DRAFT

AUSTRALIAN DEFENCE FORCE PUBLICATION

INFORMATION OPERATIONS PLANNING MANNUAL

CONTENTS

CHAPTER 1

OVERVIEW - INFORMATION OPERATIONS

BACKGROUND

Introduction

1.1 Information underpins all operational and management functions, and capabilities within the defence organisations. It is a fundamental resource critical in commander's decision-making processes. Increasingly military decision-making is becoming dependent on information systems (IS) [1] for moving, sorting, manipulating and exploiting available information. With the spread of communication systems, information is also attaining a national and global dimension. Exploitation of this dependence on information as a critical component of commander's decision-making processes is achieved through a concept called 'Information Operations' (IO).

1.2 IO, like other forms of military operations, are activities that are planned and executed, can be conducted in phases, can involve direct and indirect approaches, require resources, utilise capabilities to greater or lesser degrees depending upon the particular operation, and require doctrine and training. IO would normally be used in concert with combat operations and military support operations, but can also stand-alone.

A national threat

1.3 IO presents particular challenges to the military due to the wider range of potential protagonists that can be involved. The low entry costs associated with the conduct of basic IO multiplies the threat and offers a range of non state-actors new avenues to conduct business. Such actors include Issue Motivated Groups (IMGs), Non Government Organisations and disgruntled individuals. Additionally, the lack of strategic intelligence against some of these potential actors and reduced warning time of likely activities complicates the defensive task.

1.4 Therefore, offensive IO activity against Australia must be seen as a significant national threat. Such activity involves shaping national perceptions through manipulation of information, disrupting daily activities of national life through interference with national information infrastructure, as well as attacking a nation's capacity to wage war.

1.5 IO threats are not easily discernible or characterised. Intelligence therefore is critical in determining intent and capability, and for the successful exploitation of the IO concept. Detailed intelligence on decision-makers and their supporting decision-making processes, for a wide range of adversaries, must be provided. The global nature of the information age makes this a challenging task.

UNDERSTANDING IO

Definition

IO are defined as:

'Actions taken to defend and enhance ones own information, information processes and information systems and to affect adversary information, information processes and information systems.'

1.6 IO brings together a wide range of related activities focussed on or related to information. There is by no means a broad consensus, either within the Australian Defence Organisation (ADO) or external to it, as to what exactly constitutes IO. Consequently, IO may be portrayed as a range of interrelationships at all levels. Figure 1 represents this from a Defence centric perspective at the national level, depicting IO as the overlap of military operations, IS, relevant friendly information on those systems, and intelligence. Additionally, it shows the diverse range of interrelationships that affect IO.

---

[1] IS Definition.

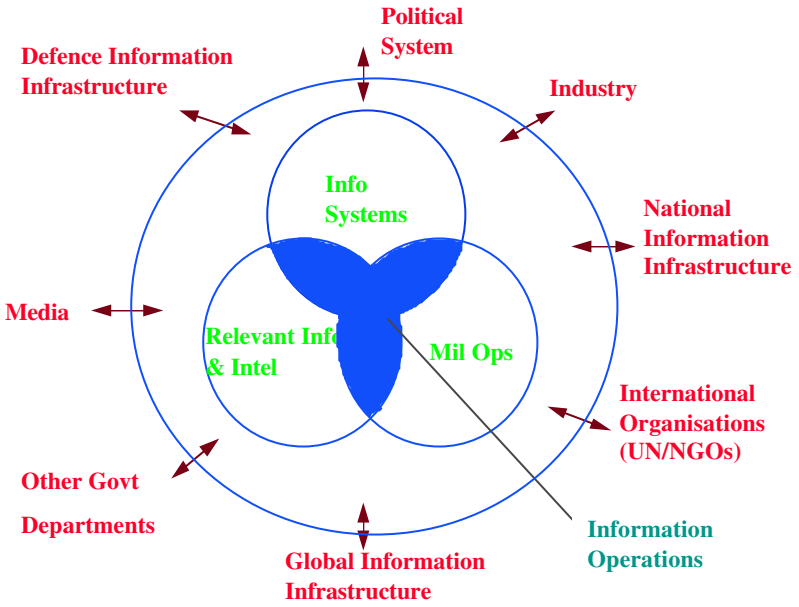


Figure 1.1 - IO Within A National Construct

The IO focus

1.7 The time taken to make decisions is being compressed, with an ever-increasing challenge or drive to remain ahead of an adversary's decision-making processes. Commander's use of and dependence upon information is not new. What is new, however, is the concept that information can be more easily managed, distributed and manipulated through modern technology, and perhaps even be considered a weapon in its own right. The aim is to speed up our own ability to observe, orient, decide and act, while slowing down, disrupting or destroying the adversary's ability to carry out a similar process (Figure 2). Further, modern information related tools are enabling the commander to increase tempo and improve decision cycles such that they can exploit the psychological dimension of the battlespace.

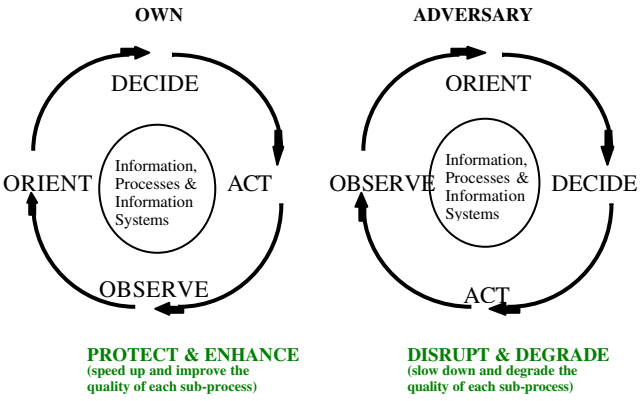


Figure 2 - The Effect of IO on the Decision Cycle

Components of IO

1.8 As an enabler to achieving an outcome of decision superiority, IO can be considered to have three components:

a. **Offensive IO**. Offensive IO are actions, synergised with wider activities and plans, designed to exploit or attack information, information processes and information systems in order to undermine decision-making processes. Offensive IO include the use of such capabilities as electronic warfare (EW), psychological operations (PSYOPS), deception, computer network attack (CNA), destruction and other conventional military capabilities

as appropriate. Non military capabilities may also be applied to achieving military objectives.

b. **Defensive IO**. Defensive IO are processes, synergised with wider activities and plans, designed to ensure friendly information, information processes and information systems are protected from malicious activity, an adversary's use of offensive IO, or from accidental and naturally occurring acts. ADO decision-making processes must be robust enough to ensure the successful achievement of designated objectives. Defensive IO include the use of such capabilities as information assurance (IA), counterintelligence, physical security, operations security, electronic warfare, counter psychological operations and other conventional military capabilities as appropriate. Non military capabilities may also be applied to support military defensive activities.

c. **IO support**. Support IO are activities and processes common to both offensive and defensive IO, or are not exclusively assignable to either. They specifically enable and enhance the effectiveness and efficiency of offensive and defensive IO. IO support activities are fundamental to the ability to conduct both offensive and defensive IO efficiently. IO support includes intelligence, public information, civil affairs, the management and command and control of IO, information and knowledge management, risk and vulnerability analysis support, network mapping support, and IO training support. IO support activities and processes can be generally divided into infrastructure and intelligence support as follows:

(1) **Infrastructure support.** Just as other military operations employ a range of capabilities, such as ships, aircraft and ground forces, IO require certain capabilities to be in place if commanders are to be able to plan and initiate action. These collective capabilities can be referred to as the **IO infrastructure**. It includes organisations, hardware and software, policies and doctrine, and trained people. Furthermore, IO employ a range of less tangible information capabilities such as public information, PSYOPS and deception to influence decision-making. At the highest level of the IO infrastructure are those **IO processes** that enable commanders to employ the IO infrastructure in flexible ways to achieve objectives.

(2) **Intelligence.** Similarly, intelligence activities provide a critical support function to the conduct and planning of IO. The nature of operating in the information age is such that the intelligence must be timely, readily accessible, accurate and sufficiently detailed to support an array of IO concept requirements, regardless of the level at which IO are conducted.

