W (psychological operations (PSYOP), deception, operations security (OPSEC), electronic warfare (EW), and physical destruction) as well as other less traditional methods focused on information systems can be employed to achieve objectives that are outside the C2 target set. (See Chapter 2, Para 201 for further C2W information)

(9) Specific IO policy guidance is set forth in NDHQ Policy Directive for Information Operations as follows:

(a) evaluate the implications of IO when planning and executing operations, developing policy, defining and validating new requirements, conducting research and development and/or acquiring new systems, to achieve a favorable outcome quickly and decisively, with minimum losses and adverse collateral effects;

(b) harmonize DND/CF IO plans and activities with overall national objectives and strategies, as well as specific military objectives, to achieve a deliberate, coherent effect on any decisionmakers;

(c) integrate, during both the planning and execution of operations, offensive and defensive IO capabilities and activities;

(d) coordinate all offensive IO between the disciplines involved. These disciplines may include psychological operations (PSYOP), deception (OPDEC), electronic warfare (EW), intelligence, computer network attack (CNA), destruction, and special information operations (SIO);

(e) coordinate all defensive IO between the disciplines involved. The defensive IO disciplines may include information security (INFOSEC), physical security, operations security (OPSEC), counter deception, counter psychological operations, counter intelligence (CI), electronic warfare (EW) and SIO;

(f) coordinate IO plans and capabilities, including development of new tactics, techniques, procedures and technology with other government departments or agencies;

(g) include Public Affairs (PA) as an integral component of IO. PA activities are governed by existing statutes, laws, policies and principles and shall not compromise nor be compromised by IO orders or directives;

(h) include civil affairs (CA) as an integral component of IO. CA activities are important to IO because of their ability to interface with key organizations and individuals in the information environment;

(i) vigorously pursue Information Protection (IP) activities to protect DND/CF information and information systems.

"We will have to say that in any cause the decisive role does not belong to technology - behind technology there is always a living person without whom technology is dead."

Mikhail Frunze, quoted in Gareyev, Frunze, Military Theorist, 1985

b. Responsibilities. Refer to NDHQ Policy Directive for Information Operations for a listing of specific authorities, operating principals and responsibilities of key IO individuals and commands or organizations. Individuals, commands or organizations not specifically addressed in above documents with substantial influence or participation in IO are listed below:

(1) Commanders

(a) Plan, exercise, and conduct IO in support of national goals and objectives.

(b) Integrate IO capabilities into deliberate and time sensitive action planning in accordance with appropriate policy and doctrine to accomplish their assigned missions.

(c) Integrate IO capabilities into all levels of planning and operations to leverage available combat power through the massing of physical and psychological effects

(d) Utilize the IOCC or similar concept within operational level headquarters and subordinate staffs to integrate effectively IO-related activities by various supporting components.

(e) Incorporate IO tactics, techniques, and procedures into exercises and training events.

(f) Identify IO capability requirements and submit capabilities deficiency statements to the ECS or DCDS/DND as appropriate for validation.

(g) Capture IO lessons learned from after-action reviews and submit them to the appropriate Lessons Learned OPI as part of the after-action report.

(2) Information Operations Coordination Cell (IOCC)

(a) As requested, provides direct support to Commanders.

(3) Through the Operational Research Staffs:

(a) Ensures modeling & simulation (M&S) efforts are coordinated to eliminate duplication of effort and helps focus on the development of systems that fulfill Commanders and Environmental IO training and exercise requirements.

(b) Stay apprised of other agency M&S efforts that could support Commanders and Environmental IO requirements.

(c) Coordinates and assists the Joint Staff, and Environmental staffs in developing IO doctrine.

(4) All elements within DND/CF. Adopt a risk management approach to protection of their information, information systems, and information-based processes based on potential vulnerability to IO.

102. TERMINOLOGY

1. The terms listed below and selected other terms used in this publication as well as all abbreviations used are listed in the glossary. **The basic definitions and concepts in this chapter are critical to understanding the rest of this publication.**

a. “Information” is defined as that which informs or has the potential to inform. Information is a combination of content and meaning communicated or received, represented by symbols and media or conduit, used or useable in a particular context. (Source: Burk and Horton, Infomap) The same information may convey different meanings and be interpreted differently by different recipients. Moreover, it may also be put to different uses by information gatherers and users, including the operations and intelligence communities.

b. An “information system” is the assembly of equipment, methods and procedures, and if necessary personnel, organized so as to accomplish specific information processing functions. (Source: NATO ADatP-2)

c. “Information-based processes” are processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes. (Source: US DoD JP 1-02) Information-based processes are found in all facets of military operations and across the spectrum of operations, and in other elements of national power. Information-based processes are included in all systems and components thereof that require facts, data, or instructions in any medium or form to perform designated functions or provide anticipated services.

d. “Information Operations” means actions taken in support of national objectives which influence decision makers by affecting other's information while exploiting and protecting one's own information. This also includes IO conducted through the continuum of operations to achieve or promote specific objectives over a specific adversary or adversaries. (Source: NDHQ Policy Directive for IO)

(1) IO requires the close integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of C2 with intelligence support. The full value of IO can only be achieved through the effective integration of many disciplines. See Figure 1-4. There are two major subdivisions within IO: offensive IO and defensive IO.

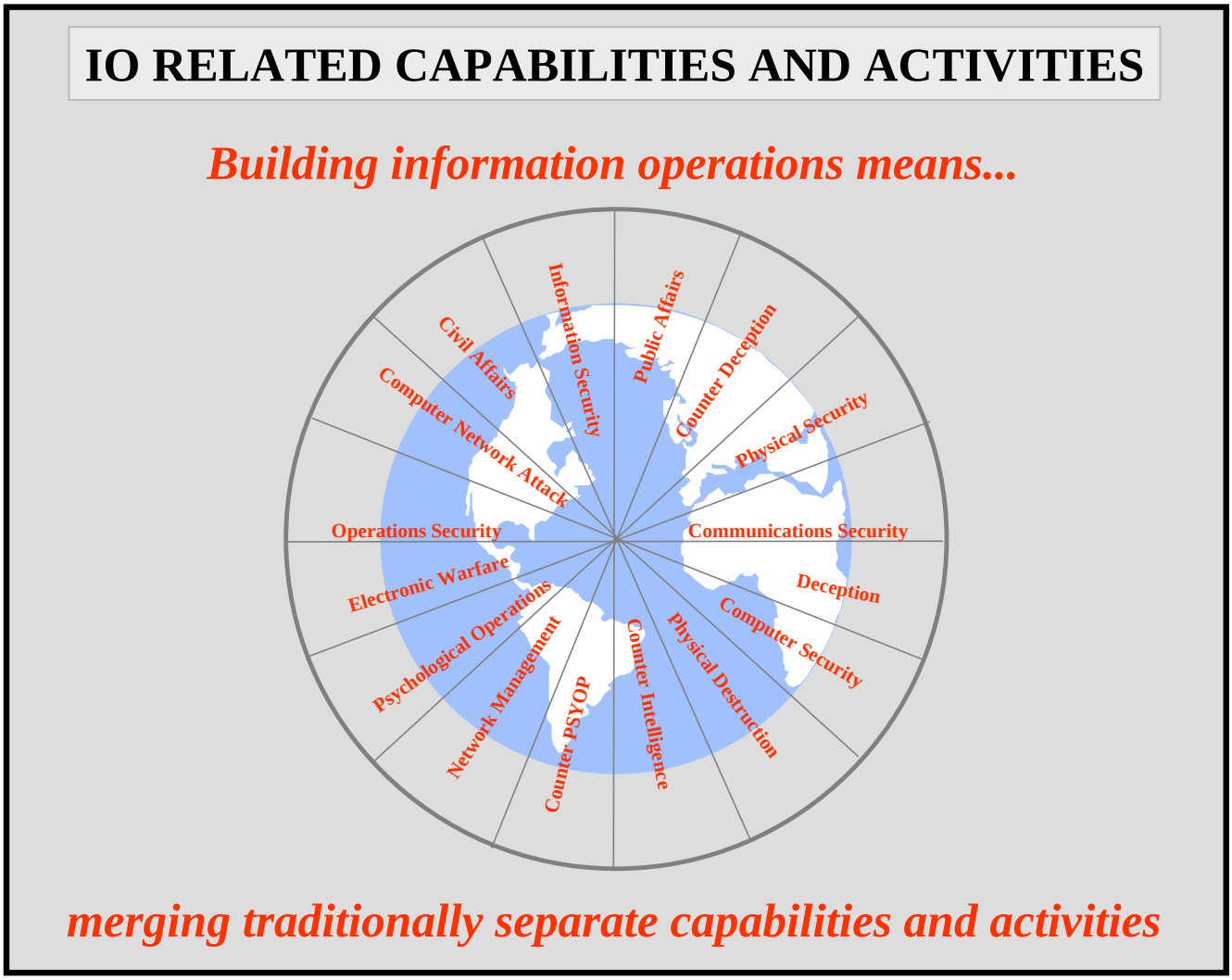

Figure 1-4. IO-Related Disciplines

(2) Offensive IO includes actions taken to influence actual or potential adversarial decision makers. This may be done by affecting an adversary's or potential adversary's use of or access to information and information systems. Offensive IO can include using PSYOP, deception, EW, intelligence, computer network attack, physical destruction, and special information operations (SIO).

(3) Defensive IO includes actions taken to protect one's own information and ensure friendly decision makers have timely access to necessary, relevant and accurate information. Defensive IO also ensures friendly decision makers are protected from any adversary Offensive IO efforts. Defensive IO strives to ensure the friendly decision making process is protected from all adverse effects, deliberate, inadvertent or accidental. Defensive IO is a process that integrates and coordinates policies, procedures, operations, intelligence, law, and technology.

e. "Information superiority" is the capability to acquire, exploit and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same. (Source: NDHQ Policy Directive for IO). Information superiority may be all pervasive in an area of operations (AO) or it may be function- or aspect-specific, localized, and temporal.

f. Special Information Operations (SIO) is IO of a sensitive nature which, owing to its potential effect or impact, security requirements, or risk to the national security of Canada, requires a special review and approval process. (Source: NDHQ Policy Directive for IO)

> ***"Force has no place where there is need of skill."***
> **Herodotus, *The Histories of Herodotus***

103. FUNDAMENTALS OF INFORMATION OPERATIONS

1. General

a. Increasingly complex information systems are being integrated into traditional military operations such as command, transport; logistics, and intelligence. Many of these systems are designed and employed with inherent vulnerabilities that are in many cases the unavoidable consequences of enhanced functionality, efficiency, and convenience to users. The low cost associated with such technology makes it efficient and cost effective to extend the capabilities (and vulnerabilities) to an unprecedented number of users. The broad access to, and use of, these information systems enhances all military operations. However, these useful capabilities induce dependence, and that dependence creates vulnerabilities. These vulnerabilities are a double-edged sword--on one hand representing areas that components must protect while on the other hand creating new opportunities that can be exploited against adversaries. See Figure 1-5.

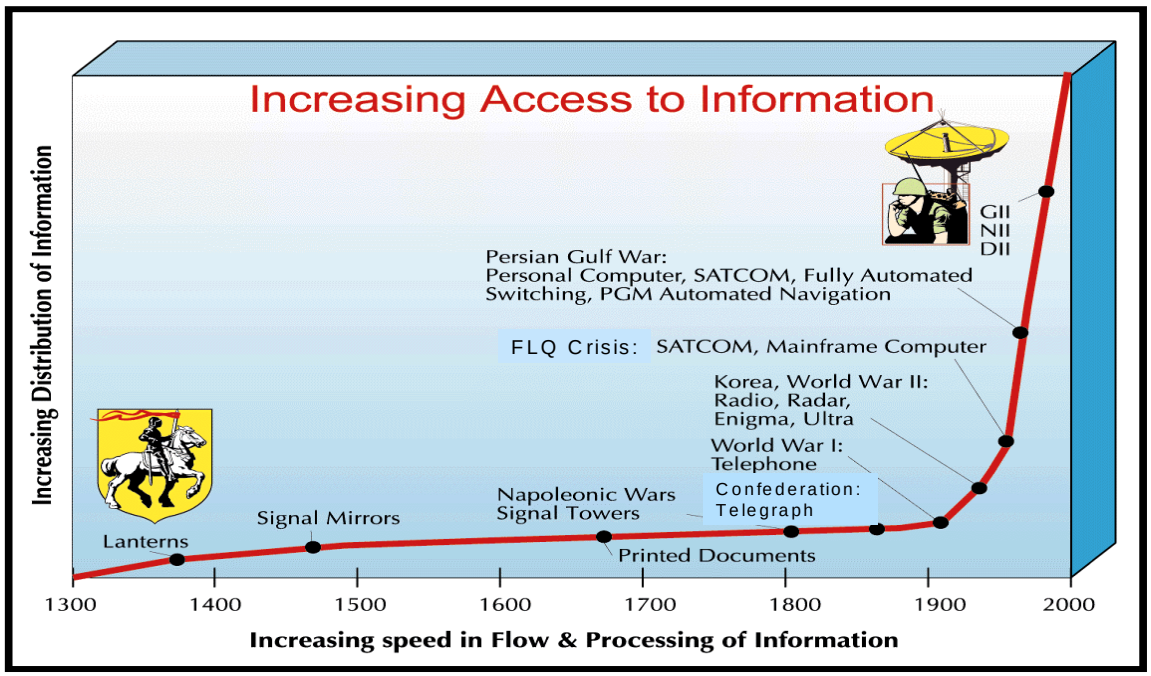

Figure 1-5. Increasing Access to Information

b. While retaining the emphasis on influencing the decision maker, IO may also be able to capitalize on the growing sophistication, connectivity, and reliance on information technology. An IO target set can be information or information systems in order to affect the information dependent process, whether human or automated. Such information dependent processes range from Cabinet level decisionmaking to the automated control of key commercial infrastructures such as transportation and electric power.

c. Many different systems, disciplines, and techniques must be integrated to achieve a coherent IO strategy. Intelligence and communications support is critical to conducting offensive and defensive IO. The thoughtful design and correct operation of information systems are fundamental to the successful conduct of IO in general, but defensive IO predominately.

d. The IO strategy must support the national military strategy and shall require coordination, participation, and support, by other Canadian departments and agencies as well as commercial industry. Although strategic and operational DND information flows depend on commercial infrastructures, the protection of these infrastructures falls outside the authority and responsibility of the DND. The DND must assist in demonstrating to service providers the compelling need for a collaborative, teamed approach in crafting solutions--not just to support the DND and to protect Canadian national security, but to protect their own proprietary interests as well. Offensive IO actions may also require interagency deconfliction and cooperation. See Figure 1-6.

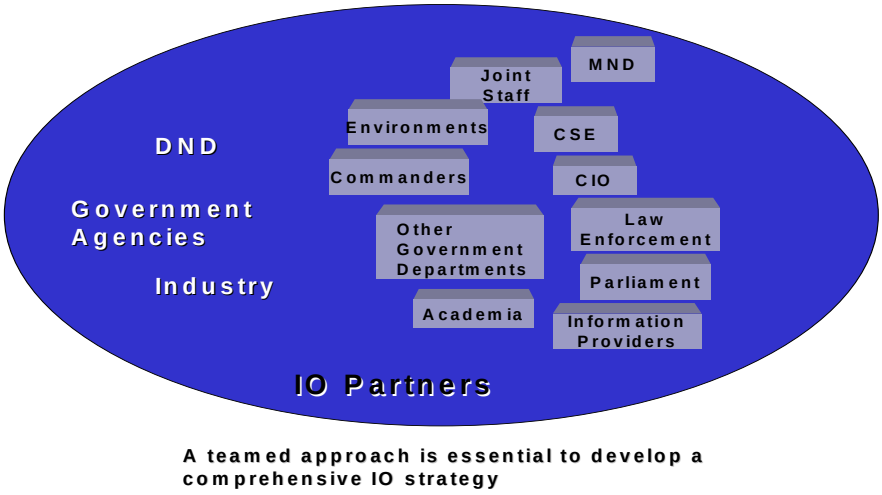

Figure 1-6 IO Partners

2. Information Environment. The continuing growth of information systems and technologies offer nearly unlimited potential for exploiting the power of information in joint warfighting. The labels placed on information systems and associated networks may be misleading as there are no fixed boundaries in the information environment. Open and interconnected systems are coalescing into a rapidly expanding global information infrastructure (GII) that enfolds the Canadian National Information Infrastructure (NII) and the DII.

a. The DII is embedded within and deeply integrated into the NII. Their seamless relationship makes distinguishing between them impossible. The two share terrestrial telecommunications networks, a variety of information databases, and satellite communications networks. These infrastructures connect geographically separated forces and span international boundaries. See Figure 1-7.

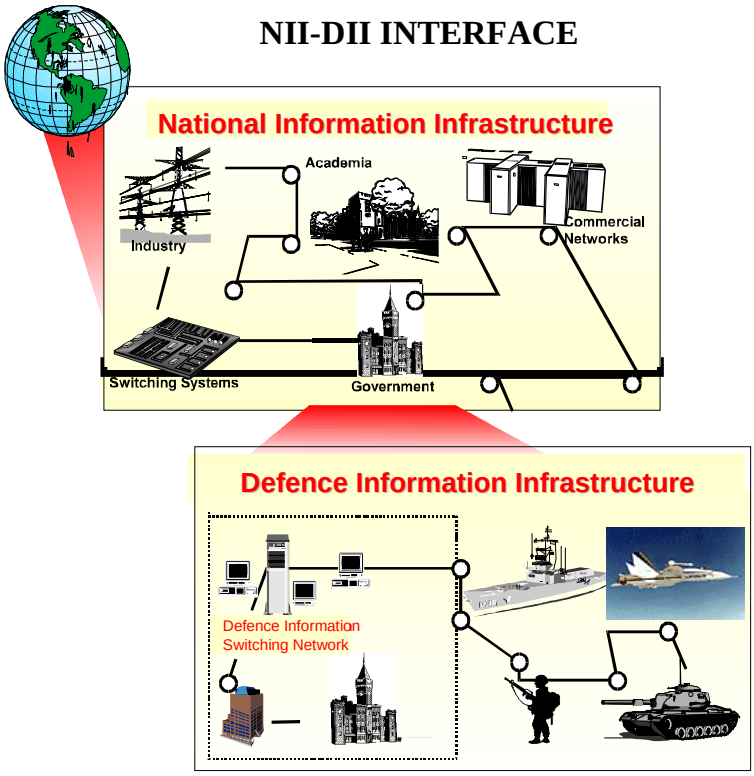

Figure 1-7. NII-DII Interface

b. The GII is the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The GII includes more than just the physical facilities used to store, process, and display information. The personnel who handle the transmitted information constitute a critical component of the GII.

c. The NII is similar in nature and purpose to the GII but relates in scope only to a national information environment.

d. The DII is the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DND local, national, and worldwide information needs. The DII connects DND mission support, C2, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the NCCIS. It includes C2, tactical, intelligence, and commercial communications systems used to transmit DND information.

3. National Command & Control Information System (NCCIS) Extensions. Commanders at all levels should understand the nature, complexities, and dependencies the GII, NII, and DII have during the various phases of an operation, warning, preparation, deployment, employment and redeployment, across the range of military operations.

a. The successful conduct of warfare in the information age requires access to information available outside the theatre of operations. Information infrastructures no longer parallel traditional command lines, and warfighters need frequent, instant, and reliable access to information at locations in Canada as well as in theatre. This may require the extension of our information infrastructure beyond the established peacetime information environment. For example, transport and sustainment of forces

are highly dependent on commercial "reach-back" infrastructures that include international telecommunications, the public switched network, transportation systems, and commercial electric power grids. Joint forces require secure video teleconferencing, detailed imagery from national and/or allied sources, intelligence, logistics, and other support data from diverse locations. Joint forces must have assurance that this expanded infrastructure can attain the level of protection required to assure mission success. The nature of these information infrastructures complicates a commander's ability to control the flow of information or dynamically manage available information and telecommunications resources. To support offensive operations, commanders may reach-back to employ information engage capabilities and techniques that provide an information advantage in their AO.

b. CF dependence on the national and international information infrastructure and the subsequent exposure to a full range of threats from computer hackers through criminals, vandals, and terrorists to nation states have brought focus and compelling relevance to emerging IO concepts. The authority to implement an appropriate level of protection for these infrastructures may lie outside of the DND and the Canadian government. Therefore, the DND/CF must work in the various interagency forums to demonstrate to service providers the compelling need for a collaborative, teamed approach to ensure friendly forces have access to timely and relevant information wherever and whenever needed.

c. The unique characteristics of advancing information-based technologies have set in motion revolutionary capabilities that will enhance and support military operations into the next century. See Figure 1-8.