IO PRINCIPLES

General

1.9 The principles for the conduct of IO are:

a. people, decision-making processes and information systems are susceptible to IO;

b. IO must be conducted within a national framework designed for IO;

c. IO are an integral part of national military strategy;

d. IO must be centrally directed at the highest level and co-ordinated in execution;

e. IO may be conducted alone or in conjunction with other military operations;

f. a comprehensive understanding of the environment in which IO are to be conducted is critical to the successful planning and conduct of IO; and

g. moral, ethical and legal considerations will influence the conduct of IO.

Susceptibility to IO

1.10 IO offers a suite of activities, both offensive and defensive, relating to the use and manipulation of information across the conflict continuum. It involves activities ranging from technological to psychological, united by a common objective. The psychological element includes aspects such as PSYOPS, deception and other methods of shaping perceptions, while the technological element involves the manipulation of electronic information.

1.11 People, decision-making processes and information systems are susceptible to IO. The ADF must therefore be prepared to conduct IO across the psychological and technological domains.

National framework for IO

1.12 IO is a national issue requiring a coordinated approach. Although the lines of distinction are blurred in places, IO has a civilian and a military dimension. Therefore, a combination of military and civilian capabilities may be required for the execution of IO.

IO as a part of national military strategy

1.13 The globalisation of information and IS, have eroded traditional state boundaries. A determined and knowledgeable adversary is able to strike at national information infrastructure such as strategic military command and control nodes, electricity grids, air traffic control systems and communications infrastructure, without recourse to the application of conventional force. This approach would undermine the effective functioning of government, as degradation of this infrastructure could have significant ramifications for a range of vital national and commercial activities.

1.14 Early identification of critical elements with respect to IO targets will be essential to enable successful offensive and defensive IO. The geo-strategic advantages enjoyed by some nations have been reduced in the Information Age. The method of delivery of some information attacks, creates an advantage of distance only for the attacker, who remains harder to detect and take action against.

1.15 IO provides a potential adversary greater flexibility in gaining leverage by attacking a nation's interests both onshore and offshore. The ability to attack economic assets, companies, diplomatic missions and nationals in a less threatening way than conventional force, makes a clear policy response by the targeted nation more complex.

Direction and coordination

1.16 IO must be centrally directed at the highest level to ensure integration of available capabilities, some of which may be resident in a number of programs within the ADO. In addition, agencies from outside of the ADO may also be required to support military IO activities. To ensure that there is economy of effort, IO must be coordinated in a coherent manner with clearly defined division of responsibility between programs.

IO and conventional operations

1.17 Information has always been a dimension of war. In the Information Age, however, it has the potential to become a major theatre of conflict, much like air, land and sea, and it has the potential to be a weapon in its own right. Aspects of IO offer the potential to minimise, and in certain circumstances may eliminate, the need for conventional military force. IO can make an important contribution to defusing crises. It can reduce periods of confrontation and enhance the impact of informational, diplomatic, economic, and military efforts. IO can forestall or eliminate the need to employ forces in a combat situation.

Understanding the environment

1.18 A comprehensive understanding of the environment is critical to the successful planning and conduct of IO, regardless of the level. It is vital therefore, that the ADF is supported by a comprehensive system involving information collection, processing and dissemination capability which supports the planning and conduct of IO. Such capability builds situational awareness in terms of knowledge on the adversary, the environment and friendly factors that impact on the conduct of IO.

Moral, ethical and legal considerations

1.19 Understanding the legal and ethical issues involved in the conduct of IO will be essential for commanders at all levels. As a general proposition, conventional attacks against IS, such as the destruction of an adversary's military computer centre, can be dealt with using traditional principles of the Law of Armed Conflict (LOAC), including military necessity, proportionality and collateral damage. On the other hand, the phenomenon of information attacks using non-traditional information weapons or techniques does not fit easily within the LOAC framework. The danger is that while some states or individuals will be restrained by moral, ethical or legal considerations, others will not. This reinforces the need to concentrate on establishing a strong defensive regime. The ADF must be prepared to conduct IO within an ambiguous legal framework.

RESPONSIBILITIES

1.20 The current policy responsibilities for IO related activities are spread throughout the following organisations;

ADHQ.

- responsible for strategic level information concepts and strategies,
- responsible for the provision of strategic policy, plans and priorities to guide the development of IO, and
- responsible for the achievement of national strategic requirements for military IO.

DEPSEC Corporate. Responsible for overall effectiveness and efficiency of Defence information management.

Defence Information Environment Board (DIEB). Directs the development of the Defence Information Environment (DIE).

Defence Information Systems Group. Responsible for managing Defence communication and information systems, including the protection of those systems and the information contained within these systems.

Defence Signals Directorate (DSD). Responsible for SIGINT support to IO.

Defence Security Branch (DSB). Responsible for Defence IA policy and standards, Defence physical security policy, and security intelligence support to IO activities.

Defence Intelligence Organisation (DIO). Responsible for provision of intelligence support to threat assessment processes.

Defence Acquisition Organisation (DAO). Responsible to manage the acquisition and introduction into service of command support, communications and electronic warfare, radar and related systems.

Defence Science and Technology Organisation (DSTO). Responsible to provide scientific and technical advice, and assistance on IO matters.

Commander Australian Theatre (COMAST). Responsible for the policy and procedures for the implementation of IO in the Australian Theatre.

IO CONCEPTS: PLANNING AND ACTIVITY

There are two ways to view IO. First, as a conceptual framework within operations planning which induces a staff effort focussed on influencing decision cycles. Second,

is those operations or activities undertaken to meet the objectives arising from this staff effort.[2]

IO - A concept in planning

1.21 IO is considered to be a conceptual approach to military planning and operations, including their support functions, rather than a new area of military specialisation. IO at the operational and tactical levels is the responsibility of operations staff assisted by other functional groups. Planning staff will also need to consider IO as part of future operations. Preferably, a dedicated staff meets the IO responsibility within a headquarters. Where otherwise constrained, this responsibility may also be met by command direction, an awareness of IO, or the establishment of an IO group or board. The manner by which the IO planning function is met must be appropriate to the headquarters and ensure that IO are considered and integrated with the plan.

1.22 **IO objective**. The objective of IO within the ADF is to contribute to the achievement of military objectives by promoting and protecting ADF decision-making, and exploiting and influencing adversary decision-making.

1.23 **IO focus**. Through IO, the ADF seeks to enable decision superiority and promote freedom of action for ADF decision-making processes, while hindering the efforts of adversaries. IO seeks to exploit the opportunities and vulnerabilities inherent in the decision making process and information-dependent systems. This includes people, infrastructure, weapons, command and control, computers and associated network systems. IO seeks to impair or distort the decision-making abilities of an adversary's leadership structure, and to influence the belief or perceptions of a nation's people. The focus is therefore on the psychology of perception and leadership, and the ability of the commanders and managers to provide effective leadership and management.

1.24 **A coordinated and integrated strategy**. ADF IO policies and plans are to be integrated within the overall military strategies and objectives to achieve a coherent effect. IO requires the close coordination of both offensive and defensive capabilities and activities, as well as effective design, integration and interaction of command and control, with intelligence and other support mechanisms.

1.25 **Conduct of IO - levels of command**. IO, like other forms of military operations, are activities that are planned and executed, can be conducted in phases, can involve direct and indirect approaches, require resources, utilise capabilities to greater or lesser degrees depending upon the particular operation, and require doctrine and training. IO may be conducted at all levels and throughout the continuum of conflict. Figures 3 and 4 describe this relationship.

[2] This includes the approach to military operations taken to disrupt or inhibit an adversary's ability to command and control his forces while protecting and enhancing our own. In the past, this has been referred to as Command and Control Warfare (C2W).

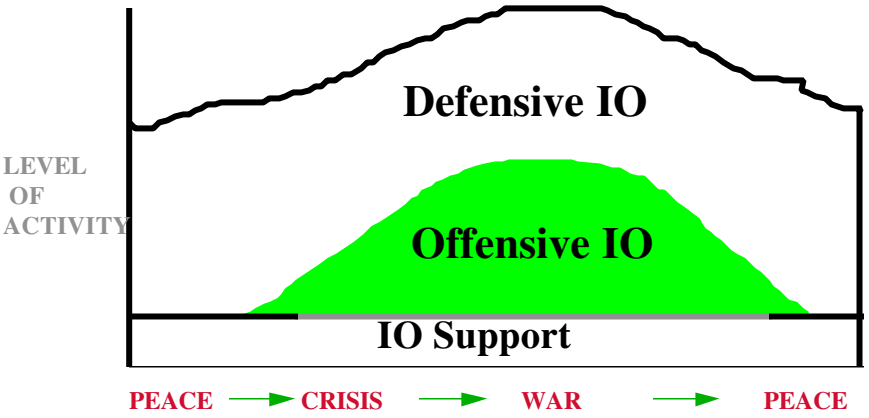


Figure 3 - IO Continuum

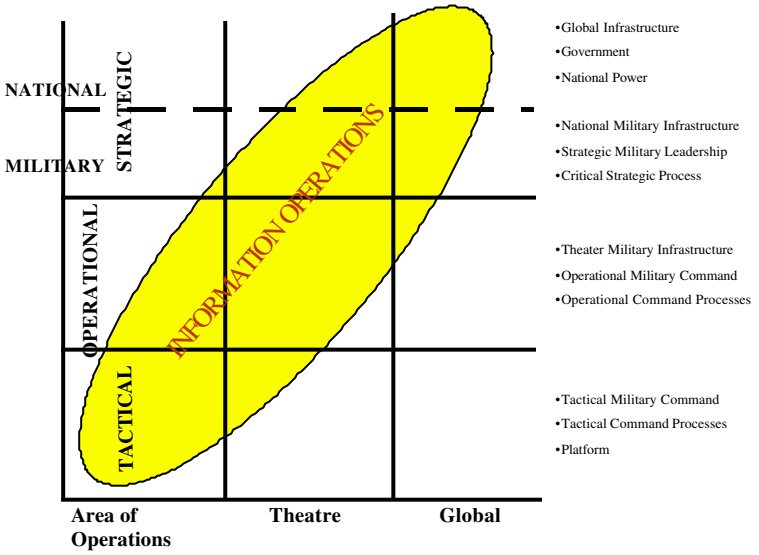


Figure 4 - IO at the Levels of Command

1.26 **IO at the national strategic level.** IO at the strategic level will be directed by Government to achieve national objectives by influencing or affecting elements of an adversary's national power (political, economic, military or societal). The ultimate strategic objective for IO is to affect strategic decision-makers to the degree that any adversary will cease actions that threaten Australian interests.

1.27 **IO at the military strategic level.** For ADF purposes, IO at the military strategic level are conducted in support of national IO objectives. The focus will be on the information related aspects of strategic military leadership, lines of communications, command and control processes, logistics and other critical strategic level processes designed to sustain military capability.

1.28 **IO at the operational level.** IO may be conducted at the operational level to support military objectives within a particular theatre of operations and would normally be carried out with theatre resources. The focus at this level will be on the information related aspects of lines of communications within the theatre, logistics, leadership, will to prosecute operations, command and control processes and infrastructure, and information sources.

1.29 **IO at the tactical level.** IO at the tactical level will be conducted to achieve specific manoeuvre objectives. Activity will only be conducted under theatre guidance. The focus in this instance will be on information related to tactical leadership, command and control processes directly related to the conduct of specific military operations, and military information processing equipment.

IO as an activity

1.30 IO is conducted through the integration of many activities. These are often delineated by the offensive or defensive outcomes required. The activities that support the components of IO are listed

below. While activities are shown as an element of Offence, Defence or Support, this does not necessarily mean they remain wholly within IO. The majority of these elements exist in their own right and contribute to other military operations and business processes in much the same way as they do to IO. IO seek to harmonise the activities to achieve the greatest offensive and defensive contribution to a commander's objectives.

1.31 **Offensive IO.** The activities which support offensive IO are:

a. **Electronic attack.** Electronic attack (EA) is that component of electronic warfare (EW) that uses electromagnetic or directed energy to attack personnel, facilities or equipment with the intent of degrading, neutralising or destroying adversary combat capability. It is addressed further in ADFP 24 – *Electronic Warfare* and includes the following:

(1) Actions taken to prevent or reduce the adversary's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception where:

(2) electronic jamming is deliberate radiation, re-radiation or reflection of electromagnetic energy used with the object of impairing the effectiveness of electronic devices, equipment or systems being used by an adversary; and

(3) electronic deception is deliberate radiation, alteration, re-radiation, absorption or reflection of electromagnetic energy in a manner intended to confuse, distract or seduce an enemy or that adversary's electronic systems.

(4) Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism such as lasers, radio frequency weapons and particle beams. Electronic neutralisation is the deliberate use of electromagnetic energy to damage, either temporarily or permanently, adversary devices that rely exclusively on the electromagnetic spectrum.

b. **Psychological operations**. Psychological operations (PSYOPS) are are planned activities in peace and war directed to adversary, friendly and neutral audiences in order to influence attitudes and behaviour affecting the achievement of political and military objectives. The objective of ADF psychological operations is to cause adversary, friendly and neutral personnel to act favourably toward Australia and its allies. PSYOPS is described in detail in ADFP 25 – *Psychological Operations* and the categories of PSYOPS are:

(1) **Psychological action**. The planned use of support activities to reduce an adversary's prestige and influence, and to increase friendly influence and attitudes in potentially hostile or neutral countries.

(2) **Psychological consolidation**. Those activities designed to foster the establishment or maintenance of order and security, and gaining the support of a local population in order to advance political and military objectives.

(3) **Psychological warfare**. Efforts designed to bring psychological pressure to bear on an enemy and to influence attitudes and behaviour of hostile groups and target audiences in areas under enemy control.

c. **Deception**. (See Chapter 7). Deception includes those measures designed to mislead the adversary or target by manipulation, distortion, or falsification of evidence to induce the target to react in a manner prejudicial to his interests and to the benefit of friendly interests. Thus deception seeks to influence the mind of the adversary commander and the requirement for deception is derived from a desire for security or a need to achieve surprise.

(1) **Security**. Security is a function of command and includes all those measures taken by a command to protect itself from espionage, observation, sabotage,

annoyance and surprise. Security denies information to an adversary and retains for the commander the ability to employ his forces more effectively. Deception may be required to assist in the protection of capability and intent from an adversary's collection system.

(2) **Surprise**. The ultimate objective of deception is the achievement of surprise. It is not essential that an adversary be taken unaware, but only that he becomes aware too late to react effectively. If a commander is to achieve surprise, he must plan to fulfil two requirements: *conceal* the true (security) and *reveal* the false (deception).

d. **Destruction**. Destruction (or physical destruction) refers to the process and activity involved in the development and selection of target sets for degradation, neutralisation or destruction through physical attack by overt, covert, or clandestine military force. Such attacks are conducted in accordance with commander's guidance and planning objectives.

e. **Computer network attack**. Computer network attack (CNA) involves the deliberate attack on adversary computer information systems (CIS) through the medium of that system's own components. These components may include inputs, outputs, software, hardware, links, connections, or personnel. CNA is thus related to but can act distinctly from EA. Such attacks occur in a variety of forms including:

(1) **Hacking**. Hacking involves the illegal entry of system, usually for one of two reasons:

(a) malicious destruction or degradation of key nodes, or

(b) curiousity.

(2) **Chipping.** Chipping is malicious hardware attack, usually conducted through the deliberate insertion of hardware that is designed to fail on initiated sequence or at a selected time.

(3) **Insider**. Insiders add a personnel risk to CIS security. They may be transient or permanent. They may be malicious or sources of information.