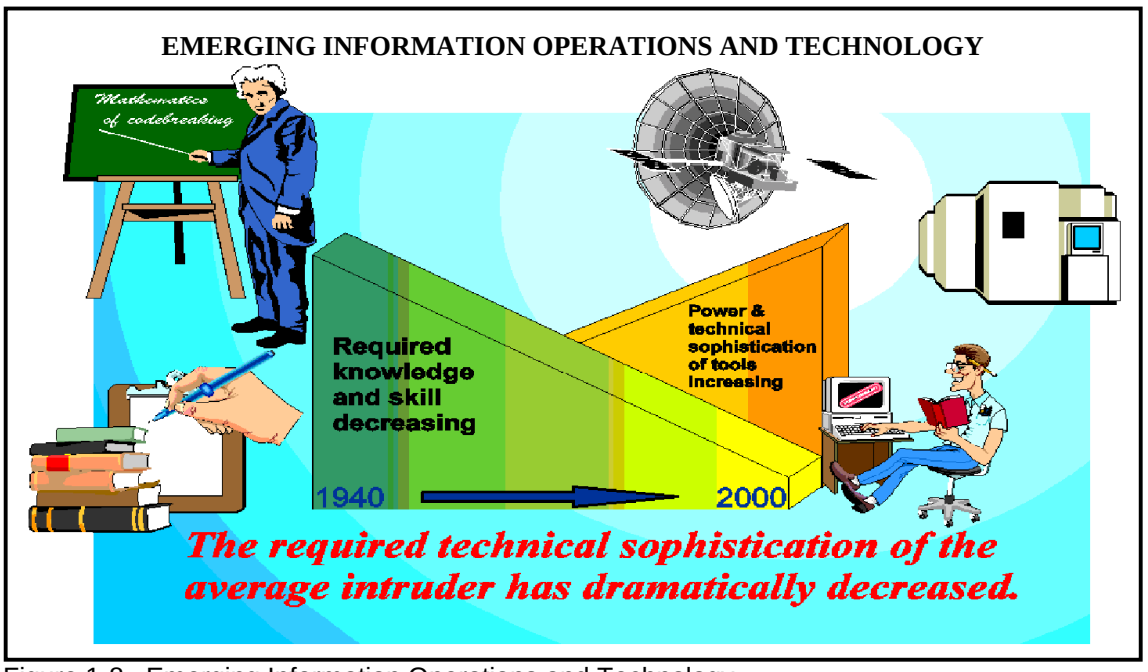

Figure 1-8. Emerging Information Operations and Technology

4. IO Target Set. IO targets are determined by the Commanders global objectives and are influenced largely by in-depth intelligence analysis. Intelligence support to the Commander should include the development of databases and templates to determine the vulnerabilities of an adversary's information, information-based processes, and information systems. Conversely, the IOCC should identify the vulnerabilities of friendly information, information-based processes, and information systems that an adversary is likely to target. Examples of IO targets are shown in Figure 1-9.

a. As shown in Figure 1-9, there are many types of IO targets. Early identification of critical elements with respect to specific IO targets is essential to successful offensive IO and defensive IO. Offensive IO may target only a key element of a specific critical adversary IO target set and attain great success. Conversely, understanding the nature of the threat will help defend against adversary offensive IO capabilities.

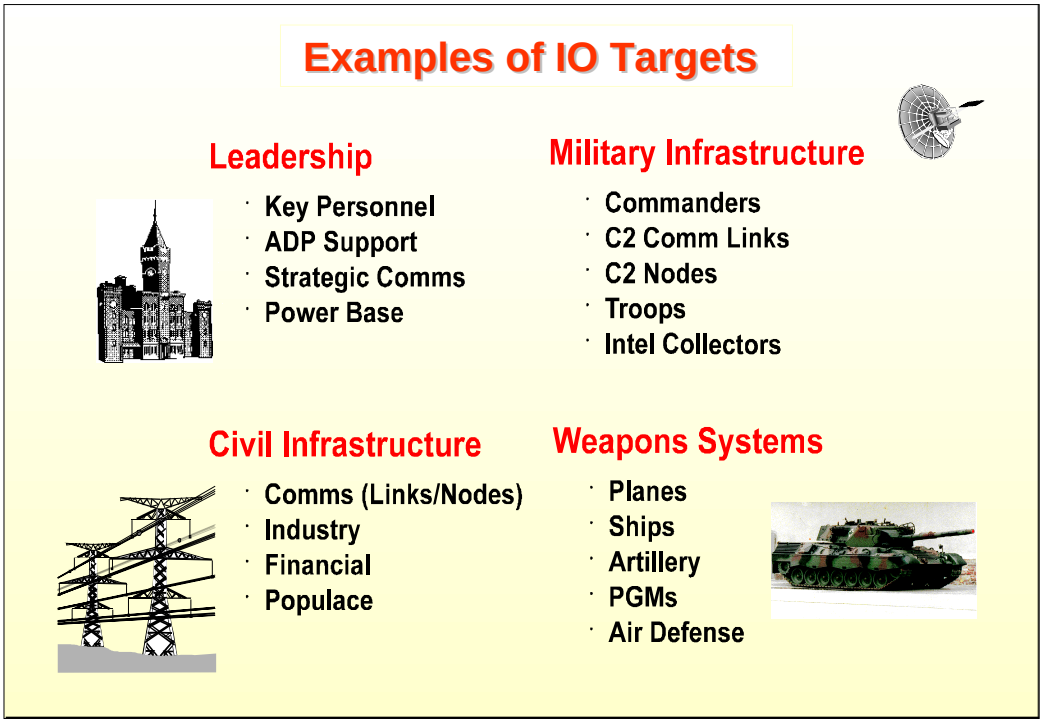

Figure 1-9. Examples of IO Targets

b. With the ultimate goal of influencing the decision maker, C2 remains a substantial target for IO. Commercial communications systems linked to friendly and adversary C2 systems offer unique challenges to offensive targeting and defensive protection.

c. Examples of key areas of warfare support comprising potential offensive target sets and requiring protection include, but are not limited to, logistics, intelligence, and non-C2 communications systems. Friendly commercial infrastructure also may be targeted by an adversary's offensive capabilities; so to is an adversary's commercial infrastructure the potential target for friendly offensive capabilities.

5. Command and Control Warfare (C2W)

a. C2W is an application of IO in military operations and is a subset of IO. C2W specifically attacks adversary C2 targets while defending the friendly C2 target set. The C2 target set includes targets which affect the adversary's ability to exercise command and control over his military forces.

b. C2W is the integrated use of all military capabilities including OPSEC, deception, PSYOP, EW, and physical destruction, supported by all source intelligence and Communication and Information Systems (CIS), to deny information to, influence, degrade, or destroy an adversary's C2 capabilities while protecting friendly C2 capabilities against similar actions.

c. C2W applies across the range of military operations and at all levels of conflict. C2W is both offensive and defensive.

(1) C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system.

(2) C2-protect. Maintain effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.

6. Other Integral Components of IO

a. Public Affairs (PA) seek a timely flow of information to both external and internal audiences. Coordination of PA and IO plans is required to ensure that PA initiatives support the commander's overall objectives. PA and IO efforts will be integrated consistent with policy or statutory limitation.

b. Civil Affairs (CA) activities are important to IO because of their ability to interface with key organizations and individuals in the information environment. CA can support and assist IO objectives by coordinating with, influencing, developing, or controlling indigenous infrastructures in foreign operational areas.

7. Intelligence Support

a. Intelligence support is critical to the planning, execution, and assessment of IO. The joint staff intelligence (J-2) representative(s) assigned to support IO should be the liaison for intelligence support for all IO planning.

b. Intelligence must be readily accessible, timely, accurate and sufficiently detailed to support an array of DND IO requirements, to include research, development, and acquisition and operational support.

c. The conduct of sophisticated IO requires unique and detailed intelligence never before asked of intelligence collection agencies and activities. Intelligence Preparation of the Battlespace (IPB) is vital to successful IO.

d. Intelligence products must support IO planning, provide analysis of a potential adversary's IO vulnerabilities, allow determination of a potential adversary's IO capabilities and intentions, provide Indications & Warning (I&W) of any potential threat and contribute directly to the Precautionary Measures System.

e. Guidance for specific intelligence support required for offensive and defensive IO is provided in Chapters II, "Offensive Information Operations," and III, "Defensive Information Operations," respectively.

> ***"Nothing is more worthy of the attention of a good general than the endeavor to penetrate the designs of the enemy."***
> **Niccolo Machiavelli, *Discourses***

8. IO as an Enabler to Commanders

a. Rapidly advancing information-based technologies and an increasingly competitive global environment have thrust information into the centre stage in society, government, and warfare in the 21st Century. Information and information-based technologies are pervasive and impact every facet of crisis and conflict from the warning, preparation, deployment, employment and redeployment phases of CF operations to the plethora of forces and weapons systems employed by Commanders. See Figure 1-10.

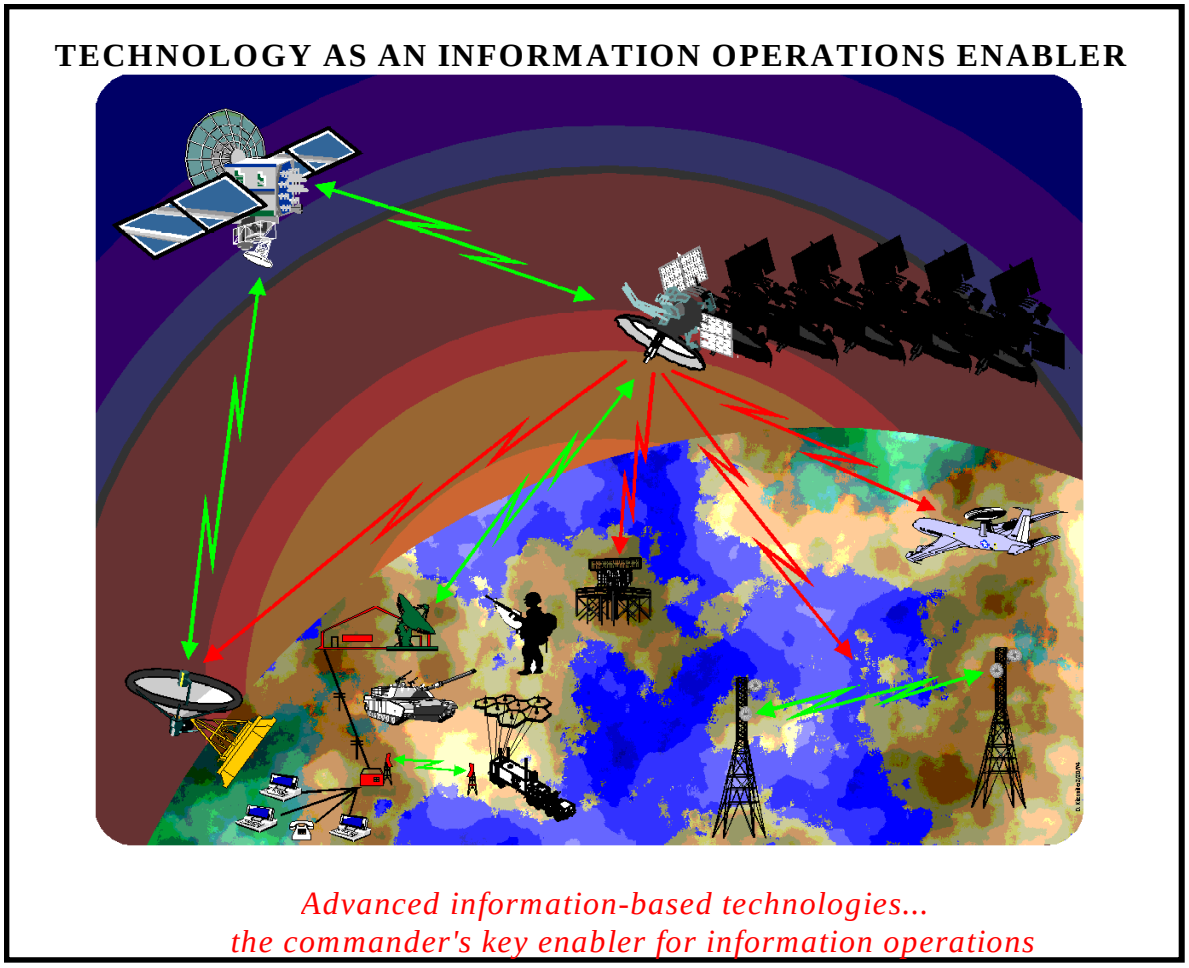

Figure 1-10. Technology as an Information Operations Enabler

b. The revolutionary changes in information technologies present to commanders unique opportunities utilizing IO to affect the actions of others through the integrated use of all capabilities. It is now possible for commanders to mass both physical and psychological effects at the right time and place to leverage their combat power and influence decision makers by using IO and its supporting information technologies.

c. Military operations and the precise application of combat power are critically dependent on many simultaneous and integrated activities that, in turn, depend on information and on information systems, especially those activities associated with critical C2 processes. Some of these activities include conducting strategic deployment, sustaining theatre forces, ensuring force protection--both in garrison and in forward-deployed areas, preserving theatre strategic C2, and developing strategic and theatre intelligence.

d. Information itself is becoming a strategic resource vital to national security. This reality extends throughout the continuum of conflict. Increasingly complex information systems are being integrated into traditional disciplines such as transport, logistics and intelligence.

e. IO can be used positively to reinforce common interests and objectives of multinational partners and to deter adversaries from initiating actions detrimental to interests of Canada or partners, or to the conduct of friendly military operations.

f. If carefully conceived, coordinated, and executed, IO will make an important contribution to operational commanders' efforts to defuse crises and return to peace, reduce periods of confrontation, enhance the impact of other elements of national power, and forestall or eliminate the

need to employ combat forces. However, simultaneously IO must also prepare the battlespace for conflict.

During the Persian Gulf War, defensive information operations ensured that the Coalition soundly defeated Saddam Hussein's political strategy, which was aimed at influencing the decision-making coalition nation leadership. Immediately after the invasion of Kuwait, Iraq began campaigning for public support. This effort included defaming Kuwait's ruling family and portraying Iraq as the champion of anti-colonialism, social justice, Arab unity, the Palestinian cause, and Islam. In an apparent move to defuse initial international condemnation of its invasion of Kuwait, Saddam falsely announced Iraqi troops would begin pulling out of Kuwait on 6 August 1990. In spite of Hussein's efforts to influence Coalition actions, the Coalition's information strategy ensured that the war was fought under favorable conditions that took full advantage of Coalition strengths and Iraqi weaknesses, ensuring Saddam's political and military strategy was soundly defeated. Despite Hussein's attempts to intimidate his neighbors, the Gulf States requested outside help and a Coalition formed. The Arab "street" did not rise up on his behalf, and Israeli restraint in the face of Scud attacks undermined his plan to turn the war into an Arab-Israeli conflict. Coalition leadership aggressively countered Saddam's widely publicized threats of massive casualties and his taking of hostages, neither of which deterred Coalition resolve. Saddam's attempts to take the offense by his use of Scuds and the attack on the Saudi town of Al-Khafji failed to achieve their strategic purpose of reducing the Coalition's will to fight. On all information fronts, the effective use of information operations by the Coalition to defend against Saddam's information strategy ensured that Iraq was not only beaten, but also failed to ever seize the initiative.

Source: Conduct of the Persian Gulf War
Final Report to Congress, April 1992

CHAPTER 2

OFFENSIVE INFORMATION OPERATIONS

> ***"Hit first! Hit hard! Keep on hitting!"***
>
> **Admiral Sir John Fisher, *Memories*, 1919**

201. PRINCIPLES AND CAPABILITIES

1. There are both offensive and defensive aspects of IO. A common link between the two aspects is the target sets involved in IO. Offensive IO capabilities are employed at every level of warfare, across the range of military operations, and will be employed to achieve mission objectives. The employment of an IO strategy to influence a decision-maker can yield a tremendous advantage to the Canadian Forces during times of crisis and conflict. As a result, Commanders must carefully consider the potential of IO for deterring and rolling back crises.

a. Principles. Offensive IO principles include the following:

(1) The decision-maker at all levels and associated decisionmaking processes are the ultimate target for offensive IO. Offensive IO are employed as an integrating strategy that orchestrates varied disciplines and capabilities into a coherent, seamless plan to achieve specific objectives.

(2) Offensive IO objectives must be clearly established, support overall national and military objectives, and include identifiable indicators of success.

(3) Selection and employment of specific offensive capabilities against an adversary should be appropriate to the situation and consistent with applicable international conventions and standing rules of engagement.

(4) Offensive IO may be the main or supporting element of a Commander's campaign or operation.

(5) Offensive IO in support of a Commander's campaign or operation may include planning and execution by non DND forces, agencies, or organizations and must be thoroughly synchronized and coordinated with all other aspects of the supported campaign or operation.

(6) In order to adequately attack information and information systems, it is necessary to be able to do the following:

(a) Determine the adversary's valuation, use, and flow of information.

(b) Identify and target discrete portions of an adversary's information or information systems.

(c) Predict the consequences of employing specific offensive capabilities with a predetermined level of confidence.

(d) Evaluate the outcome of specific IO attacks with confidence.

b. Capabilities. When viewed as an integrating strategy, IO weaves together related disciplines and capabilities toward satisfying a stated objective. Offensive IO applies traditional perception management disciplines such as PSYOP and information system attack to produce a synergistic effect against the remaining elements of an adversary's information systems. There are many capabilities and disciplines that require integration both defensively and offensively to conduct successful IO. Some of these

capabilities or disciplines appear more offensive or defensive in nature but it is their integration and potential synergy that ensures successful offensive and defensive IO. Capabilities and disciplines that can conduct offensive IO include the following:

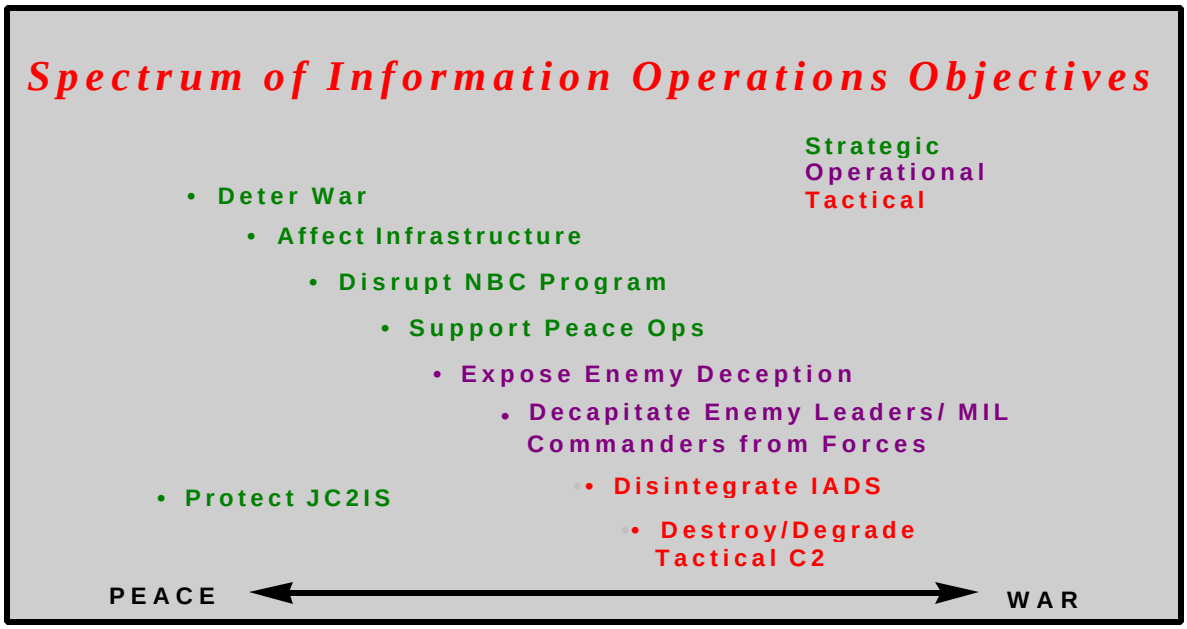

Figure 2-1. Spectrum of Information Operations Objectives

(1) C2W: The same elements that traditionally support C2W -- OPSEC, PSYOP, military deception, EW, and physical destruction - can be used to conduct offensive IO.

(a) OPSEC

1. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

2. History has shown the value and need for reliable, adequate, and timely intelligence, and the harm that results from its inaccuracies and absence. It is therefore vital and advantageous to deny the adversary commanders the critical information they need and cause them to derive inaccurate, timely appreciations that influence their actions.

3. OPSEC's most important characteristic is that it is a process. OPSEC is not a collection of specific rules and instructions that can be applied to every operation. It is a methodology that can be applied to any operation or activity for the purpose of denying critical information to the enemy. OPSEC is applied to all military activities at all levels of command. The TFC should provide OPSEC planning guidance to the staff at the time of the commander's intent and, subsequently, to supporting commanders in the chain of command. By maintaining liaison and coordinating the OPSEC planning guidance, the TFC will ensure

unity of effort in gaining and maintaining the essential secrecy considered necessary for success.

"No enterprise is more likely to succeed than one concealed from the enemy until it is ripe for execution."

Niccolo Machievelli, *The Art of War*, 1521

(b) PSYOP. While it is realized the CF currently does not possess a formal PSYOP capability, many potential allied partners do possess this capability, therefore, PSYOP must be considered for the effective integration of all IO capabilities.

1. PSYOP are actions to convey selected information and indicators to foreign audiences. They are designed to influence emotions, motives, reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals. PSYOP have strategic, operational, and tactical applications, including support to deception operations.

2. At the strategic level, PSYOP may take the form of political or diplomatic positions, announcements, or communiqués. At the operational level, PSYOP can include the distribution of leaflets, radio or television broadcasts, and other means of transmitting information that encourage enemy forces to defect, desert, flee, or surrender. Persistent attacks can have a synergistic effect with PSYOP, accelerating the degradation of morale and further encouraging desertion. At the tactical level, PSYOP includes measures to promote fear or dissension in enemy ranks.

3. PSYOP can contribute significantly to all aspects of joint operations. *Canadian Forces Operations Manual, B-GG-005-004/AF-000*, Chap 34, "Psychological Operations" provides additional information.

"The real target in war is the mind of the enemy commander, not the bodies of his troops."

Captain Sir Basil Liddell Hart, T*houghts on War*, 1944

(c) Deception

1. Deception is those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.

2. Military deception, as executed by TFCs, targets enemy decisionmakers through their intelligence collection, analysis, and dissemination systems. This deception requires a thorough knowledge of opponents and their decisionmaking processes. Anticipation is key. During the formulation of the commander's concept, particular attention is placed on defining how the TFC would like the enemy to act at critical points in the battle. Those desired enemy actions then become the goal of deception operations. Deception is focused on desired behaviour, not simply to mislead thinking. The purpose is to cause adversary commanders to form inaccurate impressions about friendly force capabilities or intentions, misappropriate their intelligence collection assets, or fail to employ combat or support units to their best advantage.