1.32 **Defensive IO.** The activities which support defensive IO are:

a. **Electronic protection**. Electronic protection (EP) involves action taken to protect personnel, facilities or equipment from the effects of friendly or adversary employment of EA. EP can be either technical or procedural. Technical EP is applied at the equipment/system level and is based on technology. Procedural EP is concerned with the manner in which EW is conducted and includes techniques such as information security (INFOSEC) and emission control (EMCON). Information security includes computer security (COMPUSEC) and electromagnetic security (EMSEC). EMSEC is further divided into communications security (COMSEC) and electronic security (ELSEC). EMCON procedures are implemented to protect essential elements of friendly information (EEFI). Further details are available in ADFP 24 - *Electronic Warfare*.

b. **Counter PSYOPS**. Counter PSYOPS seeks to counter adversary propaganda. Defensive counterpropaganda shield audiences or lessens the impact of messages, while offensive counterpropaganda takes advantage of adversary propagandist mistakes. Counter PSYOPS techniques include forestalling, direct refutation, indirect refutation, diversion, silence, immunisation, minimisation, imitative deception and ridicule. Counter PSYOPS is driven by analysis of propaganda based on:

(1) **Source**.

(a) **Black propaganda**. That which purports to originate from a source other than the true one.

(b) **Grey propaganda**. That which does not specifically identify any source.

(c) **White propaganda**. Disseminated and acknowledged by the sponsor or by an accredited agency.

(2) **Content**. The type and quality of information contained.

(3) **Audience**. Analysed by the apparent audience, the intermediate audience, the unintended audience and the ultimate audience.

(4) **Media**. The medium used to propagate the information.

(5) **Effect**. The effect on the intended audience and the secondary effects on unintended or intermediate audiences.

c. **Counterintelligence**. Counterintelligence (CI) is that aspect of intelligence devoted to destroying the effectiveness of foreign intelligence activities, and protecting information, individuals, installations, equipment, records and materiel from espionage, sabotage, subversion and terrorism. CI has both a staff component and an operator (activity) component but unlike intelligence it is not normally referred to as the product of analysis. The term security intelligence is used to designate intelligence product from CI related agencies on threats to security. Intelligence seeks to support the planning and conduct of operations by providing the commander and staff knowledge and understanding of the threat and environment. Within this function, CI seeks to prevent the adversary's intelligence system from achieving the same objective and to stop potential and real adversaries undermining the security of friendly forces. CI is discussed further in ADFP 19 – *Intelligence*.

d. **OPSEC**. Operations Security (OPSEC) is the process which gives a military operation or exercise appropriate security, using passive or active means, to **deny knowledge** of the dispositions, capabilities and intentions of friendly forces. It is a command function that involves those collective measures taken by the operational force to maintain security from generally overt and clandestine intelligence collection. It is therefore controlled and coordinated by operations staff with input from CI and other staffs. OPSEC depends on an understanding of the adversary's ability to collect information, the way information is processed, and the decision-action cycle that results from it. OPSEC is covered in more detail in Chapter 6.

e. **Protective security**. Protective security is the organised system of defensive measures instituted and maintained at all levels of command with the aim of achieving and maintaining security. Protective security measures consist of controls, which form a series of interlocking defences in depth against the threat. The protective security measures imposed by the ADF are detailed in security orders and instructions. These are designed to protect information, material and personnel from the threat and comprise:

(1) **Physical security.** The system of physical controls through which access to information and material is restricted to authorised persons.

(2) **Personnel security.** The process of personnel investigation and categorisation designed to ensure that no person is allowed access to classified information or material if there are known objections to them from the point of view of integrity or loyalty.

f. **Information assurance**. Information assurance (IA) is the protection of information and information systems by ensuring their confidentiality, integrity, availability, authentication and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection and reaction capabilities.

1.33 **IO Support.** The activities which support IO are:

a. **Intelligence support**. Intelligence support to IO is detailed in ADFP 19 – *Intelligence*. It includes the electronic support (ES) component of EW.

b. **Public information**. Public information (PI) is information that is released or published for the primary purpose of keeping the public fully informed, thereby gaining their understanding and support. In time of tension and conflict, the maintenance of Australian domestic support and an understanding of ADF operations are of great importance to the maintenance of the national effort. Should the Australian public lose confidence in the ability of the ADF to bring a conflict to a successful conclusion, restraints may be placed on the government and the ADF. In a low level conflict the results of loss of public confidence could include an unwillingness on the part of the civilian population to continue to deny the adversary achieving its aims, withdrawal of active support to authorities and a perception by the international community of the political weakening of Australian resolve.

c. **Civil affairs**. Civil affairs (CA) describes the broad range of actions conducted to establish, maintain, influence, or exploit relations between the military, civil authorities and the civilian population in order to assist a military operation. They include the provision of support to the civil administration and civil - military operations.

d. **IO command and control, and management**. Supporting IO is the level of education in IO and IO planning, the command and control mechanisms available to assist in the synchronisation and deconfliction of IO activity, and the availability of tools to assist in the planning of IO.

e. **Information and knowledge management**. The efficiency of information management systems on a headquarters, plus the way in which knowledge is held and circulated, impacts directly on decision systems.

f. **Analysis support**. The availability and competency of integral and external specialist analytical support for the risk and vulnerability analysis associated with both offensive and defensive IO is paramount to successful IO. This requires mapping support tools to define networks, command and control structures, the Defence information infrastructure and the National information infrastructure.

CHAPTER 2

DEFENSIVE INFORMATION OPERATIONS

BACKGROUND

2.1 Defensive IO are processes, synergised with wider activities and plans, designed to ensure friendly information, information processes and information systems are protected from an adversary's use of offensive IO, or from accidental and naturally occurring acts. Defensive IO involves the integration and coordination of policies and procedures, operations, personnel, and technology. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Defensive IO include the use of such capabilities as information assurance (IA), counterintelligence (CI), physical security, operations security (OPSEC), electronic warfare (EW), counter psychological operations (PSYOPS) and other conventional military capabilities as appropriate. Non military capabilities may also be applied to support military defensive activities.

2.2 **A national threat**. IO presents particular challenges to the military due to the wider range of potential protagonists that can be involved. The low-entry costs to conduct basic IO multiplies the threat and offers a range of non-state actors, including Issue Motivated Groups (IMGs), Non-Government Organisations and disgruntled individuals, new avenues to conduct their business. Additionally, the lack of strategic intelligence against some of these potential actors and reduced warning time of likely activities complicates the defensive task.

DEFENSIVE IO PRINCIPLES

2.3 The following are the principles for defensive IO:

a. defensive IO measures must permit a command to continue to operate successfully while under attack from an adversary's use of offensive IO;

b. defensive IO involves measures and processes to counter the susceptibility of decision-making processes and information systems to offensive IO;

c. defensive IO must be undertaken continuously;

d. defensive IO, offensive IO and IO support are complementary activities;

e. defensive IO must be undertaken at all levels within Defence;

f. ADF defensive IO measures must be consistent with National defensive IO measures; and

g. defensive IO must be integrated with, support and enhance military operations.

THE DEFENSIVE IO PROCESS

General

2.4 Defensive IO are concerned with planning and coordinating strategies, tactics and actions to protect friendly data, information, information systems and associated processes, infrastructures and key decision makers from structured or unstructured attacks by adversaries, and to protect against naturally occurring acts. These attacks may be based on physical, electronic, logical[3] and psychological methods. Inherent in defensive IO concepts is the assumption that IA measures will protect against threats to information from incidental acts of maliciousness or accidents.

[3] Logical attack seeks to affect the processes governing information integrity, availability, confidentiality, authentication and repudiation through manipulation of software or electronically encoded data.

2.5 Defensive IO rely heavily on IA, CI, physical and personnel security, electronic protection (EP), deception, counter PSYOPS, and other appropriate conventional military capabilities as appropriate, being employed in a truly integrated manner. Non-military capabilities, which may reside in private industry or other Government departments, may also be applied to support military defensive activities. Defensive IO processes, and the capability mix employed, are driven by the circumstances.

Defensive IO and IA

2.6 IA is a key enabler for defensive IO. IA concerns itself with measures, standards and practices to protect data, information, information systems and associated processes and infrastructures from natural, accidental and deliberate attacks, and to maintain stated levels of confidentiality, integrity and availability. Integrity of the system includes concepts of authentication and non-repudiation. Protection of information aspect includes not only information, but information processes and information systems, and includes the ability to react and restore information flows in event of loss of assurance.