3. Deception operations are an integral element of joint operations. Planning for deception operations is top-down, in the sense that subordinate deception plans support the higher level plan.

4. Commanders at all levels can plan deception operations. Plans may include the employment of lower-level units, although subordinate commanders may not know of the overall deception effort. It is therefore essential for commanders to coordinate their deception plans with their senior commander to ensure overall unity of effort.

5. Deception operations depend on intelligence operations to identify appropriate deception targets, to assist in developing a credible story, to identify the recipient of the deception effort, and to assess the effectiveness of the deception plan.

6. Deception operations are not without cost, but are a powerful tool in full-dimensional operations. Forces and resources must be committed to the deception effort to make it believable, possibly to the short-term detriment of some aspects of the campaign. OPSEC for deception operations may dictate that only a select group of senior commanders and staff officers in the joint force know which actions are purely deceptive in nature. This situation can cause confusion within the force and must be closely monitored by TFCs and their staffs.

> ***"All warfare is based on deception."***
>
> **Sun Tzu, *The Art of War*, c. 500 BC, tr. Griffith**

(d) EW

1. EW is military action exploiting the electromagnetic spectrum which encompasses the interception and identification of electromagnetic emissions, the employment of electromagnetic energy, including directed energy, to reduce or prevent hostile use of the electromagnetic spectrum and actions to ensure its effective use by friendly forces. The three major subdivisions of EW are electronic warfare support measures (ESM), electronic countermeasures (ECM) and electronic protect measures (EPM). EW is an IO capability that can support offensive and defensive IO. All three subdivisions of EW contribute to the IO effort.

2. ESM provides a source of information required for immediate decisions involving ECM, EPM and other tactical actions. ECM prevents or reduces an adversary's effective use of the electromagnetic spectrum through the use of electromagnetic energy. EPM ensures the effective use of the electromagnetic spectrum despite an adversary's use of electromagnetic energy.

3. All subdivisions of EW should be employed to affect the target set as appropriate and according to established principles of warfare. The decision to employ EW should be based not only on overall joint mission objectives, but also on the risks of possible adversary responses and other effects on the mission.

4. The TFC should ensure maximum coordination among EW and other IO intelligence and communications support activities for maximum effect. This coordination is necessary to ensure effective exchange of information, eliminate undesirable duplication of effort, and provide mutual support as well as reduce the likelihood of electronic fratricide. See *Canadian Forces Operations Manual, B-GG-005-004/AF-000,* Chap 33, "Electronic Warfare" for additional information.

(e) Physical destruction refers to the use of "hard kill" weapons against designated targets as an element of an integrated IO effort. Although an adversary's C2 nodes will be high value targets, long term advantage from their destruction cannot be assumed, since the opposition can be expected to apply equally high priority to their reconstitution. The timing for the application of physical destruction is vital to ensure that subsequent operations exploit any short-term effects.

Physical destruction may be the only choice available to attack an adversary's C2, which includes headquarters and associated CIS that may be located within hardened facilities.

(2) PA: PA is a critical element of IO that can support offensive IO through the creation of an awareness of the military goals during an operation or mission.

(a) PA activities expedite the flow of accurate and timely information to internal (own organization) and external (the public) audiences.

(b) PA activities satisfy the desires of the internal and external audiences to be kept informed about the operation or mission.

(c) PA activities encourage a favorable attitude about the operation or mission.

(d) PA activities inform internal and external audiences of significant developments affecting them.

(e) PA activities allow a TFC to influence an adversary's (or a potential adversary's) perception about the friendly force's intent, capability, and vulnerability. At the same time, PA activities will not be used as a military deception capability or to provide disinformation to either internal or external audiences. PA activities will be consistent with ongoing OPSEC efforts. See *Canadian Forces Operations Manual, B-GG-005-004/AF-000,* Chap 29, "Public Affairs" for further information.

> ***"When regard for truth has been broken down or even slightly weakened, all things remain doubtful."***
>
> **Saint Augustine, *"On Lying"***

(3) CA: CA is a critical element of IO which can support IO through the creation of a positive attitude among former warring factions, non-belligerents, and/or the general populace in an area of tension or conflict.

(a) CA activities are those interrelated military activities that embrace the relationship between military forces and civil authorities and populations.

(b) CA activities are characterized by application of functional specialties, two of which are public communications and civil information.

(c) CA activities are conducted by forces (units and personnel) possessing an in-depth understanding of politico-military, economic, and social aspects of countries or regional areas where military forces are employed.

(d) CA activities enhance and influence the civil-military operational planning and execution by DND, non-DND, multinational, and nongovernmental or private voluntary organizations and other agencies through estimates of operational impacts on civilian populace, resources, and institutions in areas where military forces are employed.

(e) CA activities encompass the fundamental concept of control of policy at the highest practical level, coupled with the integration of military and civilian efforts at the lowest echelon feasible.

(f) CA activities include the requirement to negotiate and mediate with belligerents during peace enforcement operations. See *Canadian Forces Operations Manual, B-GG-005-004/AF-000*, Chap 30, "Civil Military Cooperation" (CIMIC) for further information.

202. RANGE OF MILITARY OPERATIONS

1. Offensive IO may be conducted in a variety of situations and circumstances across the range of military operations. Offensive IO may have its greatest impact in peace and the initial stages of a crisis. The IO impact in perception management or influencing an adversary's decisionmaking is highest in peace and operations other than war (OOTW). The initial IO goal is maintaining peace, defusing crisis, and deterring conflict. As a situation or circumstance moves towards conflict, the ability to target and engage critical adversary information and information systems decrease. As an adversary prepares for conflict, information systems become crucial to adversary operations. See Figure 2-2.

a. OOTW

(1) Some elements of offensive IO related plans and their associated capabilities may be employed in peacetime to deter crisis, control crisis escalation, project power, or promote peace. The employment of offensive IO capabilities in these circumstances may require Cabinet approval with support, coordination, deconfliction, cooperation, and/or participation by OGDs and agencies. Military offensive IO efforts must be synchronized with other Canadian government IO efforts to avoid wasted opportunities and to enable IO capability when needed and to prevent confusion. To synchronize offensive efforts, a lead agent should be identified, desired objectives should be determined, and measures of IO success should be established.

(2) The IO lead agent, objectives, and measures of effectiveness will change based on the situation or circumstances--influencing a potential adversary during peace or conducting various OOTW. Depending on the military objective and increased ability to accurately target and engage adversary information systems, offensive IO can be used to deter the adversary course of action or degrade the adversary's ability to respond, thereby influencing the overall goal of returning to peace.

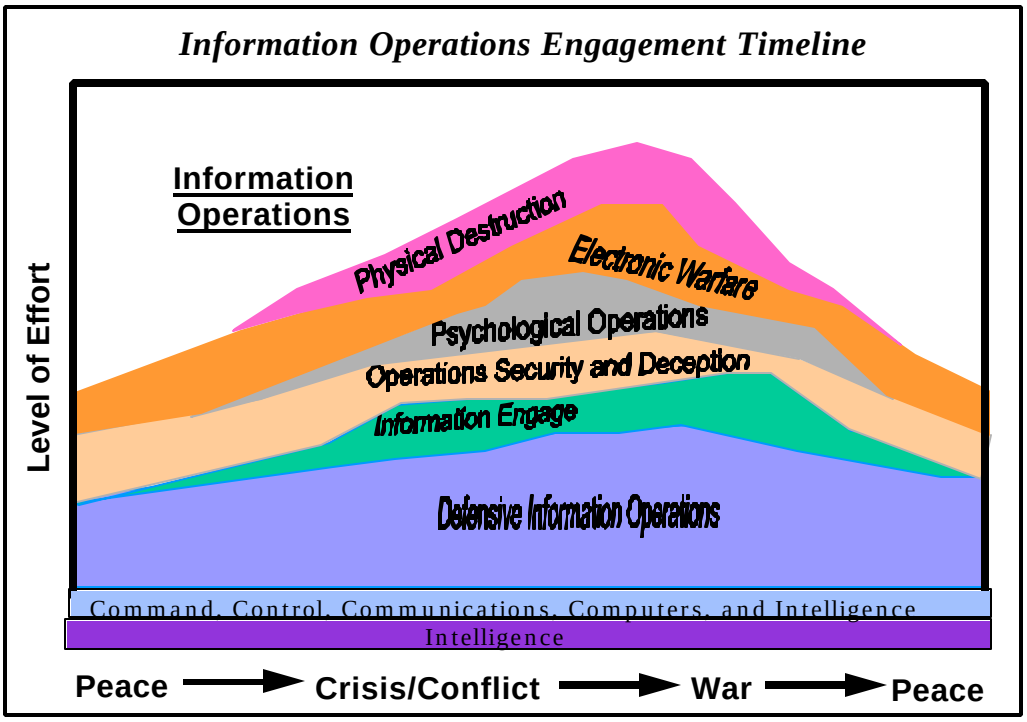

Figure 2-2. Information Operations Engagement Timeline

(3) Offensive IO may be conducted in all types of OOTW operations. For example, conducting PSYOP against a belligerent's potential allies with the goal of severing external sources of military, economic, and political support. In some cases, such as humanitarian assistance or military support to civil authorities, IO may be totally non-belligerent and focus on PSYOP and related CA or PA activities.

(4) IO planning in support of peacetime objectives and OOTW must also consider and prepare the battlespace and set the conditions for the successful execution of operations against an adversary in conflict.

b. Conflict and War

(1) Beyond the threshold of crisis, IO can be a critical force enabler for the joint warfighter. In addition to protecting information vital to the Canadian military, employment of offensive IO capabilities can affect every aspect of an adversary's decision cycle by impacting its key decision-makers, links, nodes and information. Offensive IO becomes a force multiplier to support combat operations. Degradation or destruction of adversary information systems and their (human element) will to fight are the primary goal of offensive IO in war.

(2) Offensive IO against adversary information systems and their (human element) will to fight may not take place in the same physical battlespace or be conducted in the same time frame as the combat operations they support, but must be synchronized thoroughly with the supported combat operations.

(3) Although probably not the main effort in war, offensive IO should help dominate combat operations and influence the adversary to terminate hostilities on terms favorable to Canada.

203. OFFENSIVE IO IN WAR

1. Offensive IO may be conducted at all levels of warfare inside and outside the traditional military battlespace. The level of warfare**,** strategic, operational, and/or tactical, at which IO are conducted normally will vary with the range of military operations and objectives. IO occurs throughout the spectrum of operations; warfare is but one part of this spectrum. The key concept for determining the level of IO to be employed is the endstate that is to be achieved. Any level of IO may include offensive IO or SIO and may necessitate higher level approval. All IO, especially strategic IO, must be planned and conducted in coordination with OGDs and other organizations and agencies outside DND, as appropriate. Strategic IO may also require coordination with allies or other non-governmental organizations. Strategic IO often seeks to engage adversary or potential adversary leadership to deter crisis or end hostilities once they occur. These operations may be conducted to influence or affect all elements (political, military, economic, informational) of adversary national power. See Chap 5, Information Operations Planning for further details.

204. INTELLIGENCE AND INFORMATION SYSTEMS SUPPORT

1. Intelligence Support to Offensive IO

a. General. Offensive IO requires broad-based, dedicated intelligence support. Because the effectiveness of many offensive IO capabilities is significantly improved by early employment, potential intelligence collection sources and access should be developed as early as possible. Significant lead time will usually be required to adequately fulfill IO requirements. Appropriate battle damage assessment (BDA) procedures to support IO must be established and implemented. Figure 2-3 provides a sequential overview of the relationship between offensive IO and required intelligence support.

b. Sources. To plan and execute offensive IO, intelligence must be collected, stored, and easily retrieved, especially for IO supporting short-notice contingencies. Intelligence collection for offensive IO includes all possible sources, from national-level covert operations through local open sources such as news

media, commercial world contacts, academia, and local nationals. A broad span of intelligence sources, including HUMINT, as well as those of a less traditional nature, should be developed and employed to support IO intelligence requirements.

c. Intelligence Preparation of the Battlefield (IPB). For offensive IO, IPB is the continuous process used to develop and maintain a detailed knowledge of the adversary's use of information and information systems. IPB for offensive IO uses a process of overlapping and simultaneous actions that produces situation updates, thereby providing TFCs and their subordinate commanders with flexible offensive IO options. IPB in support of offensive IO builds upon traditional combat IPB, but it also requires the following:

(1) Knowledge of the technical requirements of a wide array of information systems.

(2) Knowledge of the political, social, and cultural influences.

(3) The ability to conduct highly technical processing to produce offensive IO course of action (COA) templates.

(4) An understanding of the adversary's or potential adversary's decisionmaking process.

(5) An in-depth understanding of the biographical background of key adversary leaders, decision makers, communicators, and their advisors, to include motivating factors and leadership style.

d. Also see IPB in Chap 5, IO Planning.

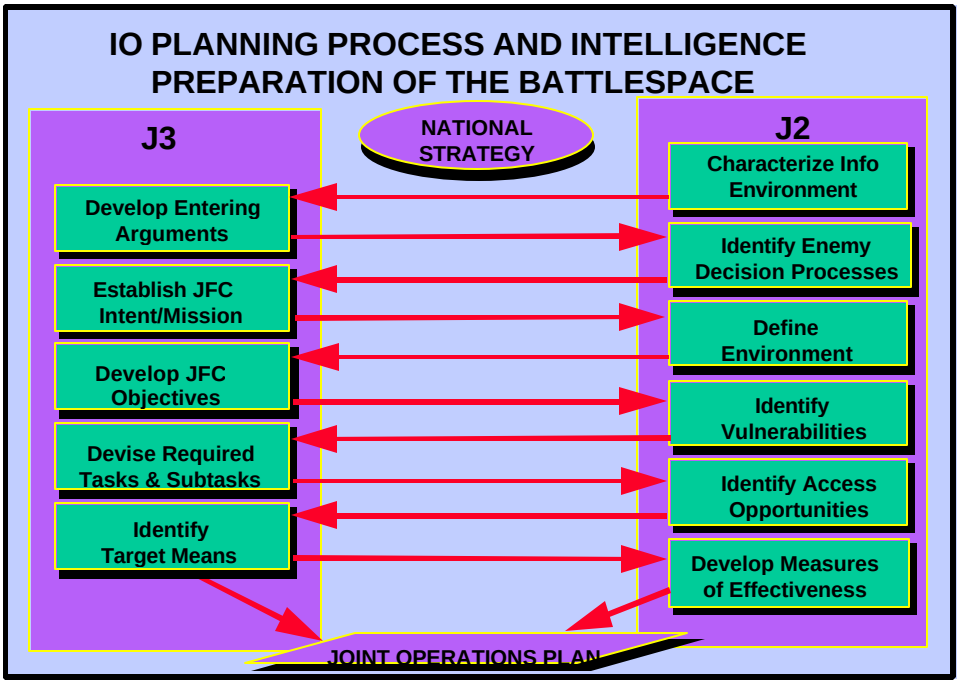

Figure 2-3. IO Planning Process and Intelligence Preparation of the Battlespace

2. Information Systems Support to Offensive IO

a. Information systems collect, transport, process, disseminate, and display information used to support offensive IO. These systems enable TFCs and their subordinates to use information effectively to maintain an accurate view of the battlespace and to plan and execute IO.

b. Information systems also provide TFCs and their subordinates with a means to interface with the GII in a manner that maximizes the scope and focuses the effectiveness of offensive IO.

c. Finally, information systems support offensive IO by providing the global reach capability that allows friendly decisionmakers and Commanders synchronization, coordination, and deconfliction of IO at all levels of war across the range of military operations.

205. OFFENSIVE IO TARGETING

1. General

a. Offensive IO targeting must maintain its focus on influencing decision-makers and can be effective against all elements of national power. Offensive IO targeting should consider all those elements to determine how best to achieve desired objectives.

b. Offensive IO can act on human decision processes (human factors), the information and information systems used to support decisionmaking (links), and the information and information systems used to implement decisions (nodes). IO efforts should examine all three target areas to maximize opportunity for success. The selection of IO targets must be consistent with Canadian objectives and applicable international conventions and rules of engagement. See Figure 2-4.

c. IO target selection will be conducted by the IOCC in accordance with the commander's guidance utilizing all available information and intelligence. Proposed targets will be prioritized by the IOCC and recommended to the commander or the targeting coordination cell (TCC) with recommended engagement strategy.

d. The IOCC will be a major source of information for the TFC during the targeting process that culminates with input to the TCC. IOCC representation on the TCC should provide an effective means by which to ensure coordination of IO information and target requirements with targeters.

e. Gain / loss considerations produced by the intelligence staff should be included in the IO targeting process.

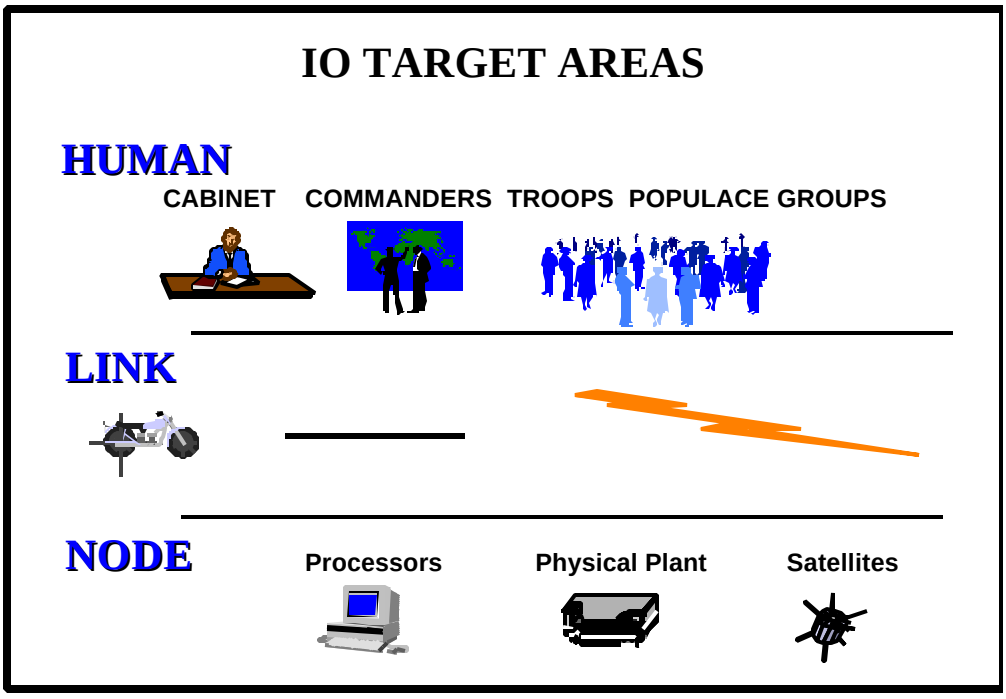

Figure 2-4. IO Target Areas

2. Strategic Targeting

a. The initial focus of offensive IO targeting at the strategic level is to act on an adversary's centre(s) of gravity within the elements of national power. Strategic offensive IO targeting may involve direct, indirect, and supporting attacks. The purpose of this targeting is to deter an adversary or potential adversary from actions leading to the outbreak of hostilities or other military or non-military activities not in the best interests Canada.

b. A direct attack is conducted on an adversary's "centre of gravity" target set. An indirect attack is conducted to impact on the adversary's "centre of gravity," but is directed against an associated target set. A supporting attack is conducted against target sets that do not directly influence the adversary's "centre of gravity," but provide pressure consistent with the main effort and in support of objective achievement.

c. Most strategic offensive IO targeting is the logical extension of the peacetime IO planning conducted on a routine basis against known adversaries and potential adversaries.

3. Response Targeting

a. Response targeting involves timely execution of offensive IO targeting for both initial IO objectives and follow-on attacks of IO targets based on BDA, or to support the response process in the defensive IO system described in Chapter 3, "Defensive Information Operations."

b. Surprise and security are critical to successful initial offensive IO targeting since adversary foreknowledge or source compromise may negate the initial offensive IO targeting effort. Offensive IO capabilities must be prepared to coordinate, synchronize, and execute initial offensive IO targeting in a highly responsive manner.

c. High-tempo operations may require rapid response to requests for follow-on attack of offensive IO targets based on BDA conducted by national, theatre, or subordinate joint force assets. Offensive IO capabilities must be prepared to quickly respond to requests for such follow-on attacks.

d. Offensive IO capabilities also may need to rapidly respond to requests for IO attacks against adversary capabilities targeting friendly information and information systems, thereby completing a vital link between offensive and defensive IO.

"Iraq lost the war before it even began. This was a war of intelligence, EW, command and control, and counterintelligence. Iraqi troops were blinded and deafened . . . Modern war can be won by informatika and that is now vital for both the U.S. and U.S.S.R."