Defensive IO and the defence information environment

2.7 Defensive IO seeks to protect the defence information environment (DIE). For successful defensive IO, it is important that commanders have a clear understanding of the DIE's components, structures, relationships, processes and capabilities. The ADF must have a comprehensive understanding of the normal state of the DIE, know, when and why change is occurring within the DIE, and identify the cause.

2.8 Figure 1 illustrates the defensive IO process and shows its continuous nature. The process recognises:

a. The need in the first instance to deter attacks against the DIE and to establish a mechanism to protect the information environment should deterrence fail.

b. That there are vulnerabilities in, and threats to infrastructure, systems, processes and procedures. There is a need therefore, to apply risk assessment and risk management to provide appropriate defensive measures, based upon the impact on the operation or business function(s) at risk.

c. The need to develop measures and capabilities such as IA, physical and personnel security, deception, CI, counter PSYOPS, electronic protection (EP), and other conventional military capabilities to defend the information environment from deliberate, malicious, structured or unstructured attacks by adversaries, and natural and accidental acts.

d. The need to continuously review and improve these measures and capabilities.

e. The cycle of action – reaction within defensive IO.

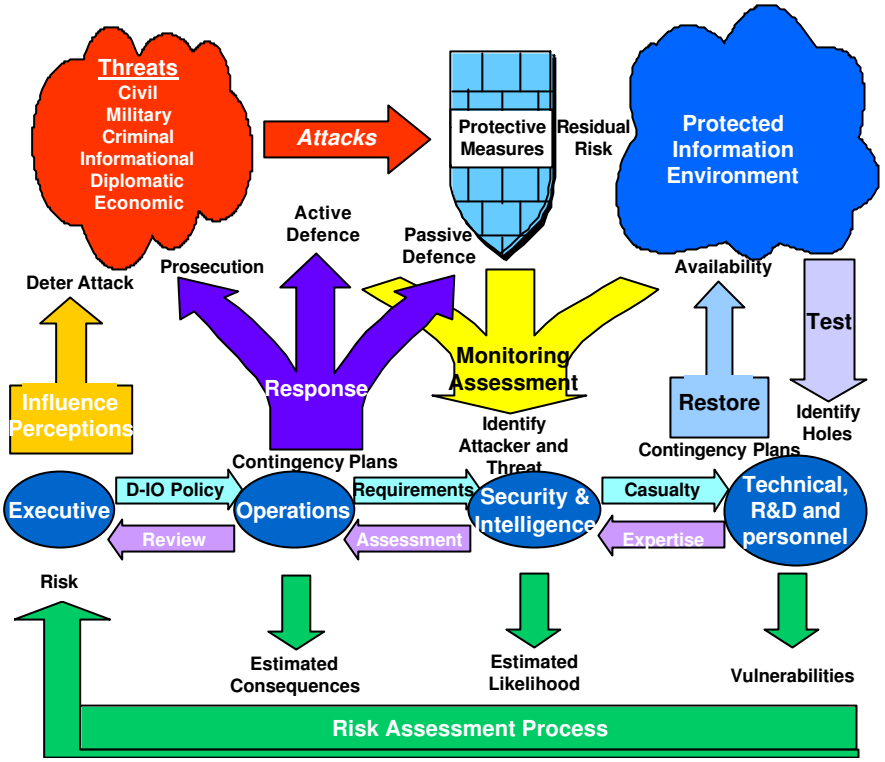
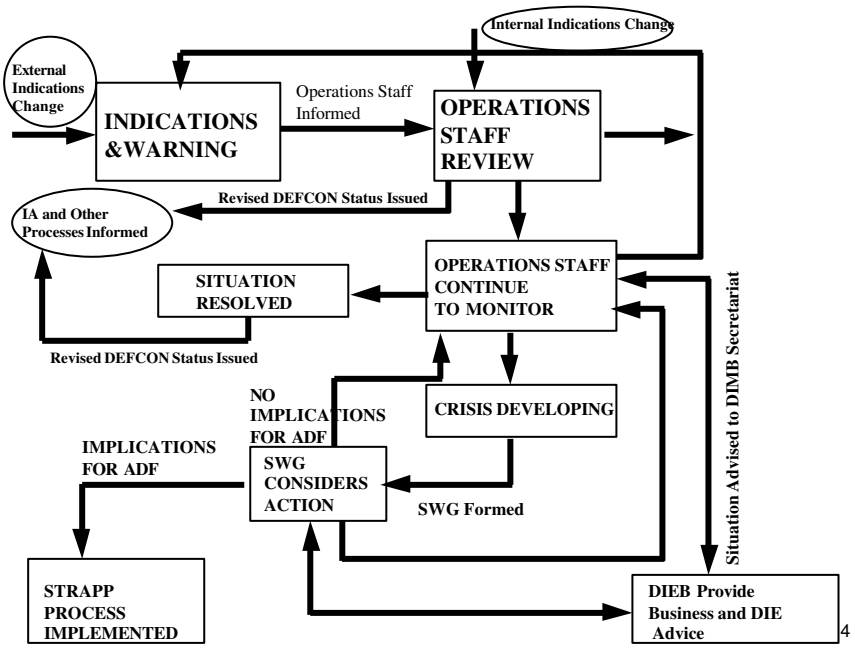


Figure 1. The Defensive IO Process

DEFENSIVE IO AS A STRATEGIC PROCESS

2.9 Defensive IO is integrated into existing Defence operational and business processes, ensuring that there is no conflict and duplication of effort. A flow diagram describing how defensive IO is integrated with the initial stages of the Strategic Planning Process (STRAPP) is shown in Figure 2.



[4]

[4] The DIEB will provide guidance and advice to the Strategic Watch Group (SWG) and operations staff on the implications for Defence business and the DII, in reaction to attacks against the DIE. This new operations support function will need to be reflected in the DIEB terms of reference and processes and procedures developed to accommodate the change.

Figure 2 - Defensive IO Process and The STRAPP

2.10 The defensive IO process relies on establishing a normal or 'steady' DIE state from which to operate. In this state, capabilities, defensive processes and procedures would be routine; implemented such that they are managed as a day-to-day activity. This normal state would be monitored for indications of significant change by appropriate management mechanisms and organisations responsible for information, security and intelligence functions. Reports and advice will be provided to operations staff personnel responsible for IO management within Strategic Command Division, for appropriate action.

2.11 Thresholds of triggers and known attack signatures are established to indicate when the attacks or disruptions might be such that they are likely to impact on Defence operations and business, and where additional measures and activities might have to be implemented. The STRAPP process is followed from this point.

Relations with other organisations

2.12 There are a number of organisations within Defence which have a responsibility for the protection of the DIE. The operations, communications and information systems, intelligence and security communities all contribute to defensive IO. Defence's defensive IO process will therefore seek to synergise all of their functions to ensure the most effective, sustainable and efficient yet affordable solutions are developed for defensive IO. As the defence information infrastructure (DII) is in part dependent upon the national information infrastructure (NII), there is a need to protect (at least) selected parts of the NII.

2.13 Elements of the NII that enable the DII are identified and as far as possible, monitored and protected. Defence's role in protecting these aspects of the NII must be determined, and in the absence of legal clarity, appropriate directives acquired from Executive Government. Likewise, both Defence and non-Defence, including Government (Federal and State) and civil/commercial information sources, on which Defence decision making and critical business processes rely, must be identified, monitored and protected. Executive Government will direct Defence's role in this process.

There are a number of agencies both within and external to Defence which have an influence on, or will be influenced by, the defensive IO relationships as shown in Figure 3.

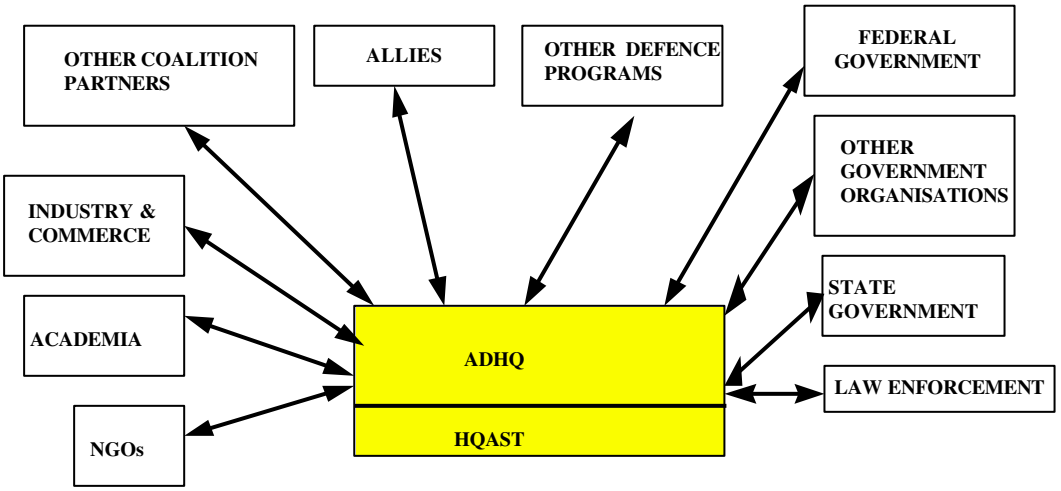


Figure 3 - Defensive IO Relationships

DEFENSIVE IO CONCEPTS

Defensive IO strategy

2.14 Managing the risk associated with defending against offensive IO attacks (including physical, electronic, psychological and logical attacks) is complex and demands increased central coordination. Further, it may not be possible to defend all information, information systems and information processes, and at the same time retain the functionality required to conduct operations. A commander must manage, rather than avoid risk, accepting that some capability loss will exist for realistic defences.

2.15 Information, information systems and information processes will be protected relative to the value of the information they contain and the risk and likely impact associated with their compromise or loss. Similarly, key decision-makers will be protected relative to their importance to the decision making process, and information infrastructure will be protected relative to its criticality. Hence, it will be necessary to identify each command's activities and processes which require protection, the key decision-makers within these processes, and the information, information flows, information systems, information processes and information infrastructure upon which they rely.

Defensive IO priority

2.16 The initiative is always with offensive IO due to the minimal entry costs available to potential attackers against distributed autonomous soft information targets. The anonymity afforded by the accessibility to, and ubiquity of, potential targets also gives the attacker a decided advantage. Offensive IO attacks, by their nature, can be implemented at 'electronic' scales and speeds and offer any potential attacker a high pay-off relative to the investment in the offensive capability.

2.17 People will always be a source of weakness in any security system. Therefore, defensive IO must address the long term yet enduring pervasiveness of global communications reaching into every household with the potential opportunity for adversaries to shape perceptions anonymously, and perhaps even subconsciously. The simplest of such threats can be manifest in the electronic and logical threat freely supported in the public domain and on the World Wide Web. Defensive IO processes and procedures must incorporate a methodology to account for this potentially open information environment.

2.18 IO attacks therefore, are not limited to times of rising tensions or conflict. Consequently, and unlike direct physical or conventional attacks, defensive IO must be conducted continuously in time and across all phases of the conflict spectrum, in peacetime, periods of rising tensions, war, post-conflict restoration and rebuilding.

Planning

2.19 **General**. Defensive IO cannot be segregated from operations planning. Defensive IO forms part of commander's intent, and is integrated into planning, execution and monitoring of all plans and operations. Operations plans require commander's direction on the priority of systems to protect, vital assets, key personnel, perception management strategies, priorities for intelligence and information requirements, and those essential elements of friendly information (EEFI) to be specifically protected from adversary collection.

2.20 **Perception management component**. Defensive IO, has its own objectives and can impact significantly on military outcomes, by protecting against adversary targeting and contributing to own targeting processes against the beliefs, cognitive and decision making processes of adversary leadership, decision makers, militaries and populations. The perception component of offensive IO targets fears, prejudices, superstitions, beliefs and cultural behaviour patterns. Therefore, the effectiveness of psychological components of defensive IO requires a knowledge of these beliefs, fears, and superstitions; as well as knowledge of the media (radio, television, press, leaflets, Internet etc) through which these ideas can be influenced.

Threats

2.21 **Know the threat**. IO threats are not easily discernible or characterised. Intelligence therefore is critical in determining intent and capability, and for the successful exploitation of the IO concept. Detailed intelligence on decision-makers and their supporting decision making processes, for

a wide range of adversaries, must be provided. Offensive IO attacks may be remotely initiated and effected at electronic speeds, and the resultant 'damage' is subtle. Defensive IO must anticipate and expect such attacks. Defensive IO processes and procedures must allow a commander to either retain the initiative and control or to restore the situation as soon as possible. Depending upon the circumstances, there may even be a need to conceal the degree of effectiveness of any adversary offensive IO activity.

2.22 **Clandestine threats**. The difficulty in establishing effective IO measures is that offensive IO is often concealed. Clandestine attacks (where the nature of the activity is concealed) exploit the intangibility of human decision-making and reasoning processes, and of supporting information and information processes. There will often be little physical damage or visible cues to initiate decisive action to defend or isolate systems, personnel or processes.

2.23 **Covert threats**. Many IO attacks will also be conducted covertly. Often, even if targeting becomes apparent, the sponsor and aim of the attack remains hidden. Damage, if detected, will appear attributable to accident, misjudgment, bad luck, a third party or other cause. Hence, efforts to damage, copy, tamper with, or alter information and information processes may not be placed in a wider context. Thus the extent of damage will not be known until too late when synchronised attacks occur with other overt and wider efforts.

Components of defensive IO plans

2.24 Defensive IO preparedness. Components of effective defensive IO preparedness are:

a. **Normalcy assessments**. A structure designed to establish a pattern of normalcy against which changes can be identified and analysed. This is factored into indications and warning (I&W) processes.

b. **Training and education**. Effective training and competence in the recognition of and differentiation between normal and abnormal behaviour and patterns of information systems, networks, and personnel. Training must include the ability to identify offensive IO 'windows of opportunity' including the establishment of, or connection to, new networks; migration to new operating systems and applications; special events and so on.

c. **Continual test procedure**. Measures enacted from the adversarial view, designed to determine vulnerability.

d. **Specialist investigative and response capability**. The often covert and clandestine nature of offensive IO requires specialist efforts, through appropriate post-attack forensics, to determine the extent of the damage, real cause and sponsor. This should be linked to a responsive repair, redundancy or exploitation capability.

e. **Research and development**. R&D into the detection of evolution in, and changes to, existing and developing offensive IO techniques and attack patterns to guide the timely development of appropriate defensive IO measures.

f. **Operations planning**. To be effective, defensive IO plans should include the following:

g. **Active measures** Corporate, command, unit and individual systems and process activity designed to deter, degrade, deny, exploit, or discover, offensive IO activity. Tactics, techniques and procedures employed in defensive IO should be protected, and mechanisms established which reduce the attacker's opportunity to accurately assess the effectiveness of his efforts.

h. **Measures of effectiveness**. Processes and exercises designed to test the effectiveness of active measures. These are mission specific aspects of the continual test procedure noted above.

i. **Rules and procedures** Guidelines, legal limitations, and procedures for the authorisation and use of special response defensive IO methods and techniques must also be established within operations plans. Use of defensive IO capabilities in normal circumstances could alert and forewarn adversaries who could develop counters to negate their effectiveness during conflict.

CHAPTER 3

OFFENSIVE INFORMATION OPERATIONS

BACKGROUND

3.1 Offensive IO are actions, synergised with wider activities and plans, designed to exploit or attack information and information systems in order to undermine decision making processes. They are conducted to exploit or attack an adversary's decision-making processes to prevent adversary commanders from making accurate and timely decisions. Offensive IO involves the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision-makers and achieve or promote specific objectives. Offensive IO include the use of such capabilities as electronic warfare (EW), psychological warfare (PSYOPS), deception, computer network attack (CNA), destruction and other conventional military capabilities as appropriate.