Lieutenant General S. Bogdanov, Chief of the General Staff
Center for Operational and Strategic Studies, October 1991

CHAPTER 3

DEFENSIVE INFORMATION OPERATIONS

> ***"We have evidence that a large number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks on military-related computers."***
>
> **John M. Deutch, Director, CIA**
> ***Washington Post*, 26 June 1996**

301. GENERAL

1. The Canadian military depends upon information to plan operations, deploy forces, and execute missions. Advances in information technologies have significantly improved the potential efficiency and volume of information flow. Complex information systems support powerful infrastructures that dramatically enhance military capabilities; however, increasing dependence upon these rapidly evolving technologies makes joint forces more vulnerable. Defensive IO ensures the necessary protection and defence of information and information systems within joint forces upon which decision-makers depend to achieve their objectives. When combined with offensive IO, the net result will be enhanced opportunity to use IO to successfully exploit the full range of conflict.

a. Defensive IO integrates and coordinates protection and defence of information, information-based processes and information systems that are critical to the achievement of objectives. The defensive IO process is an inherent part of force protection.

b. Defensive IO consists of three elements:

(1) O - Protect: the control of adversary access to those friendly elements of the information environment that are critical to the accomplishment of friendly objectives,

(2) Defensive Counter-IO: the counteraction of adversary IO attacks and the restoration of the performance and functionality of critical friendly elements, and

(3) Offensive Counter -IO: the deterrence or neutralization of adversary IO capability.

c. Information Protection (IP) is a combination of the first two elements. The last element is necessary to deter adversary intent to employ IO and exploit and/or neutralize adversary IO capability and opportunity, either preemptively or as a response.

d. The defensive IO process integrates and coordinates policies and procedures, operations, personnel, and IP technology to protect information and information-based processes, and to defend information systems.

e. Defensive IO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems for their own purposes. Defensive IO includes the technical capabilities of IP as well as universal protection capabilities such as education and training, operations security, and counter-intelligence.

f. IP protects and defends information and information systems by ensuring their availability, integrity, and confidentiality. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IP focuses on the technical capabilities and processes such as multilevel security, firewalls, secure network servers and intrusion detection software, as well

as related physical, personnel and procedural security measures (e.g. the measures taken to safeguard cryptographic equipment and material from unauthorized access). See Figure 3-1.

g. Defensive IO Integration. Defensive IO efforts should be integrated in all military operations, to include activities by other government and non-government agencies or organizations operating in the TFC's area of operations (AO).

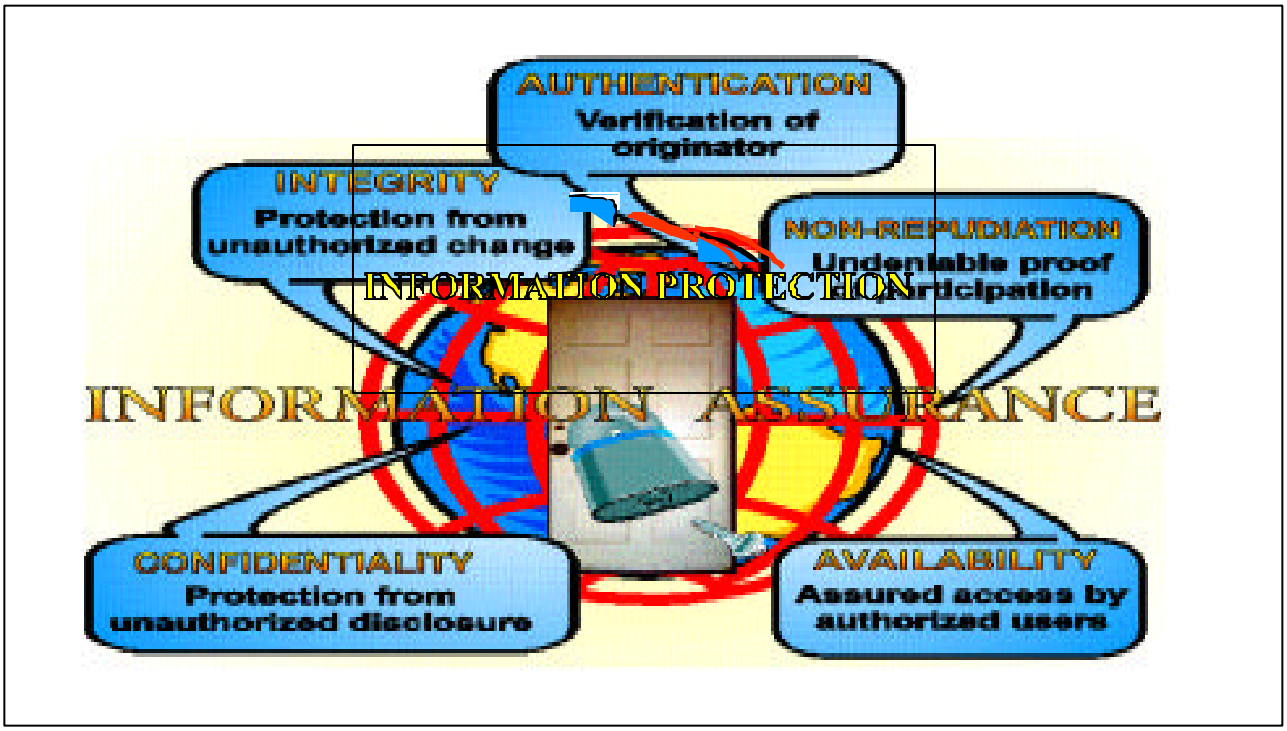

Figure 3-1 Information Protection

(1) Defensive IO Integration with Offensive IO. Defensive IO must be integrated with offensive IO to provide a timely response against identified and potential threats to friendly information and information systems. The IOCC integrates defensive IO and offensive IO for TFCs. Subordinate commanders should ensure supporting operation plans (OPLANs) and operation orders (OPORDs) make provisions for this integration.

(2) Defensive IO Integration within a Joint Force. Defensive IO integration within a joint force is necessary to ensure the three interrelated processes (protect, detect, and react (or respond)) are uniformly understood and practiced. In addition, defensive IO integration ensures employment of the most appropriate joint force IO response capabilities. The TFC's IOCC is responsible for integrating defensive IO.

(3) Defensive IO Integration within a Multinational Force. Information-based technology, weapons systems, intelligence, and other capabilities are often shared, integrated, and synchronized into multinational operations to enhance operations. While providing benefits to multinational operations, the integration of Canadian and allied or coalition information, information-based processes, and information systems creates vulnerabilities which an adversary can exploit using IO.

(a) The Combined Force Commander's IOCC is the focal point for integrating IO in multinational operations.

(b) Within the context of promulgated releaseability guidelines, and as advised by the J3 and J2, the IOCC may be delegated the responsibility to share IO-essential information with

multinational forces. This notwithstanding, in all cases Canadian national operations and intelligence authorities (i.e. NDHQ J3 and J2) shall remain the final authority for the release of operations and intelligence information which might expose Canadian operations, intelligence sources or methods, or place at risk information or information systems vital to Canadian national security.

(c) Subject to the above conditions, the IOCC may consider sharing threat data, vulnerabilities, targeting and battle damage assessment, and IO capabilities that could help mitigate vulnerabilities. See *Joint Doctrine for Canadian Forces Joint and Combined Operations, B-GG-005-004/AG-000* for additional guidance.

(4) Levels of War. Defensive IO requires close cooperation between military and non-military organizations internal and external to the supported TFC at all levels.

(a) Peacetime defensive IO efforts at all levels of war should be synchronized to support all phases of a military operation.

(b) To ensure unity of effort, defensive IO at all levels of war should be synchronized with planned or ongoing offensive IO.

"In war, the defensive exists mainly that the offensive may act more freely."
Rear Admiral Alfred Thayer Mahan, *Naval Strategy*, 1911

g. The Defensive IO Process. Three interrelated processes comprise defensive IO: IO-Protect, defensive counter-IO and offensive counter-IO. Figure 3-3 provides an overview of the defensive IO implementation process and is a model scaleable to all levels of war. The defensive IO implementation process integrates all available defensive capabilities to ensure an in-depth defense. TFCs and their subordinate commanders should plan, exercise, and employ available defensive capabilities to support the three defensive IO processes. Defensive IO capabilities which contribute to an in-depth defense range from basic awareness training to technical IP solutions such as INFOSEC devices and automated intrusion detection software.

302. INFORMATION OPERATIONS PROTECT (IO-PROTECT) PROCESS

1. Defining joint force information needs and dependencies is the focus of the IO-Protect process. The joint force information environment is bounded by what is critical to joint force operations.

a. The information environment is a combination of physical systems and facilities, as well as abstract processes such as intelligence and decision making.

b. Protection of the information environment is rooted in a sound approach to managing risk. Risk management processes include consideration of information needs, the value or sensitivity of information that may be compromised or lost if the protected information environment is breached (loss of access control), system vulnerabilities, threats posed by potential adversaries and natural phenomena, resources available for protection and defence, and the residual risk (R_R) to the information environment once protective measures have been put in place. In addition, the value or sensitivity of information can change from one phase of a military operation to the next and this must be considered in the risk management process.

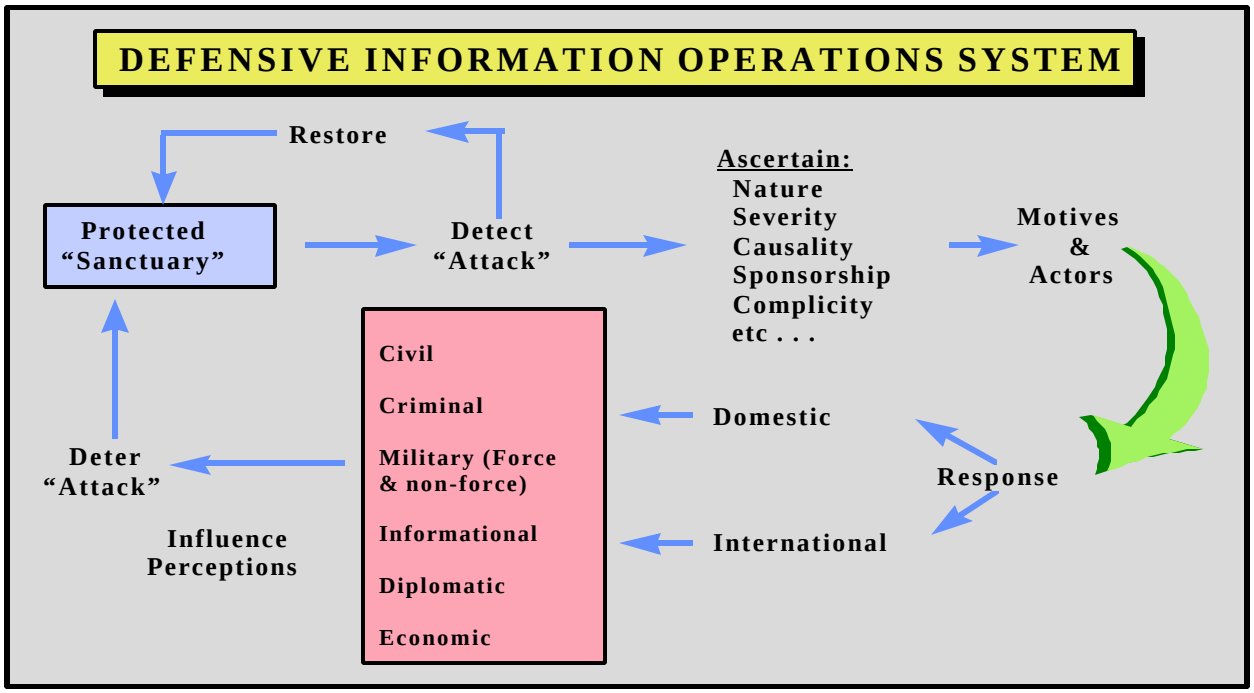

Figure 3-2. Defensive Information Operations System

c. The protected information environment not only provides the degree of protection commensurate with the value or sensitivity of its contents, but also ensures capabilities are in place to respond to a broad range of attacks.

d. Information protection applies to any information medium or form, including hard copy (message, letter, FAX), electronic, magnetic, video, imagery, voice, telegraph, computer, and human. The information protection process involves determining the scope (what to protect based on the value or sensitivity of the information) and the standards for protection (to what extent through operations and the application of protective measures and technologies). See Figure 3-3. The protection process should reflect the changing value or sensitivity of information during each operational phase.

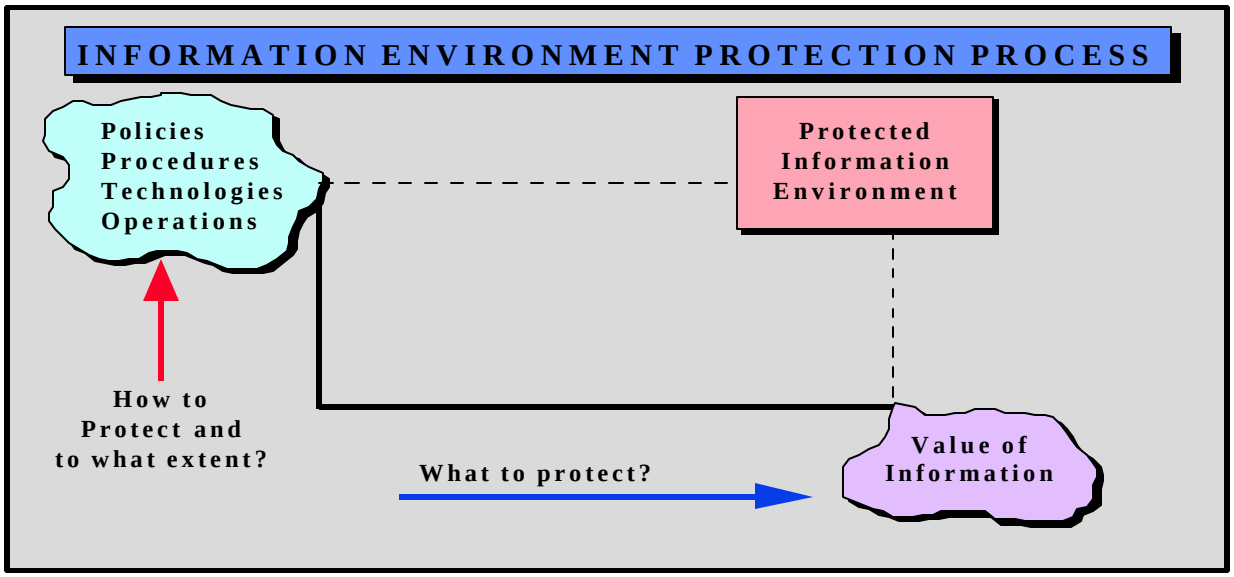

Figure 3-3. Information Operations Protect Process

e. TFCs should implement an IO-Protect process through adoption of common policies and procedures, employment of technological capabilities, and planning operations to include defensive IO objectives.

(1) Policies. TFCs need to augment standing defensive IO policies with joint force-specific policies to provide integrated and focused information environment protection tailored to their specific AOs. These policies should address vulnerabilities and threats, friendly force capabilities, and commercial infrastructure dependencies and vulnerabilities that impact the various phases of an operation.

(2) Defensive IO Procedures. Joint force procedures to implement IO-Protect policies should employ commonality to the greatest extent possible. Use of common procedures will help achieve secure interoperability between joint force components. These procedures include but are not limited to the following:

(a) Education, Training, and Awareness. A key element of information environment protection is education and training of system users, administrators, managers, engineers, designers, and requirements developers. Awareness heightens threat appreciation and the importance of adhering to protective measures. Education provides the concepts and knowledge to develop appropriate technologies, policies, procedures, and operations to protect systems. Training develops the skills and abilities required to operate while mitigating vulnerabilities.

(b) Risk Management. Risk management decisions determine limits for applying countermeasures. The risk management process includes consideration of information needs, the value or sensitivity of information at risk, system vulnerabilities, threats posed by potential adversaries and natural phenomena, resources available for protection and defence, and the residual risk (R_R) to the information environment once protective measures have been put in place. TFCs should also establish a routine for periodic risk assessment.

(c) Intelligence Support. A critical component in the intelligence process is identifying the threat. Threat information is a primary input to the risk management process and directly contributes to information environment protection.

1. Threat. Intelligence provides an understanding of the threat to information and information systems by identifying potential information adversaries, their intent, and their known and assessed capabilities. Threat information is a key consideration in the risk management process.

2. IO threats should be defined in terms of a specific adversary intent, capability and opportunity to adversely influence those elements of the friendly information environment critical to achieving friendly force objectives. See Figure 3-4.

3. Intelligence can provide TFCs with the necessary information to conduct risk assessments and develop risk management options to mitigate their vulnerabilities.

4. Threat assessment is a continuous process that reflects changes in the operating environment, technology, and threats.

Figure 3-4. Growing Threat

(d) Counter-deception. Intelligence activities contributing to awareness of adversary posture and intent also serve to identify adversary attempts to deceive friendly forces.

(e) Counter-psychological. Intelligence activities identifying adversary psychological warfare operations contribute to situational awareness and serve to expose adversary attempts to influence friendly populations and military forces.

(f) Public Affairs (PA). PA programs contribute to information protection by disseminating factual information. Factual information dissemination counters adversary deception and PSYOP. Command information programs serve the same purpose as PA with respect to defensive IO. Command information programs normally are found within joint force components and at lower level units where there is no designated PA program.

(g) Security. CI, personnel security, procedural security and physical security measures are examples of measures that contribute indirectly to information protection. Coordinated application of all these activities provides the organization a more complete vulnerability assessment and assists in risk management.

(h) Vulnerability Analysis and Assessments. Joint forces should conduct vulnerability analyses and assessments to identify potential vulnerabilities in information systems and to provide an overall assessment of system security posture. Based on an evaluation of the risk posed to the information system (IS) should such vulnerabilities be exploited, and where it does not significantly impact upon operational capabilities, identified vulnerabilities should be eliminated. Integrating vulnerability analysis capabilities into joint training and exercises helps identify and mitigate vulnerabilities and directly contributes to information protection.

1. Foreign threats are only a part of the overall threat to information systems. Internal threats from malicious (disgruntled workers) and accidental (magnetic emanations or electrical impulses) sources are significant threats. Natural phenomena such as sunspots, hurricanes, tornadoes, earthquakes, and floods also pose threats to systems. Vulnerability analysis of systems must include consideration of these factors.

2. Vulnerability analysis and assessment efforts focus on specific types of information systems. A Network Vulnerability Analysis Program has been established within DND specifically focusing on IS vulnerabilities.

(3) IP Capabilities. TFCs should ensure IP capabilities that protect information and defend information systems are integrated into their C4 systems and thoroughly tested in realistic exercises and training events. Technological capabilities include security measures such as INFOSEC devices.

(a) INFOSEC. INFOSEC is the protection of information systems against unauthorized access or information corruption. INFOSEC includes those measures necessary to detect, document, and counter such threats.

(b) Computer Security (COMPUSEC). COMPUSEC is the protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system.

(c) COMSEC. COMSEC includes measures taken to prevent compromise of information stored, transmitted or processed on an information system. COMSEC also ensures telecommunications authenticity. COMSEC includes cryptosecurity, transmission security, emission security, network security, and physical security of COMSEC materials and information.

(d) EW. Defensive EW procedures (known as EPM), including COMSEC procedures and changing call signs or words and frequencies, are examples of procedures or disciplines directly contributing to information and information system protection. Others include COMPUSEC procedures, OPSEC, and personnel information access controls.

(4) Operations. TFCs need to consider and include defensive IO objectives when planning and executing operations. Operations conducted for purposes other than mitigating IO vulnerabilities may have collateral effects supporting defensive IO objectives.

303. DEFENSIVE COUNTER-IO PROCESS

1. Given the increasing vulnerability of IS, and the increasing importance of the information on those IS, there is a requirement for a detection, tracking, analysis and response capability as a defence against intrusion, degradation and loss through external and internal IO. The speeds at which information system incidents (deliberate or accidental) occur have outpaced the capability for manual detection and response. This mandates a need for automated detection and response capabilities. These capabilities should automatically detect system intrusions or aberrations and instantly generate alerts. Additionally, automatic threat mitigation that limits the extent of damage or spread of incidents should be self- initiating.

a. Hostile incidents can be directed against different layers of the IS, and will vary in the ease with which they can be detected. Responses must be tailored to the nature and extent of the incident.

(1) Attacks against the physical layer of an IS are easiest to identify and to defend against. They involve the traditional approach of using conventional weapons to physically destroy a component or components of an IS. Destruction of the critical components, identified through a links and nodes analysis, at a key point in an operation can cripple an adversary's ability to function.

(2) Attacks against the logical (or syntactic) layer of an IS, which generally consists of the software and operating systems of an IS as well as the system operating procedures, are more difficult to detect as they typically manifest themselves as system errors (e.g. slow execution of procedures, misdirection of information). The ability to distinguish between accidental and deliberate system errors is key to responding to this form of attack.

(3) Attacks against the semantic layer of the IS are no longer directed on the components or the operating systems but seek to affect and exploit the trust users have in the integrity and validity of the information in the IS (i.e. perception management). All personnel involved in information operations (across the full spectrum of conflict) will have access to open-source information, media and perhaps dis-information. These are the most difficult to detect and the TFC needs to be advised by appropriate agencies when this occurs and be prepared to react accordingly. Effective counter-deception and counter-PSYOP programs are essential.

b. Timely incident detection and reporting are the keys to initiating defensive counter-IO process. The defensive counter-IO process includes the following elements:

(1) Intelligence. Intelligence contributes to defensive counter-IO by providing warnings of potential adversary activity and cueing collection to specific activity indicators. Close coordination is required between intelligence, law enforcement, system developers, providers, administrators, and users to ensure timely sharing of relevant information. Intelligence and C3 processes form the foundation for indications and warnings (I&W). See Figure 3-5.

(a) I&W. I&W for defensive IO draw from current intelligence reports, organic joint force assets, component command I&W support, and correlation of force movements in the AO. In addition, national-level intelligence assets provide I&W of imminent adversary activity.

(b) Defending against an attack, whether against a TFC's intelligence database or against a component of the commercial national power grid, is predicated on how well the intelligence threat and associated I&W processes function and on the ability of systems providers, users, and administrators to implement protective countermeasures.

(c) In defensive IO, I&W fuses knowledge of adversary IO capabilities with intelligence to assess the probability of adversary IO actions, and provides sufficient warning to preempt, counter, or otherwise moderate their effect.