IO support

3.2 Fundamental to being able to conduct offensive IO is IO support. These include but are not restricted to: intelligence (including signals intelligence and its electronic support component), public information (PI), psychological action, information management, situational awareness, and command, control, communications and intelligence systems infrastructure. Personnel must also receive training and be competent in planning offensive IO and in recognising offensive IO opportunities.

IO and the indirect approach

3.3 IO, like other forms of military operations, are activities that are planned and executed, can be conducted in phases, can involve direct and indirect approaches, require resources, utilise capabilities to greater or lesser degrees depending upon the particular operation, and require doctrine and training.

MEANS AVAILABLE FOR OFFENSIVE IO

General

3.4 A weapon can be described as an instrument that has a desired effect on a target. This required effect may be physical or intangible, and the weapons which achieve it may be lethal or non-lethal, including:

a. delivered munitions;

b. special purpose weapons, such as immobilising agents;

c. electromagnetic impulses;

d. propaganda;

e. deceptive information and

f. disabling technologies, for example computer viruses.

3.5 **Combinations**. Offensive IO will seek to use any weapon or combination of weapons. The key component is the effect desired. Determination of the means is then related to the nature of the target, the level of the effect desired, and the time for the effect to occur. For example, to achieve a psychological effect the same 'message' may be sent by leaflet, radio emission, physical attack, manoeuvre, or combinations of any such medium.

Lethal weapons

3.6 **General**. Lethal weapons achieve their effects through such readily identifiable mechanisms as blast, penetration, fragmentation, cratering or fire. The often brutal nature of lethal weapons should not negate their use in an indirect approach to undermining an adversary target system.

3.7 **Air-delivered weapons.** Guided weapons (laser, infra-red or electro-optical), hardened target penetrating weapons, sea and land mines, free fall weapons (often known as dumb bombs), area denial weapons (often termed cluster bombs) and anti-radiation missiles are all examples of air delivered weapons. Each of these weapon types produces different effects, which can be modified by factors such as fuze delays, impact velocities and angles, and the hardening characteristics of the target.

3.8 **Land based fire and manoeuvre.** Land based fire and manoeuvre can incorporate all the arms and supporting arms in a targeting role. The characteristics of land based weapons, enable a force to occupy, threaten, harass, and neutralise land targets. A land-based commander's reserve force can also be manoeuvred to strike to achieve an operational level effect at a designated time and place. In order to strike in the deep, penetration by land forces must be achieved by manoeuvre, amphibious assault or airborne operation.

3.9 **Naval targeting.** Naval surface fire support includes those weapon systems that can be employed in support of operations ashore, such as guns or missiles. Also naval assets can be used to target key maritime assets, choke points or sea lanes through surface manoeuvre, sub surface strike or harassment, and mine warfare. Mining achieves its objectives by making an area unsafe for the passage of enemy forces. It is the minefield, therefore, that should be regarded as the weapon rather than the individual mine.

3.10 **Special operations.** Special Forces (SF) can be used independently or in conjunction with conventional force application options. The ability of SF to operate in the deep battlespace, particularly denied areas, allows teams to directly attack targets or provide support to air, land and sea attacks. The ability for SF to conduct sabotage, selective killing and IO targeting requires specialist advice from special operations components or special operations planning teams.

Non-lethal weapons

3.11 **Non-lethal weapons**. Tactical, non-lethal personal weapons such as immobilising agents, blinding lasers, rubber bullets and so on, are not normally considered as part of IO. The use of large scale immobilising agents and electromagnetic pulse and burst weapons are sensitive and beyond the scope of this publication. However, if available for employment they would be required to meet the terms of targeting doctrine in ADFP 23 - *Targeting*.

Perception management weapons

3.12 Often confused with non-lethal weapons, perception management weapons such as propaganda, deception, and some aspects of EW, often use lethal or non-lethal means to achieve shifts in perception. For example, a physical destruction mission can be directed for psychological effect. A feint is a type of deception operation that involves actual contact with an adversarial force. Moreover, EA includes attacks on an adversary's electronic systems that may prove lethal to system operators and users.

Weaponeering

3.13 Capability specialists will be required for advice on PYSOPS, CNA, deception, EA, and strike systems to enable the planning of IO and promote confidence in the level of effects to be achieved. Specialist advice aims to minimise the effort and resources applied to achieve maximum effect, while also minimising the risk of collateral damage. This advice equates to the weaponeering phase of the targeting process. Weaponeering, in an IO sense, considers target vulnerability, weapon delivery accuracy, exploitation or degradation criteria, probability of achieving the desired effect, and the reliability of the capability. The result is the development of a range of options with which to exploit, degrade, or destroy a particular target.

CHAPTER 4

STAFF PLANNING

SECTION 1: INTRODUCTION

4.1 Information operations (IO) is considered to be a development in the conceptual approach to military planning and operations, including their support functions, rather than a new area of military specialisation. IO at the operational and tactical levels is the responsibility of operations staff assisted by other functional groups. Planning staff will also need to consider IO as part of future operations. Within a joint headquarters a dedicated staff preferably has the IO responsibility. Where otherwise constrained this responsibility may also be met by command direction, an awareness of IO, or the establishment of an IO group or board. The manner by which the IO planning function is met must be appropriate to the headquarters and such that IO are considered and integrated with the plan.

4.2 **IO objective**. The objective of IO within the ADF is to contribute to the achievement of military objectives by promoting and protecting ADF decision making, and exploiting and influencing adversary decision making.

4.3 **IO focus**. Through IO, the ADF seeks to enable decision superiority and promote freedom of action for ADF decision making processes, while hindering the efforts of adversaries. IO seeks to exploit the opportunities and vulnerabilities inherent in the decision making process and information-dependent systems. This includes people, infrastructure, weapons, command and control, computers and associated network systems.

4.4 IO seeks to impair or distort the decision-making abilities of an adversary's leadership structure, and to influence the belief or perceptions of a nation's people. The focus is therefore on the psychology of perception and leadership, and the ability of the commanders and managers to provide effective leadership and management.

4.5 **A coordinated and integrated strategy**. ADF IO policies and plans are to be integrated within overall military strategies and objectives to achieve a coherent effect. IO requires the close co-ordination of both offensive and defensive capabilities and activities, as well as effective design, integration and interaction of command and control, with intelligence and other support mechanisms.

SECTION 2: PLANNING CONSIDERATIONS

4.6 Effective IO planning requires:

a. clear strategic guidance;

b. a clear operational mission and intent;

c. clear and achievable IO objectives that support the operational intent and lead to decision superiority;

d. integration and synchronisation of offensive, defensive and supporting IO-related activities within the wider planning process;

e. resource capability, capacity and availability, including limitations and constraints;

f. IO concepts (or themes) that focus IO effort on objectives;

g. consideration of the effect of IO on third parties; and

h. a mechanism for the monitoring and evaluation of the effectiveness of IO.

SECTION 3: IO PLANNING METHODOLOGY

The Joint Military Appreciation Process

4.7 Effective decision making must take account of all aspects of operational planning. This includes deliberate planning prior to operations (contingency planning), responsive and quick planning during operations and the concurrent planning of future operations. The joint military appreciation process (JMAP) addresses planning before and after the start of operations. JMAP provides clear methods for concurrent and responsive planning for ongoing and future operations and for crisis situations. The process enables the commander to select courses of action with an understanding of the associated risks. The JMAP consists of four consecutive steps with an integral and continuous part known as joint intelligence preparation of the battlespace (JIPB). The four steps of the JMAP and their relationship with the JIPB process are shown at figure 1.