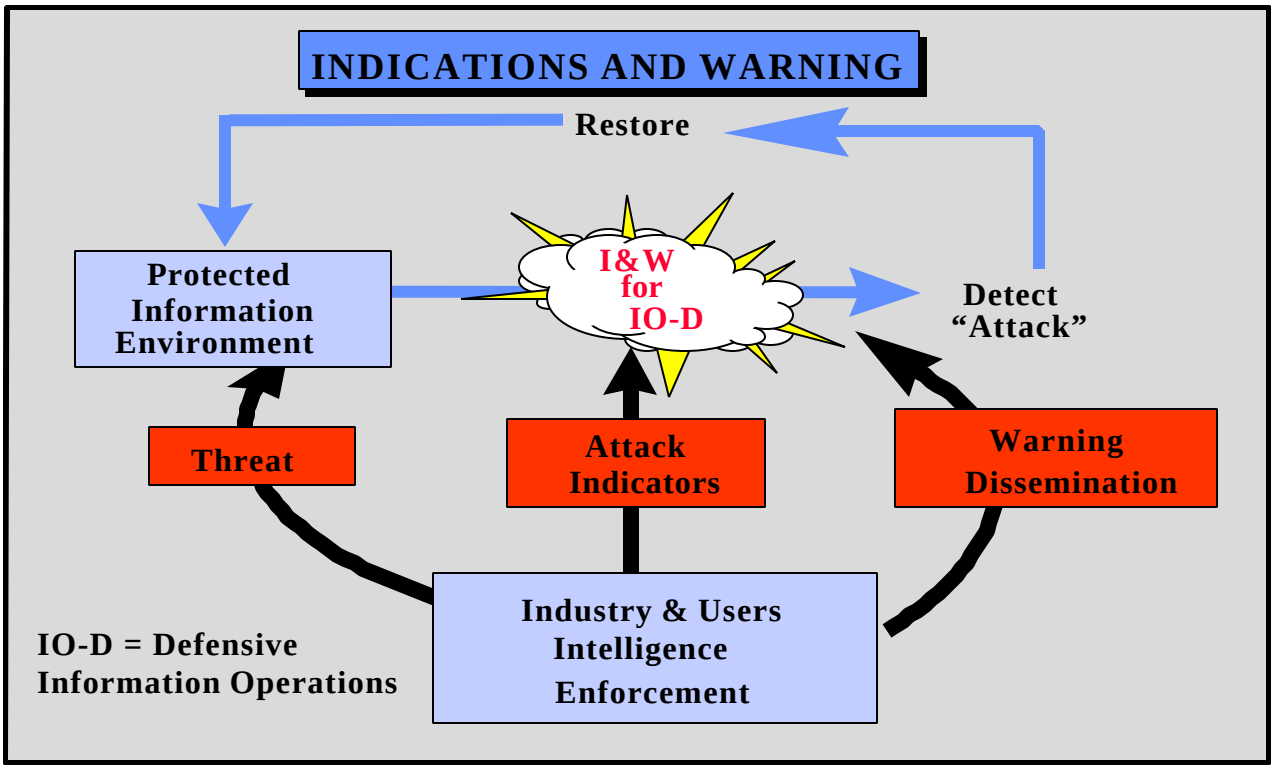

Figure 3-5. Indications and Warning

(d) Joint Force I&W support to defensive IO relies on indicators from sources both internal and external to DND. Joint forces should continue to analyze traditional attack indicators until a comprehensive national I&W process is established that reflects the unique characteristics of IO. For additional information regarding the national I&W process, refer to MC 166, MIP 260, and CONOPS - Intelligence Support to Deployed Forces.

(2) Incident Detection. Systems designed to detect incidents and alert managers and administrators at all levels to abnormalities help contribute to defensive counter-IO processes. Incident detection can be conducted on a real time or off-line basis, centralized or decentralized. Traditional detection techniques such as audit log review can be supplemented by automated tools and by effective counter-deception and counter PSYOP programs. Provision should be made for detection or mitigation system updates. The detection technique used will depend upon the operational threat, the criticality of the system being protected, the sensitivity of the information on that system and the consequences of any delays in responding to an incident.

(3) Incident Reporting. When an incident occurs, it is essential that specific details of the incident are recorded and reported for analysis purposes. The TFC's IOCC will establish standardized reporting procedures. Reporting shall consist of an immediate initial report to initiate the I&W process, with follow-up reporting as necessary. The nature and extent of the incident will dictate the extent of the reporting. Timely collation, correlation, information analysis, and warning dissemination requires a continuously functioning reporting structure. A reporting structure linked to intelligence, law enforcement, policy makers, and the information systems community, both government and commercial, is essential to defensive IO.

(4) Incident Tracking. Intrusions may occur over an extended period of time or series of user sessions, or may be initiated by multiple intruders working in concert. Depending on the sophistication of the intruder, hostile intent may only be determined when the sequence of the attack is assembled, as each individual action may have the appearance of legitimacy. It is therefore essential that once an incident has been detected, the activities of the intruder shall be tracked in order to gather evidence

for possible prosecution, and for purposes of I&W. Automated record keeping will assist in this regard. The TFC's IOCC shall be responsible for coordinating incident tracking across components of the force.

(5) Incident Analysis. The nature and extent of the incident shall be determined using either automated tools or more traditional techniques. A distinction needs to be made between deliberate attacks and accidental abnormalities in order to employ the most appropriate countermeasures to mitigate the effects of the incident. In addition to establishing intrusion signatures trends, identifying weaknesses in security mechanisms and aiding in the development of countermeasures, incident analysis will permit the conduct of Information Battle Damage Assessment (I-BDA).

(6) Once restorative actions are complete, there will be a requirement to conduct defensive information battle damage assessment. This will involve identification of the damage caused by the attack, any consequences arising from the restorative actions themselves (e.g. temporary degradation of service pending recovery from uninfected sources) as well as an assessment of the potential impact on operations.

b. Incident Response. Incident detection mechanisms serve to trigger the response process. Automated alerting mechanisms provide commanders with enhanced situational awareness. Timely identification of actors and their motives, establishing cause and complicity and restoring capability are the cornerstones of effective and properly focused response. The effectiveness of the response process is dependent upon efficient integration of intrusion detection and analysis capabilities, as well as having established and tested response procedures. The process contributes to defensive IO by countering threats and enhancing deterrence.

(1) Incident response may involve some form of action against the perpetrators. The range of actions that may be taken in response to adversary actions will be constrained by the rules of engagement established by the Government and the CDS, and by existing national and international law. Responses can range from terminating the specific connection with the illegal activity up to and including military force. The ROE should clearly define what constitutes self-defence and all responses should be based on the principle of proportionality.

(2) Immediate termination of adversary system access to protect against further actions and information exploitation is one possible response. Termination should be weighed against the needs of the legal and intelligence communities to collect against and exploit the adversary. The system owner, designated approving authority, or higher authority decides whether to allow an intruder to maintain access in order to gather information for the response process. The decision relies on a risk assessment of continued access, consideration of current and future operations, and intelligence impact.

(3) Capability restoration relies on pre-established and proven mechanisms for the prioritized restoration of minimum essential capabilities. The commander shall establish the restoration priorities in accordance with direction from appropriate higher authority.

(a) Capability restoration may rely on backup or redundant links or system components, backup databases, or even alternative means of information transfer. Information system design and modification should consider incorporating automated restoration capabilities and other redundancy options.

(b) In some cases, the required technical restoration capabilities are beyond the abilities of the affected sites. On-line or deployable restoration assistance capabilities can provide required additional expertise and tools to restore services. These capabilities may take the form of a help desk or an Information System Incident Response Team (ISIRT).

(c) ISIRTs may be formed for rapid response to deployed forces and by some component commanders for similar response to subordinate forces within the AO.

(d) A key step in the capability restoration process is to inventory system resources to identify surreptitious adversary implants.

(3) Information system security incidents frequently involve a breach of national or international laws. Monitoring organizations may encounter incidents requiring law enforcement attention. In such instances, military and civilian law enforcement agencies should be contacted to provide expert assistance.

(a) Law enforcement assistance can range from advice on how to preserve evidence to the provision of specialist investigative skills. The ability to investigate an incident for retaliatory purposes may deter other adversaries. Information system incidents or intrusions detected and reported to military and civilian law enforcement agents during criminal investigations help support systems administrators, the intelligence community, system developers, and, as necessary, the producers and users of affected information. Investigation procedures should protect law enforcement's ability to continue their operation while protecting individual privacy rights.

(b) Post-attack analysis provides information about vulnerabilities exploited and leads to security improvements. Audit trails such as automated recording of specific attack techniques and attack events during the incident can provide information required for analysis. These same capabilities can also provide the evidence necessary to pursue legal options.

(4) Military force is a response option that directly eliminates the threat, or interrupts the means or systems that an adversary uses to conduct an information attack. Military force may be applied in a pre-emptive manner (offensive counter-IO) or in a reactive manner (defensive counter-IO), and can include conventional or IO attacks. At the theater-strategic or tactical levels, possible response options will be defined in terms of rules of engagement provided to the commander.

304. OFFENSIVE COUNTER-IO

1. There may be occasions where it is necessary to deter adversary intent to conduct IO against friendly forces or to neutralize adversary IO capabilities in order to defend friendly information systems. A proactive and aggressive strategy to deny an adversary information, electronic capability, command and control and counter-intelligence can be very effective. Judicious application of IO activities prior to hostilities may cause the enemy to abort conflict prior to the commencement of conflict.

a. Offensive Counter-IO analysis identifies adversary IO systems of interest and determines the critical nodes, links and processes in those systems. Strategic and tactical intelligence plays a major role by providing information on adversary IO capabilities. The Offensive Counter-IO analysis has the purpose of increasing payoff by identifying key target vulnerabilities. The IOCC will coordinate the offensive counter-IO analysis on behalf of the TFC.

b. Analysis will consider physical destruction, EW, deception and PSYOPS means available to the TFC and how they might be applied to adversary IO systems. The product will be a prioritized list of critical nodes, links and processes that must be attacked in order to cripple the adversary system, as well as recommendations as to the best attack method and a concept for the conduct of offensive counter-IO.

(1) Offensive counter-IO plans shall be based on the TFC's mission, commander's intent and concept of operations.

(2) Offensive counter-IO will be synchronized with and support the commander's plan.

(3) Offensive counter-IO should aim to take and hold the initiative by degrading the adversary's IO capabilities.

(4) IO targets at the operational level must be evaluated carefully. Attacking IO targets only at the tactical level, without joint oversight, risks the loss of useful paths to valuable operational targets.

c. Once an offensive counter-IO has been conducted, there should be some means to determine if the attack has been successful. This will be similar to conventional battle damage assessment, but unless the attack was physical in nature, it will be more difficult to ascertain the effect of the attack on the adversary system. All-source intelligence will be critical to this analysis. The IOCC will coordinate the IO damage assessment.

"Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing."

Frederick the Great
quoted in Foertsch, *The Art of Modern War,* 26 June 1996

CHAPTER 4

INFORMATION OPERATIONS ORGANIZATION

> ***"Organization is the vehicle of force, and force is threefold in nature; it is mental, moral, and physical."***
>
> **Major General J.F.C. Fuller,**
> ***The Foundation of the Science of War,* 1926**

401. GENERAL

1. A fully functional IO Coordination Cell (IOCC) is paramount to successful IO at both the national and operational level. The IOCC integrates the broad range of potential IO actions and activities that help contribute to the commander's desired end state in an AO.

a. The organizational structure to plan and coordinate IO should be sufficiently flexible to accommodate a variety of planning and operational circumstances. This chapter focuses on how to organize to plan and execute IO.

b. IO should be an integral part of all military operations. This requires extensive planning and coordination among many elements of the joint headquarters, component staffs, OGDs and agencies to ensure IO is fully integrated with other portions of mission and operation plans.

c. It is the Commander's responsibility to create an IOCC which will be tasked with IO coordination within theatre supported by the National IOCC. Since staffs with diverse structure, scope of responsibilities, and supporting infrastructure support TFs, the commanders should tailor their organizations according to unique mission requirements.

d. The principal staffs that may be involved in IO planning are the Joint Staff, the TFC and subordinate components staffs. The circumstances in which these staffs conduct IO may affect the optimal organization to carry out their responsibilities.

(1) The TFC staff can call on the expertise of personnel assigned to their subordinate commands and the National IO staff to assist in the planning process as specified by the Operations Planning Process. During crisis or other short-notice operations, the TFC can call on the expertise and technical support of the National IO staff.

(2) A joint force (normally a TFC) staff may be designated to plan and/or execute IO at short notice. A TFC staff may be required to plan and/or execute IO immediately upon arrival in the operational area, while conducting forward presence operations, or after a short notice deployment while the infrastructure to support the staff is developed.

e. The IOCC is formed from representatives of each staff element, component, and supporting agencies responsible for integrating the capabilities and disciplines of IO into a synergistic plan. The cell coordinates staff elements and/or components represented in the IOCC to facilitate the detailed support necessary to plan and execute IO. Figure 4-1 provides an overview of a typical joint IO cell. The actual composition or members and their status--resident or nonresident--of the IOCC may vary based on the overall mission of the joint force, the role of IO in accomplishing the commander's objectives, and the adversary's or potential adversary's capability to conduct IO. Positions are described as either resident or nonresident. Resident implies the individual fulfilling the function should preferably be collocated with or in close proximity to the other IOCC members. Nonresident implies the individual performing the

function would not require frequent contact with other IOCC members, but still plays a critical role in IO planning and coordination.

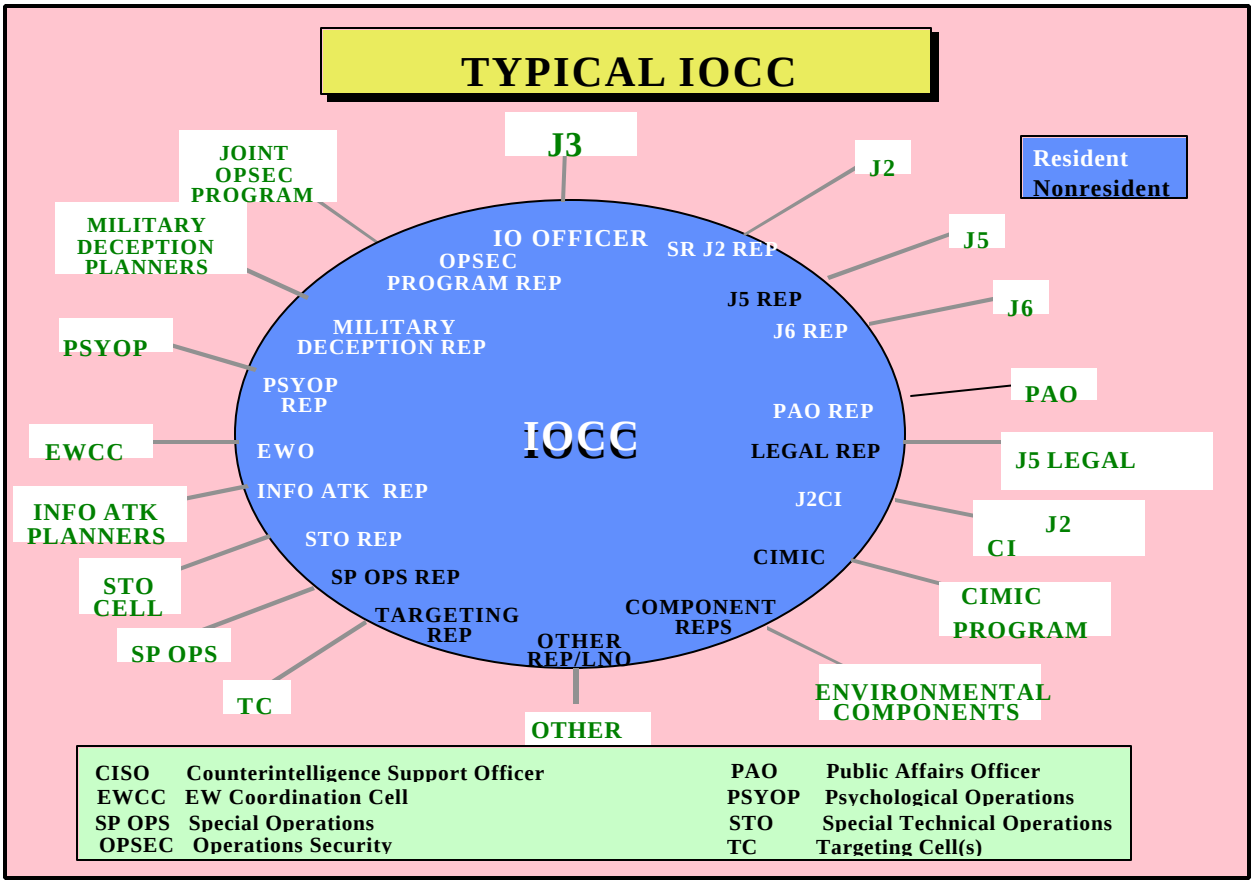

Figure 4-1. Typical IOCC

f. IOCC and EWCC Relationship. The EWCC will closely coordinate EW activities with the IOCC to ensure the synergistic effects of their respective activities. *Canadian Forces Operations Manual, B-GG-005-004/AF-000*, Chap 33, “Electronic Warfare.” provides additional information for the development and utilization of EW and an EWCC. This provides the TFC with the capability to integrate, coordinate, and deconflict the full spectrum of IO.

402. IO ORGANIZATION

1. The Commander should provide guidance for planning and conduct of IO and assign responsibility for the employment of IO resources in joint operations. In multinational operations, the TFC is responsible for coordinating the integration of joint IO with multinational IO assets, strategy, and planning. The TFC may delegate responsibility for IO to a member of the joint staff, normally the J-3. When authorized, the J-3 will have primary staff responsibility for planning, coordination, and integrating joint force IO.

2. IO Organization. To assist the J-3 in exercising joint IO responsibilities an IO officer will be designated. The primary function of an IO officer should be coordination of the IO strategy and the supporting capabilities and disciplines between the various TFC, higher echelon, component, and multinational staffs. The IO officer will ensure IO is implemented per the Commander’s guidance. This may entail representing IO concerns at critical planning meetings, leading the IOCC, and/or directly facilitating coordination between the staff organizations or components responsible for each element of IO.

a. J-3 Operations/Plans: **Resident.** Principal staff officer for IO, JTCB (or functional equivalent) representative and coordinator of all IO functional areas. J-3 Operations/Plans, or designated representative, will have access to and cognizance of the TFC's Information Coordinating Committee (ICC) (or functional equivalent) proceedings to ensure deconfliction and unity of effort for information activities within an AO. The TFC's PSYOP Officer participates as a member of the IOCC. Functioning as the IOCC Chief, J3 Ops/Plans or designated deputy normally ensures the functions shown in Figure 4-2 are performed.

IO OFFICER FUNCTIONS

- **Coordinating and directing the overall IO effort for the TFC**
- **Coordinating IO issues within the joint staff and counterpart IO planners on subordinate staffs**
- **Coordinating IO defensive and offensive concepts to support the TFC concept of operations**
- **Establishing IO priorities to accomplish planned objectives**
- **Determining the availability of IO resources to carry out IO plans.**
- **Recommending tasking to the J-3 for joint organizations, staff, and elements (i.e., EWCC, military deception planners, etc.) that plan and supervise the various capabilities to be utilized. Consolidated J-3 tasking ensure efficiency of effort in planning and executing integrated IO.**
- **Serving as the primary "advocate" for IO targets nominated for attack throughout the target nomination and review process established by the TFC.**
- **Coordinating the planning and execution of IO between the joint organizations responsible for each element of IO.**
- **Coordinating intelligence support to IO.**

Figure 4-2. IO Officer Functions

(1) IOCC methods. The J-3 or IO officer should determine the methods used by the IOCC to carry out assigned responsibilities. During the planning phases of an operation, IO planners should facilitate the planning efforts between various staffs, organizations, and parts of the TFC staff responsible for planning elements of IO. During the execution phase of an operation, IO planners should be available to the joint operations centre (JOC) or its equivalent to assist in deconfliction, support, or adjustment of IO efforts as necessary. If IO manning permits and the J-3 or IO officer designates, IO personnel may be part of the JOC watch team or stand a separate watch during the execution phase of an operation. IO personnel should have the communications connectivity, either through the JOC or separately, to effectively coordinate changing IO requirements during the execution phase. All members of the IOCC should have appropriate security clearance and access necessary to fulfill their IO responsibilities, due to the sensitive nature of some aspects of IO, such as military deception.

b. DG INT: Sr. J2 Rep: **Resident**. Plans all intelligence support required to support compartmented and non-compartmented IO. When an IOCC is established at a location other than NDHQ, serves as theatre liaison for DG Int (for all IO-related matters dealing with finished analytical support), and all other intelligence entities.

c. J-5 Planner: **Nonresident**. Integrates Civil Affairs into the IO planning process.

d. J-6 Planner: **Resident**. Facilitates defensive IO coordination between information system planners and managers and members of the IOCCs. Coordinates with the J3 to minimize offensive IO operations impact on own force C2. Principal liaison with the joint communications control centre (JCCC). Coordinates information system support to the IOCC. Serves as the joint COMSEC monitoring activity (JCMA) point of entry into the staff. JCMA capabilities affords the potential for near-real-time evaluation of the communications security posture of planning efforts and ongoing operations.

e. PSYOP Planner: **Resident**. International information/PSYOP planner. Integrates, coordinates, deconflicts, and synchronizes PSYOP plans with other Canadian Government information efforts. Serves as entry point for liaison with the in-theatre multinational PSYOP cells, as appropriate.

f. EW Planner: **Resident**. Serves as EWCC leader. Also serves as CFEWC and Defence Electronics & Communications & Spectrum Services (DECSS) liaison officer. Coordinates closely with J6 planner to deconflict IO on the friendly communications spectrum.

g. OPSEC Planner: **Resident**. Coordinates TFC or subordinate command OPSEC activities. Works closely with J6 planner for JCMA liaison.

h. Deception Planner: **Resident**. Coordinates IO inputs to military deception planning.

i. Special Technical Operations (STO): **Resident**. The STO planner should be fully integrated into the IOCC to ensure STO planning and capabilities are fully integrated and coordinated.

j. J2 Counterintelligence: **Resident**. Coordinates IO inputs to CI operations that have significant roles in both information attack and information protection. Works under the overall guidance and direction of the Senior J2 Representative.

k. Information Attack Planner: **Resident**. Serves as principal liaison with CSE, Environmental IO activities, component IOCCs, and Environmental Cryptologic Direct Support Elements for all IO-related cryptologic matters, including computer-related IO areas. Supports deconfliction for intelligence gain or loss assessments and related IO.

l. Public Affairs Officer: **Resident**. Media interface. Coordinates media interface.

m. Legal Officer: **Nonresident**. Ensures all IO complies with domestic and international law.

n. CA Officer: **Nonresident**. Ensures consistency of PSYOP message to the targeted audience in situations where CA activities or CIMIC units are employed.

o. Special Operations Planner (as required): **Nonresident**. Coordinates use of special operations forces within a TFC's AO in support of IO.

p. Targeting Representative: **Nonresident**. Represents the targeting cell(s) and coordinates IO targeting with targeting cell(s).

q. Other Representatives and Liaison Officers: Figure 4-1 is intended as a guide in determining which members of a joint staff should coordinate with IO planners. The Commander should tailor the composition of the cell as necessary to accomplish the mission.

3. Role of Functional and Environmental Representatives in IO. Functional and Environmental Commanders should organize their staffs to plan and conduct IO. An IO point of contact or IO officer should be designated. This officer or an assistant will interface with the joint force IOCC to provide component expertise and act as a liaison for IO matters between the joint force and the component. These representatives also may serve as members of one or more of the supporting organizations of IO (i.e., the EWCC). In addition,

Environmental and functional components requesting specific IO support from sources internal or external normally should request such support through the IOCC.

4. Role of OGDs and Agencies / Representatives of Multinational Forces and their Governments. OGDs and agencies may have a role in the accomplishment of IO. TFCs and their IO officers should ensure OGDs and agencies having ongoing programs and interests in the AO are consulted in the development of IO plans. The supporting OGDs and agencies should be considered as part of the IO plan when appropriate. Likewise, the potential contributions and concerns of multinational forces and their governments should be considered when appropriate.

> ***"In war it is not always possible to have everything go exactly as one likes. In working with allies it sometimes happens that they develop opinions of their own."***
>
> **Sir Winston Churchill, *The Hinge of Fate, 1950***

403. RELATIONSHIP WITH OTHER ORGANIZATIONS

1. General. As discussed above, IO planners use other organizations to plan and execute IO. Support from these organizations currently includes, but is not limited to, personnel augmentation from CFEWC, DECSS, and JCMA. Additionally, through the various planning organizations that plan and direct IO capabilities and elements of IO, the IO planners have access to the Environmental or functional component expertise necessary to plan the employment or protection of Environmental component systems or units.

2. CF Electronic Warfare Centre (CFEWC). The CFEWC may provide direct support to the Commander through the Commander's IOCC.

3. Defence Electronics & Communications & Spectrum Services (DECSS). The DECSS can provide the following direct support to the Commander through the Commander's IOCC:

a. Locational and technical characteristics about friendly force C2 systems.

b. Assistance in development of the joint restricted frequency list (JRFL) for deconfliction purposes. The DECSS may deploy an augmentation team trained to prepare JRFLs or provide training and assistance in how to prepare a JRFL.

c. Assistance in the resolution of operational interference and jamming incidents. The DECSS may deploy personnel to assist in quickly locating and identifying interference sources and recommending technical and operational fixes to resolve identified interference sources.

d. Locational and technical characteristics about adversary force C2 systems.

e. Unclassified C3 & I area studies about the regional C3 infrastructure, to include physical and cultural characteristics, overview of telecommunications systems, and electromagnetic frequencies registered for use within the geographic boundaries of each country in the region.

5. CF Information Operations Group (CFIOG) in conjunction with the Communications Security Establishment (CSE).

a. Provides COMSEC monitoring and analysis support.

b. Provides timely, tailored report to supported commanders. Where this reporting is of an intelligence nature, it shall be under the overall direction and coordination of the J2 Representative.

6. J6 Ops. Commanders normally receive tactical communications support, to include augmentation by a wide array of tactical and commercial communications equipment from J6 Ops. J6 Ops personnel provide defensive IO planning and deconfliction expertise to the IOCC and ensure appropriate protection for J6 Ops-provided telecommunications and information systems services.

7. JCCC. Commanders normally establish a JCCC to support top-level network control and management within the AO. JCCCs play a vital role in IO, particularly in the defensive IO process, where they provide J-6 connectivity throughout the chain of command.

404. TFC IOCC RELATIONSHIPS WITH SUPPORTING DND ORGANIZATIONS

1. CSE. If assigned a CSE representative, the IOCC should receive direct support for the following:

a. advice, guidance and services to DND on the planning, acquisition, installation, and procedures for use of secure communications systems;

b. supply cryptographic keying material, devices and documentation;

c. conduct research, development and evaluations on security aspects of automated information and communications systems, with a view to advising CFIOG on the security of these systems and their application

d. advise and guide CFIOG in developing secure communications and information systems for government requirements; and

e. provide advice, guidance and services for the protection of the security and privacy interests of Canadians.

2. DG Int / J2. A DG Int / J2 representative to the IOCC will plan and coordinate all IO intelligence requirements. This will include (but not be limited to) the following:

a. Precise and timely intelligence for IO target selection and post-strike analysis.

b. Coordinate IO requirements and interface with J2 I&W activities including a capability to analyze and disseminate IO attack warnings.

c. Coordinate the provision of intelligence assistance in the planning and execution of defensive IO activities.

d. Assistance in identifying friendly vulnerabilities and the most probable friendly targets within the adversary's or potential adversary's capabilities and concept of operations.

3. CFIOG. When assigned a CFIOG representative, the following support will be provided to the IOCC:

a. Coordination with DG Int / J2, CSE and the Environments to ensure sufficient database support for planning, analysis, and execution of IO.

b. Assistance in disseminating warnings of IO attacks.

c. Assistance in establishing a security architecture and standards for protecting and defending the integrated information environment (IIE) within the AO.

d. Development of an information system incident program and a security incident response capability or protecting and defending the IIE within the AO.

e. Assessment of the vulnerabilities of information and information systems and development within available capabilities of procedures to mitigate assessed vulnerabilities and threat effects.

f. Development of INFOSEC education, training, and awareness program guidelines, including minimum training standards, for use by the TFC headquarters, components, and subordinate commands.

> ***"The primary object of organization is to shield people from unexpected calls upon their powers of adaptability, judgment, and decisions."***
>
> **General Sir Ian Hamilton,**
> ***Soul and Body of an Army,*** **1921**

CHAPTER 5

INFORMATION OPERATIONS PLANNING

> ***"War plans cover every aspect of a war, and weave them all into a single operation that must have a single, ultimate objective in which all particular aims are reconciled."***
>
> **Major General Carl von Clausewitz**
> ***"On War,"* viii, 1832, tr. Howard and Paret**

501. IO PLANNING METHODOLOGY

1. General

   a. IO planning is an integral part of the operations planning process.

   b. IO planning must be broad-based and encompass employment of all available IO resources - DND, OGD and multinational.

   c. Mission specific IO planning must begin at the earliest stage. Ideally, peacetime IO planning will be ongoing at all times, and as such, provide a basis for subsequent IO in OOTW and/or conflict in that AO.

   d. IO planning must analyze the risk of compromise, reprisal, escalation of hostilities, and uncoordinated or inadvertent counteraction of IO activities by the various joint, environmental, and/or interagency IO capability providers that may be released to the Task Force Commander (TFC) for employment.

2. IO Planning Fundamentals. Planning for employment of IO begins with understanding and articulating the objective, purpose of operations, and commander's intent. A joint campaign is the synchronization of Sea, Land, Air and Special Operations (as well as interagency) in harmony with diplomatic, economic, and IO to attain national and multinational objectives. The same fundamentals of operations planning listed in Chap 1/Sect 1/Art 102/para 2 of the *CF Operations Manual, B-GG-005-004/AF 000* apply to the IO portion of a plan. Some of these fundamentals are particularly important in planning and execution of IO.

   a. The synchronization and integration of the IO requires clear national strategic guidance. This strategy, shaped by and oriented on national security policies, must provide overall direction to the DCDS. This direction is required to ensure IO planning and execution supports national objectives. The DCDS in turn, provides guidance and direction for the employment of the Canadian Forces in Joint or Combined military operations, and in support to OGD both National and Allied. These strategies should support the DCDS stated objectives across the range of military operations. The DCDS and TFC must consider the strategic environment during the estimate and planning process in order to determine potential constraints. These constraints will limit the TFC's freedom of action and influence the timing and form of the operation. The TFC must provide components and subordinate joint forces critical planning guidance to include primary targets/goals and those areas/actions to be avoided. This guidance will establish the "boundaries" for IO planning, identify target limitations based on policy, and serve to reduce the uncertainty associated with IO planning.

   b. IO planning requires an orderly schedule of decisions. Generally IO will require long-term development of intelligence and preparation of the battlespace for optimal use of capabilities. The use of IO in peacetime as a principal means to achieve national objectives and preclude other conflict requires an ability to integrate IO capabilities into a coherent strategy.

   c. Strategic level IO planners must also consider integration with and support to operational and tactical level IOCCs in the development of the Information Operations plan to support the commander's objectives. The direction and inputs necessary for these subordinate IOCCs to function effectively

must be provided clearly in a timely manner. IO plans and activities must also be integrated and coordinated with the actions of OGDs and other involved agencies.

d. Establishing the organization of subordinate TFs and designating command relationships is also very important in developing and executing IO. Establishing these relationships is the basis for achieving unity of command and effort among sea, land, air, space, and special operations forces. This also establishes interagency agreement on the synchronization, coordination, and deconfliction process for IO planning and execution.

e. In planning for IO, the planners will identify an adversary's vulnerabilities, devise required tasks and sub-tasks, and identify the methodologies to exploit these vulnerabilities in order to achieve the desired objectives. The means or capabilities employed may include organic or non-organic/international capabilities. This requires the planners/IOCC to identify all IO resources available for the operation in order to provide the TFC with a "Toolbox" which can be used in developing the IO plan and facilitating an effective capability to target match. As part of the planning process, designation of release and execution authority for SIO is required. Release authority grants approval for employment of IO and normally specifies allocation of specific offensive IO means and capabilities available to the TFC and/or his subordinates. Executive authority is the authority to conduct SIO at a designated time and/or place. Executive authority will normally be vested in the TFC.

f. The identification of the adversary's strategic and operational centers of gravity and development of a methodology for defeating them is a fundamental to IO planning. The Intelligence preparation of a battlespace (IPB) for IO differs from traditional requirements, and will normally need greater lead time and expanded collection requirements. The intelligence community must have access to systems; gain knowledge of installation schematics and physical and virtual connectivity; and develop dynamic tools to exploit this information and other specialized information such as psychological profiles and infrastructure models. Figure 5-1 shows a means to template IO planning and assessments against an adversary. Defensive IO planning has specific intelligence requirements for determining adversary IO capabilities and intentions as well as developing an IO I&W process.

g. Identifying and providing guidance on protecting the critical friendly information centers of gravity at the TFC operational level and those at the strategic level IIE is important. Identifying friendly information priorities requires close coordination and cooperation between DND, OGD and industry. Protection of the IIE requires collaborative efforts to implement protective measures commensurate with the value of the information or information systems protected.

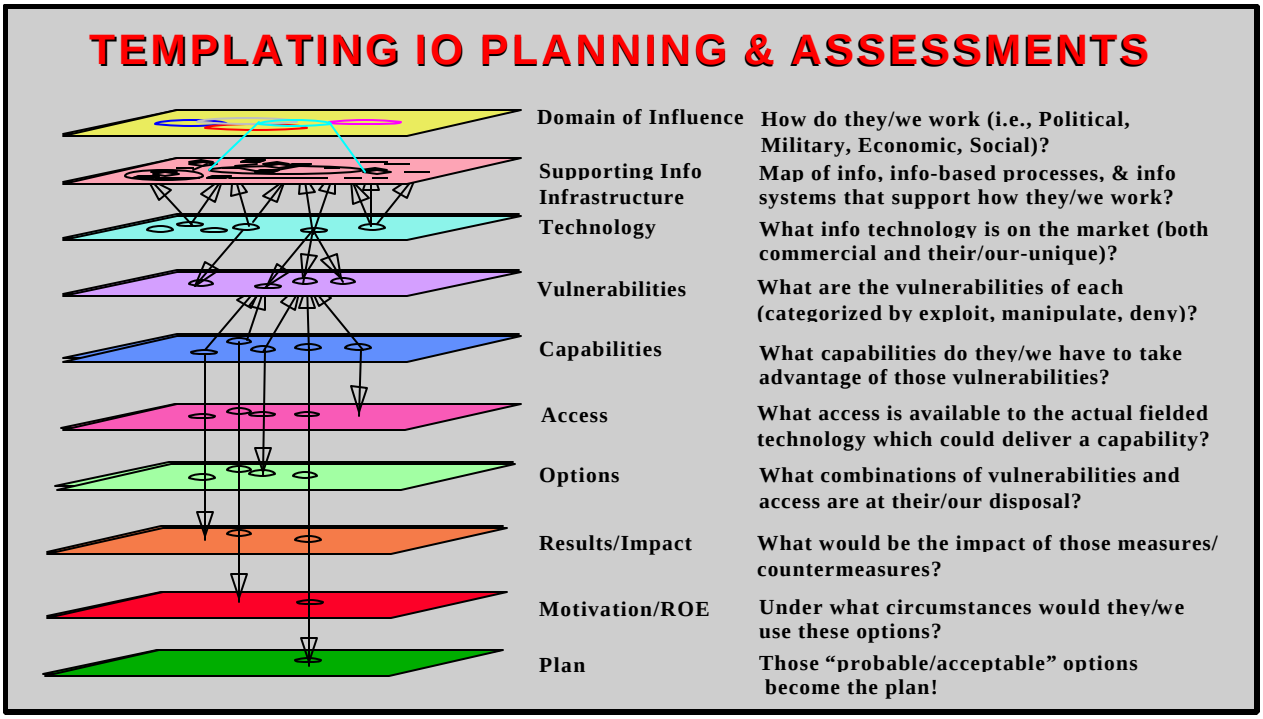

Figure 5-1. Templating IO Planning & Assessments

Adherence to a common level of protection requires determining the scope of what needs to be protected and the standards for how much protection is needed.

3. IO Coordination Cell (IOCC)

a. At the strategic and operational levels, the IOCC is the focal point for IO planning which must include synchronization, coordination, and deconfliction of all available IO resources and efforts. The prime function of this coordination is the integration and deconfliction of IO capabilities to accomplish mission objectives.

b. The IOCC should be represented in all planning activities. The relationship of the IOCC to other planning activities is provided in paragraph 503 below.

502. FUNDAMENTALS OF OPERATIONS PLANS

1. There are several fundamental principals that must be included in Operations Plans.

a. Provide broad strategic concepts of operations and sustainment for achieving multinational, national and AO strategic objectives.

b. Provide an orderly schedule of decisions.

c. Achieve unity of effort with sea, land, air, and special operations forces, in conjunction with interagency, nongovernmental, or private voluntary organizations or United Nations or other multinational forces, as required.

d. Incorporate the TFC's strategic intent and operational focus

e. Identify any special forces or capabilities which may be present in the AO.

f. Identify adversarial strategic and operational centres of gravity and provide guidance to subordinates for conducting operations against the identified centres of gravity.

g. Identify friendly strategic and operational centres of gravity and provide guidance to subordinates for protecting them.

h. Sequence a series of related major joint operations conducted simultaneously in depth.

i. Establish the organization of subordinate forces and designate command relationships.

j. Serve as the basis for subordinate planning and clearly define what constitutes success, including conflict termination objectives and potential posthostilities activities.

k. Provide strategic direction; operational focus; and major tasks, objectives and concepts to subordinates.

2. See the CF Force Employment Manual, Chap 4, for further details on the fundamentals of operations plans.

503. IO PLANNING COORDINATION

1. General. IO coordination is continuous, from the earliest indication that military action may be required, through all stages of planning, force generation, force employment, and ultimately post-conflict actions or activities within the AO. These post-conflict actions/activities include transition of the operation to foreign military or non-military agencies and organizations.

2. Joint Staff Action Team (JSAT). The JSAT must have representation from the IOCC to ensure the IO aspects of any and all operations are considered at the earliest stages of deliberations regarding possible military actions.

3. Joint Planning Team (JPT). The TFC's planning team must also have representation from the IOCC. Early and continuous exchange of information between the JPT and the IOCC is essential to successful integration of IO planning in the overall Force Employment Process.

4. Target Coordination Cell (TCC). As with the JPT, IOCC representation in the TCC (if established) is essential if effective IO coordination is to be provided the targeteers. This representation will also provide a means to coordinate TF capabilities with the application to IO and other conventional operations.

504. IO INTEGRATION AND DECONFLICTION

1. IO Integration. In order to ensure effective IO, its planning must be integrated with other aspects of the operation at the earliest possible stage. This planning must cross all boundaries between components, groups, organizations, and/or agencies that may be involved in execution of the operation.

a. IO by its nature is often de-centralized. As a result, it is imperative the lowest practicable levels of Command be provided knowledge of the plan and participate in its development as appropriate.

b. The IOCC should provide the overall integration strategy for IO and ensure it is integrated.

(1) The IOCC will normally have the assigned personnel, communications linkages, and connectivity with J-6 and defensive IO providers to effectively integrate defensive IO planning.

(2) Strictly within the context of IO, the IOCC also maintains connectivity with OGD such as CSE, CSIS, and the RCMP, who have a role in IO.

c. Compartmentalized IO Capabilities. Members of the IOCC possessing the proper security clearance and access will integrate compartmentalized IO capabilities into plans. Normally, the cell is the appropriate entity to conduct this integration. In addition, the IOCC has the connectivity to higher authority for plan approval normally associated with compartmentalized operations. Close

coordination between the IOCC and the joint force STO cell, is essential to this integration effort. Additional considerations are addressed in Annex A.

2. IO Deconfliction. IO deconfliction will likely be required at several levels of planning, i.e., within, above, and below the joint force, and at several levels of war. In addressing deconfliction, it will be necessary to address both inter-level and intra-level aspects. As with integration, deconfliction of IO should begin at the earliest possible stage of IO planning.

a. IO deconfliction must be a continuous process that allows for flexible phasing of IO employment options. The likelihood of simultaneous IO at all levels of war and command is quite high. Additionally, the relatively large number of potential IO capability providers in the same AO, particularly when IO is a prime element of a TFC operation, makes early identification of IO deconfliction issues essential.

b. The IOCC is the best entity for coordinating and overseeing IO deconfliction as it has connectivity with all IO providers within the Joint Force. In addition, the IOCC has connectivity with IOCCs above and below it in the chain of command. Finally, the IOCC works with and has input to defensive IO within the Joint Force, thereby providing the IOCC with the best overall view for ensuring IO deconfliction.

505. GUIDANCE FOR IO PLANNING

1. General. IO plans should be developed in support of the overall operational plan. To accomplish this, IO planning should occur simultaneously with operation planning. *The CF Force Employment Manual B-GG-005-004/AF-004* is the operational planner's guide to developing OPLANs through the planning process.

a. IO at the Strategic Level. Figure 5-2 provides a general guide to IO planning as an integrated part of the strategic level planning process as shown in the *CF Force Employment Manual, B-GG-004-005/AF-004*, Annex A, Chap 4. The figure may be adapted for similar IO planning guidance at subordinate TF and component levels as required. When IO planning is being conducted below the strategic level, the subordinate IOCCs should keep the IOCC at the next higher level of command fully apprised of all IO planning activities that may require synchronization, coordination, or deconfliction.

Strategic Process Step	**IOCC Planning Action**	**IO Planning Outcome**
Analyse Mission	Identify information requirements needed for mission planning.	Tasking to gather/obtain required information.
	Assist in development of DCDS's IO planning guidance to support overall operational planning guidance.	DCDS's planning guidance for IO.
Develop Initial COAs	Support the development of intelligence, operations, and communications staff estimates.	IO portion of staff estimates.
Determine preferred COA	Assist in transforming staff estimates into the Commander's Estimate. Assist in the IO aspect of DCDS's Operational Concept as required.	IO portion of overall plan approved.
Prepare Warning Order	Initial liaison with units and agencies that may participate in or support IO operations.	

Strategic Process Step	IOCC Planning Action	IO Planning Outcome
Conduct Detailed Operations Planning	Develop the complete IO plan and the plans for each of the IO elements in coordination with appropriate staff sections, operational units, and supporting agencies.	Approved offensive and defensive appendices with element tabs, completed supporting plans, and inclusion of IO requirements in TFMT.
	Subordinate units and supporting agencies prepare their own IO plans. Coordinate/assist subordinate and supporting IO plans as necessary. Ensure TFMT supports IO plan.	Completed subordinate and supporting agencies' supporting plans. IO plan supported by TFMT.

Figure 5-2. IO Planning at the Strategic Level

b. IO at the Operational Level. Figure 5-3 provides a general guide to IO planning at the operational level in concert with the *CF Force Employment Manual B-GG-004-005/AF-004*, Annex A, Chap 3. As with Figure 5-2, Figure 5-3 may be adapted as required for similar IO planning guidance at the subordinate TF and component levels.

2. Offensive IO Guidance. The final offensive IO planning product at both the strategic and operational planning levels is an approved Operations Plan. This plan contains the overall concept for both offensive and defensive IO with respect to the plan or OPORD in which it appears. It should include the timing, constraints and goals for each action/force effort.

3. Defensive IO Guidance. The final defensive IO planning product at both the strategic and operational planning levels is an approved OPLAN. This OPLAN will be included as a separate Annex in the overall OPORDER. Specific guidance on the preparation of this appendix is included as Annex B.

"The stroke of genius that turns the fate of a battle? I don't believe in it. A battle is a complicated operation, that you prepare laboriously. If the enemy does this, you say to yourself I will do that. If such and such happens, these are the steps I shall take to meet it. You think out every possible development and decide on the way to deal with the situation created. One of these developments occurs; you put your plan in operation, and everyone says "What genius . . ." whereas the credit is really due to the labor of preparation."

Ferdinand Foch, Interview, April 1919

STEPS	KEY ELEMENTS	IOCC TASKS	OUTPUT
INITIATION	Receive Planning task	Notify IOCC members of Planning requirement. Identify information requirements needed for mission planning.	Tasking to gather/obtain required information.
ORIENTATION	Conduct Mission Analysis Attend Mission Analysis Briefing Commander's Planning Guidance Issued	Assist in development of TFC's IO planning guidance to support overall operational planning guidance.	Planning guidance for IO.

STEPS	KEY ELEMENTS	IOCC TASKS	OUTPUT
COA DEVELOPMENT	Analyse Factors Develop COA Information Brief	Support the development of intelligence, operations, and communications staff estimates.	IO portion of staff estimates.
DECISION	Commander's Decision	Assist in transforming staff estimates into the TFC's Estimate. Assist in the IO aspect of TFC's Concept as required.	IO portion of overall plan approved as required.
PLAN DEVELOPMENT	Develop, Co-ordinate, Seek approval Issue plan	Develop the complete IO plan and the plans for each of the IO elements in coordination with appropriate staff sections, operational units, and supporting agencies.	Approved offensive and defensive appendices with element tabs, completed supporting plans, and inclusion of IO requirements in TFMT.
PLAN REVIEW	Plan Review Plan Evaluation Revised Decision Briefing (if req'd)	Modify/refine plan as necessary.	Approved offensive and defensive IO appendices.

Figure 5-3. IO Planning at the Operational Level

CHAPTER 6

INFORMATION OPERATIONS IN TRAINING AND EXERCISES

601. ESSENTIAL ELEMENTS IN IO TRAINING

1. General

   a. Effective employment of IO in joint operations depends on the ability to organize and train in the manner that Canada intends to employ military force. The fundamental task is to train personnel and organizations that are responsible for planning and conducting IO on the concepts and doctrine found in this publication. Opportunities exist for IO training within industry, during allied exercises and at allied training courses; IO training is being introduced all levels of staff training. Policy staff should ensure that IO remains a fundamental part of formal training.

   b. Commanders at all levels should ensure that key personnel responsible for planning and conducting IO fully participate in all available IO training opportunities and receive the appropriate IO training. This training should focus on the AO where IO is likely to be conducted. This training should be directed at routine peacetime IO activities within each Commander's AO as well as transition to crisis and conflict resolution.

   c. The Canadian Forces Military Education system should ensure that officers understand the importance of IO as an overall strategy at the strategic, operational and tactical levels, throughout the continuum of conflict.

2. Offensive IO Training

   a. Offensive IO training should include integration of all available offensive IO capabilities, to include multinational and other DND and non-DND offensive IO capabilities.

   b. Offensive IO training should consist of both individual and organizational training and should emphasize IO attack planning.

   c. Offensive IO training should include planning for and use of all potentially available offensive IO capabilities.

3. Defensive IO Training. Defensive IO training should:

   a. include integration of all available defensive IO capabilities including DND, OGD and commercial defensive IO capabilities;

   b. encompass the training of individuals and organizations, emphasizing the protection of information and the defence of information systems; and

   c. build upon the routine peacetime information and information systems protection procedures used throughout DND, OGDs and the commercial sector.

602. IO IN EXERCISES

1. General

   a. IO should be incorporated in all exercises, joint and combined, at a level appropriate to the scope and duration of the exercise. The implementation of IO during exercises illustrates the complex issues raised by the strategy to exercise planners; the need to coordinate within DND departments, with OGDs and with the Commercial Sector is also highlighted.

   b. Exercises may incorporate IO training in two ways: stand-alone and supporting.

(1) Stand-alone: IO is the only strategy used to affect an adversary.

(2) Supporting: IO is used as a force multiplier within a conventional campaign.

c. Figure 6-1 contains fundamental IO exercise planning considerations.

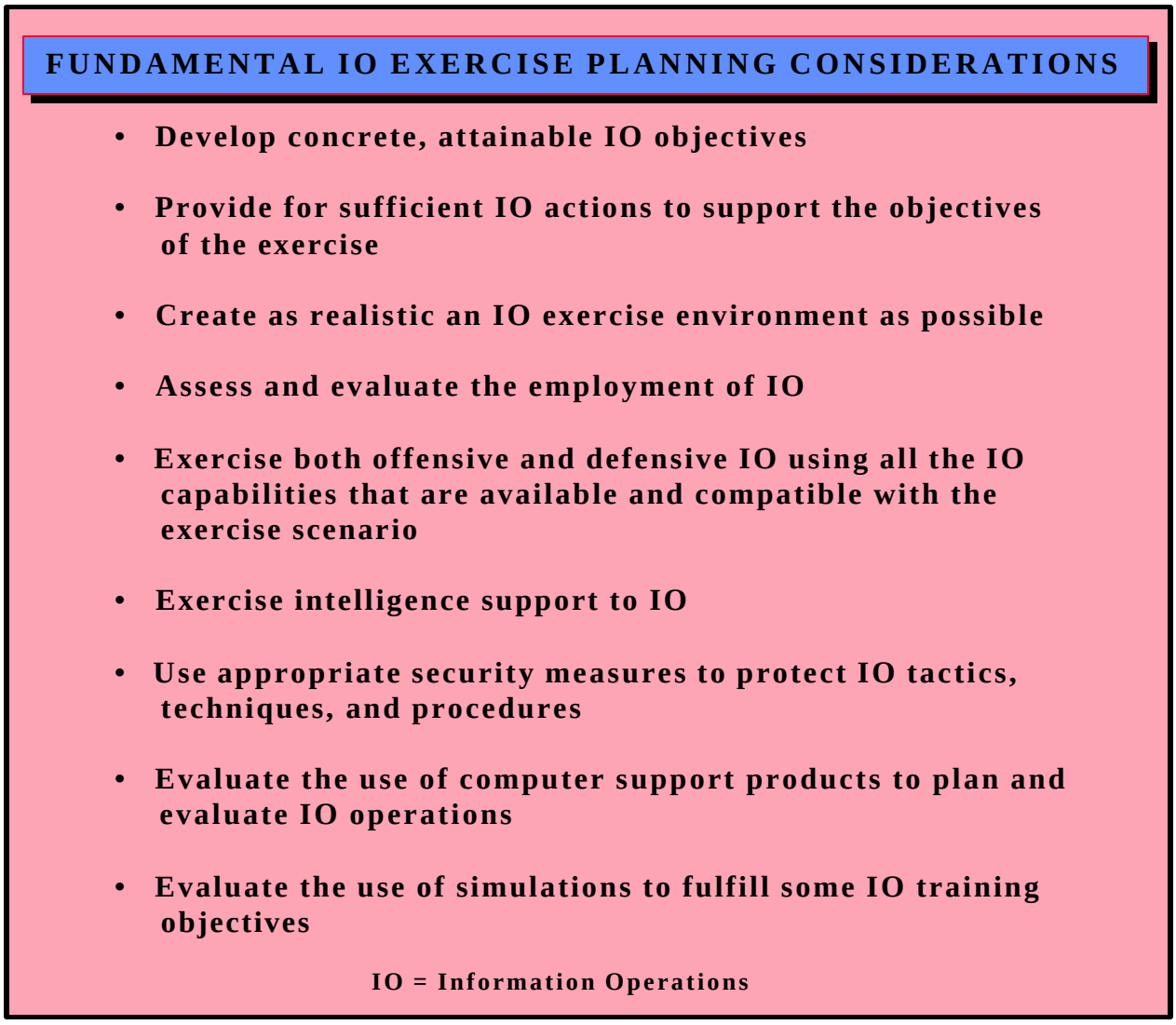

Figure 6-1. Fundamental IO Exercise Planning Considerations

2. Offensive IO

a. Offensive IO planning and execution in joint exercises should emphasize IO attack and use capabilities normally available to the joint force conducting the exercise.

b. Offensive IO capabilities in joint exercises should be provided full intelligence support, particularly intelligence concerning the Opposition Force. In addition, the Opposition Force should be allowed realistic free play to provide an appropriate challenge to both friendly intelligence development and IO targeting efforts.

3. Defensive IO

a. Defensive IO planning and execution in joint exercises should emphasize protection of information, vulnerable to attack through counter psychological operations, counter deception and propaganda

from an adversary, and defence of information systems. Defensive IO capabilities normally available to the joint force should be exercised.

b. Defensive IO planning in exercises also should include protective and defensive considerations for DND, OGDs, and the supporting commercial communications infrastructure.

c. As in offensive IO play in exercises, the Opposition Force should be allowed realistic free play to ensure defensive IO capabilities are stressed or exercised to the appropriate degree. Senior exercise participants should allow the C2 and other information deprivation chaos that arises when ineffective defensive IO measures are planned and implemented. This will encourage exercise participants to work through defensive IO problems caused by effective adversary IO.

603. IO IN PLANNING AND EXERCISE MODELING AND SIMULATION

1. General. IO should be incorporated in all planning and exercise M&S at the earliest practicable stage of model development. Only in this fashion can IO M&S be integrated appropriately with that of the other warfare areas.

2. IO in Planning Models

a. Offensive IO. Planning models should incorporate offensive IO capabilities and principles, to include offensive IO capabilities normally organic to DND and OGDs. Multinational offensive IO capabilities should be included as they become known and available for planning purposes.

b. Defensive IO. Planning models should include potential defensive IO capabilities from the CF, other DND and non-DND OGDs sources, and such commercial defensive IO capabilities as may reasonably be expected to be available for planning purposes. Potential multinational defensive IO capabilities also should be catalogued and included in planning models.

3. IO in Exercise Modeling & Simulation (M & S)

a. Offensive IO. Offensive IO capabilities should be incorporated in exercise M&S to allow realistic free play between friendly joint forces and the Opposition Force. Where possible and when practicable, capabilities should be tailored to fit the offensive IO capabilities of the participating friendly forces and the likely Opposition Force for the exercise AO. In addition, multinational offensive IO capabilities likely to be made available for planning and operations in the region should be added to the exercise model(s) wherever possible.

b. Defensive IO. Defensive IO capabilities organic to the exercising force, DND, OGD and the commercial sector, likely to be available in the exercise AO, should be added to exercise model(s). Commercial defensive IO capabilities and multinational defensive IO resources known to be available in the affected exercise region should be added if possible; this will allow realistic M&S IO play between the joint force and its multinational partners and the Opposition Force.

c. Assessment and Evaluation. The model(s) used in IO M&S should provide a means to assess and evaluate IO employment in both offensive and defensive IO and allow for unambiguous feedback to exercise participants, both the friendly forces and the Opposition Force. The evaluation and assessment also should provide a means to control IO play and make adjustments if IO adversely affect or negate the other training objectives of the exercise.

ANNEX A

INFORMATION OPERATIONS GUIDANCE

The guidance in this annex relates to the development of the Information Operations portions of any and all plans developed for use by the CF.

1. Situation

a. Enemy

(1) What are the enemy situation, force disposition, intelligence capabilities, and possible COAs?

(2) Is there any specific information that bears directly on the planned IO?

b. Friendly

(1) What is the situation of friendly forces that may directly affect attainment of IO objectives?

(2) Are there any critical limitations and other planned IO?

c. Assumptions

(1) What are the assumptions concerning friendly, enemy, or third-party capabilities, limitations, or COAs?

(2) What conditions does the commander believe will exist when the plan becomes an order.

2. Mission. What is the IO mission (who, what, when, where, why)?

3. Execution

a. Concept of Operations

(1) How does the commander visualize the execution of IO from beginning to termination?

(2) How will IO support the commander's mission?

(3) What are the concepts for supervising and terminating IO?

b. IO Tasks

(1) What are the major tasks for military deception? See Appendix A, "IO (Military Deception) Guidance," for further guidance.

(2) What are the major tasks for EW? See Appendix B, "IO (Electronic Warfare) Guidance," for further guidance.

(3) What are the major tasks for OPSEC? See Appendix C, "IO (Operations Security) Guidance," for further guidance.

(4) What are the major tasks for PSYOP? See Appendix D, "IO (Psychological Operations) Guidance," for further guidance.

(5) What are the major tasks for physical destruction related to IO? See Appendix E, "IO (Physical Destruction) Guidance," for further guidance.

(6) What are the major tasks for PA? See Appendix F, “IO (Public Affairs) Guidance,” for further guidance.

(7) What are the major tasks for CA? See Appendix G, "IO (Civil Affairs) Guidance," for further guidance.

c. Coordinating Instructions. What, if any, are the mutual support issues relating to the elements of IO?

4. Administration and Logistics

a. What are the administrative requirements related to IO?

b. What are the logistics requirements related to IO?

5. Command and Control

a. What are the C2 instructions related to IO?

b. What is the command structure for IO?

c. Are there any special communications and reporting requirements for IO? If so, what are they?

IO (MILITARY DECEPTION) GUIDANCE

The guidance in this Appendix relates to the development of the Military Deception portion of any and all plans developed for use by the CF.

1. Situation

a. General. What is the general overall situation concerning military deception?

b. Enemy

(1) General Capabilities. What are the enemy military capabilities relating directly to the planned deception?

(2) Deception Targets. What are the deception targets?

(3) Target Biases and Predispositions. What are the target biases and predispositions?

(4) Probable Enemy COA. What is the probable enemy COA? (Refer to Intelligence portion of the basic plan.)

c. Friendly

(1) What is the friendly forces situation?

(2) What, if any, are the critical limitations?

(3) What is the concept of friendly operations?

d. Assumptions.

(1) What are the assumptions concerning friendly, enemy, or third-party capabilities, limitations, or COAs?

(2) What conditions does the commander believe will exist when the plan becomes an order.

2. Mission

a. Operational Mission. See basic plan or order.

b. Deception Mission

(1) Deception Goal. What is the desired effect or end state the commander wishes to achieve?

(2) Deception Objective(s). What is the desired action or inaction by the adversary at the critical time and location?

(3) Desired Enemy Perceptions. What must the deception target believe for him/her to make the decision that will achieve the deception objective?

(4) Deception Story. What scenario will cause the deception target to adopt the desired perception? Consider one of the COAs discarded during plan preparation.

3. Execution

a. Concept of the Operation

(1) General. What is the framework for the operation? Include a brief description of the phases of the deception operation.

(2) Other IO Elements

(a) What other IO elements will be used to support the deception operation?

(b) What are the other IO element plans and operations pertinent to the deception?

(c) What coordination and deconfliction is required?

(3) Feedback and Monitoring

(a) What type of feedback is expected, if any, and how will it be collected?

(b) What impact will the absence of feedback have on the plan?

(3) Means. By what means will the deception be implemented?

(4) Tasks. What are the execution and feedback taskings to organizations participating in the execution and monitoring of the deception?

(5) Risks

(a) Deception is successful. What is the likely adversary response? What will be the impact on friendly forces from adversary intelligence sharing?

(b) Deception fails. What is the impact if the deception target ignores the deception or fails in some way to take the actions intended?

(c) Deception is compromised to multinational partners or adversaries. What is the impact of such compromise on friendly forces and attainment of friendly objectives?

b. Coordinating Instructions

(1) What are the tasks or instructions listed in the preceding subparagraphs pertaining to two or more units?

(2) What is the tentative D-day and H-hour, if applicable, and any other information required to ensure coordinated action between two or more elements of the command?

4. Administration and Logistics

a. Administration

(1) General. What are the general procedures to be employed during planning, coordination, and implementation of deception activities?

(2) Specific. What, if any, are the special administrative measures required for the execution of the deception operation?

b. Logistics. What are the logistics requirements for the execution of the deception operation (transportation of special material, provision of printing equipment and materials, etc.)?

c. Costs. What are the applicable costs associated with the deception operation?

NOTE: Do not include those administrative, logistics, and medical actions or ploys that are an actual part of the deception operation.

5. Command, Control, and Communications

a. Command Relationships

(1) Approval. What is the approval authority for execution and termination?

(2) Authority. Who are the designated supported and supporting commanders and supporting agencies?

(3) Oversight. What are the oversight responsibilities, particularly for executions by non-organic units or organizations outside the chain of command?

(4) Coordination

(a) What are the in-area coordination responsibilities and requirements related to deception executions and execution feedback?

(b) What are the out-of-area coordination responsibilities and requirements related to deception executions and execution feedback?

b. Communications

(1) What are the communications means and procedures to be used by control personnel and participants in the deception operation?

(2) What are the communications reporting requirements to be used by control personnel and participants in the deception operation?

6. Security

a. General. What are the general security procedures to be employed during planning, coordination, and implementation of deception activities?

b. Specific

(1) What are the access restrictions and handling instructions to the deception appendix or plan?

(2) Who has authority to grant access to the deception appendix or plan?

(3) How will cover stories, codewords, and nicknames be used?

(4) How will planning and execution documents and access rosters be controlled and distributed?

NOTE: Additional exhibits to the Military Deception portion of the plan may be required as shown below.

Exhibits:

1--Task Organization

2--Intelligence

3--Operations

4--Administration and Logistics

5--Command Relationships

6--Execution Schedule

7--Distribution

IO (ELECTRONIC WARFARE) GUIDANCE

The guidance in this Appendix relates to the development of the Electronic Warfare portion of any and all plans developed for use by the CF

1. Situation

a. Enemy Forces

(1) What are the capabilities, limitations, and vulnerabilities of enemy communications, non-emitting, and EW systems?

(2) What is the enemy capability to interfere with accomplishment of the EW mission?

b. Friendly Forces

(1) What friendly EW facilities, resources, and organizations may affect EW planning by subordinate commanders?

(2) Who are the friendly foreign forces with which subordinate commanders may operate?

c. Assumptions. What are the assumptions concerning friendly or enemy capabilities and COAs that significantly influence the planning of EW operations?

2. Mission. What is the EW mission (who, what, when, where, why)?

3. Execution

a. Concept of Operations

(1) What is the role of EW in the commander's IO strategy?

(2) What is the scope of EW operations?

(3) What methods and resources will be employed? Include organic and non-organic capabilities.

(4) How will EW support the other elements of IO?

b. Tasks. What are the individual EW tasks and responsibilities for each component or subdivision of the force? Include all instructions unique to that component or subdivision.

c. Coordinating Instructions

(1) What instructions, if any, are applicable to two or more components or subdivisions?

(2) What are the requirements, if any, for the coordination of EW actions between subordinate elements?

(3) What is the guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered elsewhere in this tab?

(4) What is the emissions control guidance? Place detailed or lengthy guidance in an exhibit to this tab.

(5) What coordination with the J6 is required to accomplish the JRFL?

4. Administration and Logistics

a. Administration

(1) What, if any, administrative guidance is required?

(2) What, if any, reports are required? Include example(s).

b. Logistics. What, if any, are the special instructions on logistics support for EW operations?

5. Command and Control

a. Feedback

(1) What is the concept for monitoring the effectiveness of EW operations during execution?

(2) What are specific intelligence requirements for feedback?

b. After-Action Reports. What are the requirements for after-action reporting?

c. Signal. What, if any, are the special or unusual EW-related communications requirements?

IO (OPERATIONS SECURITY) GUIDANCE

The guidance in this Appendix relates to the development of the Operations Security portion of any and all plans developed for use by the CF.

1. Situation

a. Enemy Forces

(1) Current Enemy Intelligence Assessment

(a) What is the estimated enemy's assessment of friendly operations, capabilities, and intentions?

(b) What is the known enemy knowledge of the friendly operation addressed in the basic plan?

(2) Enemy Intelligence Capabilities

(a) What are the enemy's intelligence collection capabilities according to major categories (signals intelligence, HUMINT, imagery intelligence, etc.)?

(b) What potential sources (including other nations) provide support to the enemy?

(c) How does the enemy's intelligence system work? Include the time required for intelligence to reach key decisionmakers.

(d) What are the major analytical organizations and who are the key personalities?

(e) What, if any, unofficial intelligence organizations support the national leadership?

(f) What are the enemy intelligence capabilities strengths and weaknesses?

b. Friendly Forces

(1) Friendly Operations. What are the major actions to be conducted by friendly forces in the execution of the basic plan?

(2) Critical Information. What is the identified critical information? Include the critical information of higher headquarters. For phased operations, identify the critical information by phase.

c. Assumptions. What are the assumptions upon which this OPSEC plan is based?

2. Mission. What is the OPSEC mission (who, what, when, where, why)?

3. Execution

a. Concept of Operations

(1) What is the role of OPSEC in the commander's IO strategy?

(2) What is the general concept for the implementation of planned OPSEC measures? Describe these by phase and major activity (maneuver, logistics, communications, etc.), if appropriate.

(3) What will be the OPSEC support to other elements of IO?

b. Tasks. What are the specific OPSEC measures to be executed? List these by phase and include specific responsibilities for subordinate elements.

c. Coordinating Instructions

(1) What are the requirements for coordination of OPSEC measures between subordinate elements?

(2) What is the required coordination with public affairs?

(3) What is the guidance on termination of OPSEC-related activities?

(4) What is the guidance on declassification and public release of OPSEC-related information?

4. Administration and Logistics

a. What, if any, are the OPSEC-related administrative or logistics support requirements?

b. What, if any, are the administrative- or logistics-related OPSEC measures?

5. Command and Control

a. Feedback

(1) What is the concept for monitoring the effectiveness of OPSEC measures during execution?

(2) What are the specific intelligence requirements for feedback?

c. OPSEC Surveys. What are the plans for conducting OPSEC surveys in support of this operation?

d. After-Action Reports. What are the requirements for after-action reporting?

e. Signal. What, if any, are the special or unusual OPSEC-related communications requirements?

IO (PSYCHOLOGICAL OPERATIONS) GUIDANCE

The guidance in this Appendix relates to the development of the Psychological Operations portion of any and all plans developed for use by the CF.

1. Situation

a. Overview

(1) What is the general psychological situation in the AO?

(2) What, if any, are the on-going PSYOP programs?

(3) What are the significant factors influencing PSYOP activities?

(4) What are the competing PSYOP goals in the AO?

(5) What is the PSYOP task to be accomplished?

b. Canadian (or Canadian and Allied/Coalition) Perspective

(1) How will the assigned PSYOP task be accomplished?

(2) What resources will be used?

(3) What will be the general phasing of current actions with future actions?

c. Neutral Perspective (if applicable)

(1) What are the estimated neutral intentions under various circumstances?

(2) What activities and resources are available to these neutral intentions?

(3) What neutral actions and behavior would favor mission accomplishment?

(4) Which apparent current COAs might affect mission accomplishment?

(5) What resources are available to execute alternative COAs?

(6) What objective and subjective factors could affect decisions and resource effectiveness?

(7) What are the staff factions and who are the particularly influential individuals?

(8) What are the characteristics of decisionmakers and their key advisors, major staff planners, staff factions (to include particularly influential individuals), and intelligence system analysts?

(9) What are the groups of related planner and decisionmaker essential elements of friendly information (EEFI)?

(10) What is the estimated background knowledge and desired and harmful appreciations for each group?

d. Enemy Perspectives

(1) Decisionmaker and Staff

(a) Who are the decisionmakers who can direct development or allocation of resources of COA pertinent to the task assigned?

(b) What feasible alternative actions would favor or harm friendly operational effectiveness?

(c) What COAs might affect friendly task accomplishment?

(d) What resources are available to execute each COA?

(e) What are the characteristics of enemy decisionmakers, their key advisors, and staff (particularly intelligence analysts)?

(2) Intelligence Systems

(a) What are the intelligence systems that support decisionmakers and their staffs?

(b) What are the intelligence systems' capabilities pertinent to the situation?

(c) What are the objective and subjective factors and the characteristics of collection planners and decisionmakers that affect their development and selection for use of information gathering resources?

(d) What are the groups of related planner and decisionmaker EEFI?

(e) What is the estimated background knowledge and desired and harmful appreciations for each group?

(3) Target Audiences

(a) What groups can influence plans, decisions, and operational effectiveness in task accomplishment?

(b) What is these groups' susceptibility to PSYOP?

(c) What group behavior is favorable or harmful to task accomplishment?

(d) What are the apparent goals, motivations, and characteristics of each group?

(e) Who are the leaders who can cause these groups top behave in various ways?

(f) What are the groups of related target audience EEFI?

(g) What is the estimated background knowledge and desired and harmful appreciations for each group?

(4) Command Systems

(a) What communications systems and command centres will be used to plan COAs and control, coordinate, and supervise execution of the planned COA?

(b) What is the purpose and what are the characteristics of each command and control communications net?

(c) What are the PSYOP targets for jamming or attacking?

(d) When should PSYOP operations to demoralize and disorganize opposing command be executed?

(e) When should PSYOP operations to reduce opposing operational effectiveness be executed?

(f) When should PSYOP operations to enhance the effectiveness of planned deceptions and PSYOP be executed?

(g) When should PSYOP operations to support OPEC to the maximum advantage be executed?

2. **Mission**. How will the PSYOP mission support the maneuver commander?

3. **Execution**

a. Concept of Operations

(1) Overview

(a) What is the commander's intent?

(b) What is the overall concept for using PSYOP in support of task accomplishment?

(c) Who will plan and conduct strategic PSYOP in peacetime and in support of pre-conflict deterrence options? Who are the supporting commanders?

(d) Who will plan and conduct strategic and operational PSYOP in support of sustained hostilities? Who are the supporting commanders?

(e) Who will plan and conduct joint tactical PSYOP is support of operational COAs? Who are the supporting commanders?

(2) General Guidance to Units and Forces

(a) What are the valid PSYOP themes to be promoted to induce strategic and theatre PSYOP objectives?

(b) What are the valid or invalid PSYOP themes to be discouraged? Include indications of specific target audience sensitivities and harm that might occur if the themes are accepted by target audiences.

(c) PSYOP Actions Suitable for Use

1. What is the guidance for the conduct of military operations and actions and personnel behavior to promote valid PSYOP themes?

2. What is the guidance for avoiding military operations and actions and personnel behavior that would result in harmful target audience attitudes and behavior?

3. What are the cultural and psychological characteristics of target audiences which will aid operational planners and personnel in selecting COAs and interacting with target audience members?

(d) Adversary PSYOP

1. What adversary PSYOP will be directed at Canadian personnel and at foreign groups in the AO.

2. What is the guidance for countering such adversary operations?

(3) Outline of Each Planned PSYOP Operation

(a) What is the target audience and set of PSYOP objectives, overall themes, subgroups to be targeted (to include their characteristics), and specific themes to be promoted for each subgroup?`

(b) What are the provisions for testing, producing, stocking, and disseminating PSYOP materials and for measuring PSYOP effectiveness?

(c) What are the command and staff arrangements? Who are the supporting commanders?

(d) What resources are required to plan and conduct PSYOP actions? Include civil capabilities; indigenous assets; exploitation of enemy prisoners of war (EPWs), internees, and detainees for PSYOP; and military PSYOP resources.

(e) What are the logistics requirements? Include preparation, distribution, and stocking of PSYOP materials; transport of PSYOP material and personnel to operational areas and their basing and support while conducting PSYOP; provisions for the supply and maintenance of Canadian and indigenous PSYOP material; and fiscal and personnel matters.

(f) What are the requirements for implementing schedules and PSYOP operation control sheets?

(g) What is the codeword for OPSEC-sensitive PSYOP?

(4) What is the OPSEC planning guidance? Include planning for, preparing for, and conducting PSYOP and PSYOP actions to maintain essential secrecy for the commander's intention and to gain and maintain essential secrecy for OPSEC-sensitive PSYOP COAs.

b. Situation Monitoring

(1) How will intelligence, multi-discipline CI, security monitoring, and operational feedback be provided?

(2) What is the requirement for running situation estimates; periodic estimates of target appreciations responsive to EEFI, actions, and attitudes and behavior; and current reporting of intelligence and multi-discipline CI information, security monitoring results, and implementing actions.

(3) What resources are required? What is their availability?

c. Control

(1) How will control be affected and implementation centrally coordinated?

(2) What are the coordinating instructions?

(3) How will implementation planning and supervision of the planned action be accomplished?

(4) What is the need for specific PSYOP operations?

(5) What coordination is required with adjacent commands and civilian agencies, to include Canadian diplomatic missions?

(6) What coordination is required with military deception and OPSEC planners, EW planners, and planners in the fields of civic action, humanitarian assistance, civil affairs, EPWs, CI, detainees, C3, legal, captured Canadian or allied personnel, and operations?

d. Tasks

(1) What responsibilities must be assigned to implement the concept?

(2) Is designation of an executive agent to coordinate implementation among multiple organizations required?

(3) How will feedback to ensure effectiveness of tasks be provided?

4. Administration and Logistics

a. Logistics

(1) What is the guidance on stocking of propaganda and information materials and provisions to disseminating organizations?

(2) What are the provisions for the supply and maintenance of PSYOP-unique supplies and equipment?

(3) What are the provisions for control and maintenance of indigenous equipment and materials?

(4) What are the fiscal matters relating to special funds?

(5) What are the personnel matters relating to indigenous personnel?

b. Administration

(1) What are the requirements for special reports?

(2) What are the requirements for planning and operations is support of education programs regarding EPWs and civilian internees?

(3) What will be the participation in interrogation of EPWs, internees, and detainees to obtain information essential or peculiar to PSYOP?

5. **Command and Control**. Refer to appropriate sections the basic plan and provide pertinent extracts of information included in the basic plan, to include the following:

a. What are the recognition and identification instructions?

b. What is the electronic policy?

c. What are the headquarters locations and movements?

d. What are the codewords?

e. What is the frequency allocation?

IO (PHYSICAL DESTRUCTION) GUIDANCE

The guidance in this Appendix relates to the development of the Physical Destruction portion of any and all plans developed for use by the CF.

1. Situation

a. Enemy Situation. What is the general situation in the target country?

b. Friendly Situation

(1) What is the situation of those friendly forces (higher, adjacent, supporting, and reinforcing) that may affect directly C2 and key infrastructure destruction operations?

(2) What, if any, are the critical limitations and any other planned IO?

c. Assumptions. What, if any, are the assumptions on which this plan is based?

2. Mission. What is the C2 and infrastructure physical destruction mission?

3. Execution

a. Overview

(1) How does the commander visualize the execution of this supporting plan to the IO plan from its beginning to its termination?

(2) What are the phases of the operation?

(3) What is the TFC's intent and desired end state?

b. Tasks for Subordinate Commands. What are the major tasks of each subordinate command?

c. Coordinating Instructions. What are the rules of engagement that impact the C2 and infrastructure destruction plan?

4. Administration and Logistics

a. What are the applicable administrative arrangements, if any, not covered in the basic plan?

b. What are the applicable logistics arrangements, if any, not covered in the basic plan?

5. Command and Control. What are the applicable command and control arrangements, if any, not covered in the basic plan?

IO (PUBLIC AFFAIRS) GUIDANCE

The guidance in this Appendix relates to the development of the Public Affairs portion of any and all plans developed for use by the CF.

1. Situation

a. General. What are the general responsibilities and guidance for military PA actions (public information, command and internal information, and community relations)?

b. Enemy. What are the expected actions of enemy forces and forces hostile to Canadian interests?

c. Friendly. What are the friendly agencies not under TFC control who will contribute to the PA effort? Include Director General Public Affairs, Canadian ambassadors, and allied/coalition PA programs.

d. Policy. What is the applicable PA policy pertaining to this plan?

e. Assumptions

(1) What are the host-nation preferences to be considered in developing and executing PA programs?

(2) Should the TFC be prepared to host the DND National Media Pool during the initial stages of operations?

2. Mission. What are the task and purpose of PA in the operation?

3. Execution

4.

a. Concept of Operations

(1) What PA support will be required in the following five phases:

(a) Warning

(b) Preparation

(c) Deployment

(d) Employment

(e) Redeployment

b. Tasks

(1) What are the PA tasks to be completed during the above-listed phases?

(2) What, if any, are the additional information release instructions to the TFC and other supporting commands, to include release authority and guidance on casualty and mortuary affairs, postal affairs, and POW or MIA and EPW matters?

(3) What are PA visual information and combat camera requirements?

(4) What are the detailed personnel and equipment support requirements to component commands? Include access to the secure voice circuit that connects the Joint Information Bureau (JIB) and on-scene commander, supported operational commander, and the Department of Foreign Affairs and International Trade representative; access to hard copy message facilities between the same points; and inter-theatre and intra-theatre transportation for escorted media.

(5) What are the TFC, and other supporting commands' support requirements?

c. Coordinating Instructions

(1) Command Relationships. What are the PA command relationships?

(2) Coordination of Release of Information. What are the detailed procedures for all supporting commands for handling or forwarding to the supported command queries, responses, and proposed news releases for clearance?

(3) Other Coordinating Instructions

(a) What is the guidance for interviews and news conferences with returned Canadian personnel and EPWs or detained personnel?

(b) What is the required PA coordination with other staff elements involved in release of information outside the command?

(c) What are the procedures for keeping PA historical records?

4. Registration. What is the guidance for military support to the media?

5. Security Review. What, if any, are the security review procedures?

6. Arrangements for the Media. What are the details on planned media support? Include details concerning messing, billeting, emergency medical treatment, access to transportation and communications facilities at Government expense, access to unclassified operational information, and other support.

a. Facilities. What facilities support will be provided to members of the DND media pool and other media?

b. Inoculations. What inoculations will be required for correspondents accompanying troops in the field or embarked on ships of the task forces?

c. Expenses

(1) What services will be provided to the media on a reimbursable basis?

(2) What are the requirements for reimbursement?

d. Simulated Rank. What will be the simulated rank of news media representatives for messing, billeting, and transportation?

e. Communications. What will be the procedures for handling media traffic?

f. Transportation. What are the procedures for transporting media personnel into, out of, and within the AO?

g. Travel Orders. What are the procedures for authorizing and issuing travel orders to correspondents.

h. Pools. What are the detailed procedures for media participation in media pools?

7. Security of Operations and Personnel

a. Operations. What are the guidelines to follow when correspondents are present in the operating areas? Include a balance between security and providing information to the public. Diplomatic and political considerations of all statements and news releases to media representatives should be weighed carefully at all echelons of command.

b. Personnel

(1) Personal Security. What personal security measures apply to correspondents in the operating areas?

(2) Physical Security. What physical security measures apply to correspondents in the operating areas?

8. Operations Security. What detailed security procedures, if any, are to be followed by PA personnel?

9. Audiovisual and Visual Information. What are the guidelines that apply to providing PA, audiovisual, and visual information coverage of the operation?

10. Internal Information. What are the internal information requirements for subordinate commands?

11. Community Relations. What, if any, coordination is required with DGPA or designated representative?

IO (CIVIL MILITARY COOPERATION / CIVIL AFFAIRS) GUIDANCE

The guidance in this annex relates to the development of the Civil Affairs or CIMIC portion of any and all plans developed for use by the CF.

1. Situation

a. General

(1) What is the legal basis for CIMIC/CA activities in this operation?

(2) What is the expected scope of CIMIC/CA activities in this operation? Include the identification of pertinent international and civil-military agreements.

(3) What is the purpose of this Appendix? Normally, the purpose is to provide instructions for guiding all relationships between the military force and civil authorities and inhabitants in the AO.

b. Enemy

(1) What is the impact of enemy capabilities and probable COAs on the CIMIC/CA situation? Include particular emphasis on identifying requirements for CIMIC/CA functions and activities.

(2) What is the expected CIMIC/CA situation? Include government institutions, customs and attitudes of the population, and availability of indigenous resources.

c. Friendly

(1) What are the CIMIC/CA functions to be performed by civilian authorities of Canada and friendly governments in the operational area?

(2) What local indigenous assets are available to support and assist in CIMIC/CA activities?

d. Assumptions. What are the basic assumptions on which CIMIC/CA planning is based? Include attention to enemy COAs, availability of indigenous resources, conclusion of necessary agreements with foreign governments on forces.

2. Mission. What is the mission to be accomplished by CIMIC/CA activities in support of the operations envisaged in the basic plan?

3. Execution

a. Concept of Operations

(1) Operations not involving the establishment of a military government

(a) What are the operational variations due to alternate COAs in the basic plan?

(b) What will be CIMIC/CA support of diplomatic, economic or other efforts underway?

(c) Do CIMIC/CA activities support time-phasing of the operation?

(d) What will be the deployment and employment of forces to support CIMIC/CA operations?

(e) What will be the scope and duration of CIMIC/CA operations? Include post-conflict CIMIC/CA operations.

(f) What are the desired end states in CIMIC/CA activities? These should be clear, concise, and subdivided as necessary to describe the successful completion of each phase and COA.

(g) What is the planned allocation and use of military units and resources for the performance of CIMIC/CA functions?

(h) What are the principal CIMIC/CA functions to be performed within the command area? Include any significant variations by country, state, or region.

(i) What will be the function and operation of civil-military operations centres, if they are established?

(2) Operations involving the establishment of a military government

(a) What is the constructive or restrictive guidance on each CIMIC/CA functional area?

(b) What CIMIC/CA authorities are required?

(c) What additional CIMIC/CA coordination is required?

b. Tasks. What are the specific tasks assigned to each element of the TFC and supporting commands? Each task should be a concise statement of a mission to be performed either in future planning for the operation or on execution of the OPORD and must include all key elements required for CIMIC/CA functions.

c. Coordinating Instructions

(1) What are the instructions applicable to the whole command; two or more elements of the command; and the command or its elements and agencies external to the command?

(2) What, if any, are the established CIMIC/CA boundaries?

(3) What, if any, are the liaison arrangements with allied/coalition forces and between subordinate commands?

(4) What are the claims policies? See also legal annex.

(5) What is the application or negotiation of status-of-forces agreements? See also legal annex.

(6) What is the required liaison and coordination with Canadian Government and non-government agencies? See also legal annex.

(7) What proclamations are to be issued to the civil populace in coordination with the legal annex?

(8) What is the required liaison and coordination with host country or other friendly countries and government and non-government agencies?

(9) What are the emergency measures, if any, for defense of civil populations?

(10) What will be the PSYOP support to CIMIC/CA operations?

4. Administration and Logistics

a. Military Resource Requirements. What, if any, are the applicable requirements to maintain military equipment and supplies for support of the CIMIC/CA function?

b. Civilian Personnel. What is the estimated local civilian labor required and available to support the operation?

d. Civilian Facilities and Supplies. What are the estimated local civilian facilities and supplies required and available to support the operation?

e. Reports. What, if any, are the administrative reporting requirements?

5. Command and Control

a. What, if any, are the differences between the command channels for the conduct of CIMIC/CA activities and the command relationships established.

b. Who has command responsibility for operational control, administrative control, and logistics of CIMIC/CA forces and activities? Emphasize difference between activities and forces and include any changes or transitions between C2 organizations and the time of the expected shift.

c. What, if any, command arrangement agreements and memorandums of understanding are being used. Which of these, if any, require

ANNEX B

DEFENSIVE INFORMATION OPERATIONS GUIDANCE

The guidance in this Annex relates to the development of the Defensive Information Operations portions of any and all plans developed for use by the CF.

1. Situation

a. General

(1) What are the defensive IO objectives?

(2) How do these objectives relate to mission accomplishment?

b. Enemy. What are the enemy capabilities that affect friendly information, and information systems, and IO not already discussed?

c. Friendly. What are the organizations that are not subordinate to this command and the specific tasks assigned to each supporting defensive IO objective?

2. Mission. How do defensive IO support the accomplishment of the mission assigned in the basic plan?

3. Execution

a. Concept of Operations

(1) General. What is the overall concept for ensuring friendly information access and availability despite enemy IO use? Pay particular attention to physical security and survivability of friendly information system capabilities and facilities.

(2) Phasing

(a) What are the defensive IO activities occurring in each operational phase? Describe activity sequences in each phase keyed to phase initiation and supported operational events.

(b) What is the time-phased guidance for accomplishing actions implementing the defensive IO plan?

b. Tasks

(1) What command element is responsible for coordinating defensive IO actions?

(2) What are the assigned tasks and responsibilities of each subordinate command to implement and accomplish defensive IO actions, to include identification of vulnerabilities?

c. Coordinating Instructions

(1) Integration

(a) What are the detailed instructions for accomplishing integration of physical security and survivability measures, electronic protection measures, INFOSEC, CI, PA, counter-PSYOP, counter-deception, and OPSEC means of performing defensive IO?

(b) What is the guidance for mitigation and/or negation of adversary IO capabilities?

(3) Coordination. What are the detailed requirements for coordinating among elements involved in defensive IO? Emphasize close coordination with IO, C2W, deception, OPSEC, EW, PSYOP, intelligence, and other key planners that rely on friendly information resources.

(4) Security. What, if any, are the special security or handling requirements for defensive IO planning and actions envisaged by this Annex?

(5) Reports. What, if any, are the operational reporting requirements necessary for effective monitoring of defensive IO activities?

4. Administration and Logistics

a. Personnel. What, if any, are the requirements for specialized personnel qualifications and/or qualification?

b. Supply. What, if any, are the specialized equipment supply requirements?

c. Reports. What, if any, are the required administrative reports?

5. Command and Control. What special systems or procedures, if any, are required for C2 of defensive IO actions?

LIST OF ABBREVIATIONS

AO	area of operations
BDA	battle damage assessment
C2	command and control
C2W	command and control warfare
C3	command, control, and communications
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
CA	civil affairs
CERT	computer emergency response team
CFEWC	Canadian Forces Electronic Warfare Centre
CFIOG	Canadian Forces Information Operations Group
CI	counterintelligence
CIMIC	Civil Military Cooperation
CISO	counterintelligence support officer
COA	course of action
COMPUSEC	computer security
COMSEC	communications security
CONPLAN	operation plan in concept format
CSE	Communications Security Establishment
DII	Defence Information Infrastructure
DECSS	Defence Electronics & Communications & Spectrum Services
EEFI	essential elements of friendly information
ECM	electronic countermeasures
ESM	electronic warfare support measures
EPM	electronic protect measures
EPW	enemy prisoner of war
EW	electronic warfare
EWCC	electronic warfare coordination cell
GII	global information infrastructure
HUMINT	human intelligence
I&W	indications and warning
IADS	integrated air defence system
I-BDA	information battle damage assessment
IIE	integrated information environment
INFOSEC	information security
IO	information operations
IOCC	information operations coordination cell
IP	information protect
IPB	intelligence preparation of the battlespace
IS	information system
ISIRT	information system incident response team
JCCC	joint communications control center
JCMA	joint COMSEC monitoring activity
JIB	Joint Information Bureau
JOC	joint operations center

JPT	joint planning team
JRFL	joint restricted frequency list
JSAT	joint staff action team
M&S	modeling and simulation
NBC	nuclear, biological, chemical
NCCIS	national command & control information system
NII	National Information Infrastructure
OGD	other government departments
OOTW	operations other than war
OPFOR	opposition force
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PA	public affairs
PSYOP	psychological operations
SATCOM	satellite communications
SIO	special information operations
STO	special technical operations
TCC	targeting coordination cell
TFC	task force commander