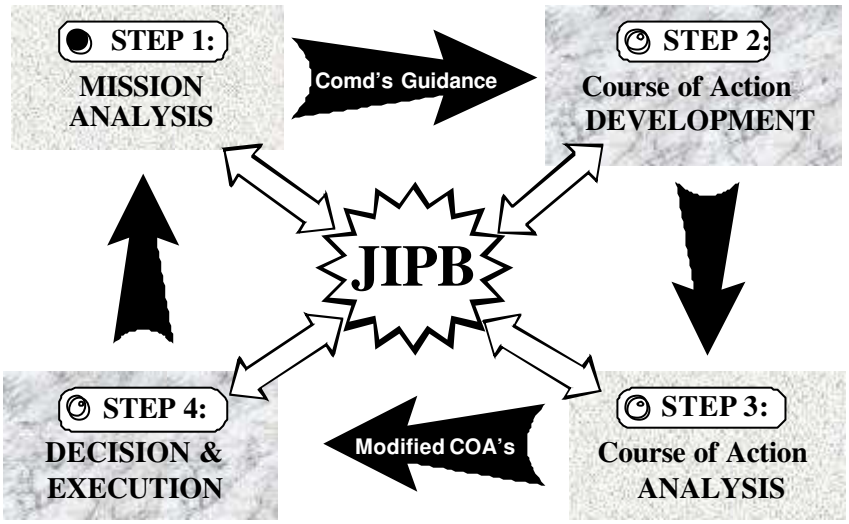


Figure 2 - JMAP - showing the link with JIPB

4.8 IO planning is integral to the JMAP process. IO brings to Course of Action (COA) Development a range of activities that can be synergised within the traditional manoeuvre of major force elements to achieve decisive points. It is not a separate planning activity, nor can IO be considered as a separate manoeuvre element, force element or battle operating system.

JIPB and IO

4.9 **Overview**. The JIPB process requires a thorough study of the total operating environment, including political and social influences and their cumulative effects on possible COA and friendly forces. It requires a detailed analysis of the full range of possible threats, including an adversary's likely COA. JIPB recognises the uncertainty of conflict and allows assumptions to be made to keep the planning process active. It focuses information-gathering sources on validating those assumptions and possible threat COA as early as possible. Hence JIPB will provide the critical vulnerability analysis of the adversary and the environment that can be exploited through offensive IO. It will also provide a basis for understanding own vulnerabilities through assessing what friendly critical vulnerabilities the adversary is likely to target; hence it will be fundamental to defensive IO. Full detail on intelligence support to IO is available in ADFP 19 - *Intelligence*.

4.10 **Determining equity**. Intelligence staffs assist the planning of IO as part of their wider support to the operations planning process. A central part of this support is providing analysis of the objectives and/or endstates stakeholders' desire. These objectives or endstates may be grouped on a matrix as displayed at Annex A. At the strategic level, this grouping may occur in terms of politics, economics, military, and social matters. In joint operations, the grouping may be related more to military characteristics of the environment such as manoeuvre objectives, sustainment, local support, command, intelligence, communications, and so on. Intelligence staff will also provide detail on stakeholder capacity to conduct or sustain information operations. This analysis may be divided into offensive and defensive capability and/or actual and potential capability. It may also be used to address vulnerabilities of the friendly force to offensive IO.

4.11 **Steering collection**. In turn, the intelligence process will receive direction from IO planning. In the pre-conflict period, this will require the development of substantial databases of value to IO planners, including such aspects as biographical data, psychological operations studies, infrastructure and communications data, and capability studies. Subsequently, during conflict planning, gaps in intelligence relating to IO will be identified during JIPB and throughout the continuum of planning and conducting IO. Significantly, steering the intelligence system to collect on assessed measures of effectiveness (MOE) of IO efforts is of paramount importance to this process (see Chapter 5).

Mission Analysis & equity comparison

4.12 **Comparing equity**. From the JIPB stakeholder analysis, the IO planner can compare the relationship between stakeholders to ascertain where mutual benefit occurs, where conflicting aims occur, and where aims are relatively neutral to each other. (This process is illustrated at Annex A). Relative to the friendly mission analysis, the IO planner can then indicate one of the following:

a. Where mutual benefit or support occurs - whether this should be enhanced, neutralised, or made to conflict.

b. Where conflicting aims occur - whether this should be promoted or neutralised.

c. Where neutral or ambivalent aims occur - whether conflict, stasis, or support should be engendered.

4.13 **Mission Analysis** The review of the situation from the IO perspective will provide the basis of advice on the types of IO objectives to be included in Mission Analysis and Commander's Guidance. The IO planner's involvement in Mission Analysis is to provide IO input on:

a. Situation.

b. Assumptions.

c. Mission.

d. Tasks:

(1) specified,

(2) implied, and

(3) essential.

e. Limitations.

f. Planning considerations.

Commanders guidance

4.14 Commanders are central to the operations planning process and their guidance on IO will include an assessment of how the commander views friendly and adversary vulnerabilities. This may translate into a priority of critical vulnerabilities (CV) and priorities of effort for scarce resources. The

commander may also indicate the level of acceptable risk to be sustained and the perceptions to be manipulated. Commander's guidance may also include direction as to the deception target and deception objective (see Chapter 7) and those key elements of information (see Chapter 6), personnel and materiel to be kept secure.

4.15 Central to the development of commander's guidance in relation to IO and targeting is the continuing balance between the implications of the Laws of Armed Conflict (LOAC) and the principles of war. ADF offensive IO will be conducted as a legitimate response, and hence, the selection of targets, the means of attack, the level of force applied, and the risk of collateral damage will all be in accord with national and international law.

COA Development and nodal analysis

4.16 **COA Development**. Supported by JIPB, the COA Development stage will group and link critical vulnerabilities to potential lines of operation and determine the decisive points to be achieved. By this stage, the IO planner has come to terms with the environment and has identified a list of vulnerabilities within the battlespace that may require exploitation through IO. These vulnerabilities form part of the wider range of CV that are developed and analysed within the COA Development process of the JMAP. The operations planning staff will, with advice from specialists, select those adversary critical vulnerabilities, infrastructure targets and high value targets that can be degraded or exploited to achieve the commander's intent.

4.17 **Identify vulnerabilites**. For each COA developed, IO planning assists in the identification of ways to exploit or protect CV, and in the designation of the effects to be achieved. Own CV will be assessed from an adversary perspective as to how they may be affected and IO planning will identify defensive and offensive means to reduce pressure on friendly decision-making capability. Adversary CV will be assessed in concert with manoeuvre and targeting elements as to the capacity for IO to achieve desired results. Assessments will have an offensive and defensive IO component.

4.18 **Nodal analysis**. To conduct such assessments, IO planners will need to conduct nodal analysis. A node is the point where human and machine sensors, processors, decision-makers, databases and the interconnecting communication systems converge. Analysis of such nodes seeks to identify the specific parts or points that can be exploited to undermine wider target systems. Such analysis uncovers potential targets, further elaborates on vulnerabilities, identifies potential ways to achieve effects, and assesses the potential of defence mechanisms. In offensive planning, this nodal analysis will need to be integrated with the wider target systems analysis conducted in support of targeting. In a defensive sense, nodal analysis will need to be integrated with the information assurance and information management activity of the communications staff on the planning headquarters. This process is detailed at Annex B.

4.19 **Designate effects**. As part of the designation of effects within a wider course of action, IO planning will require the derivation of effects relative to nodes and the rationalisation of these effects into objectives for prioritisation of effort. The details of nodes not considered for exploitation or protection can be retained for use later in support of contingency planning.

4.20 **Assign assets to achieve effects**. Against each objective is apportioned the force or asset required to achieve the desired effect. This will require some initial deconfliction between IO elements and sychronisation and sequencing with other assets and effects.

COA Analysis

4.21 There are four main activities undertaken in IO planning during COA Analysis. These are:

a. **Shaping friendly offensive IO plans to achieve desired effects**. This will require reviewing the scale, nature and command arrangements of assets fulfilling IO tasking, and developing time lines and resource requirements for the achievement of effects. Such efforts will also confirm objectives, tasking, groupings and priorities and assist in defining guidelines and restrictions for subordinates.

b. **Assessing adversary actions and reactions from a defensive IO perspective**. The wargamed adversary actions and reactions will require analysis to assess the need to

counter adversary action by pre-emptive IO efforts or increased defensive action. This may also include an evaluation of how to exploit any adversary offensive IO and also where the adversary's defensive IO may become degraded over time.

c. **Deconflicting and synchronising IO activity**.

(1) **Deconfliction**. It is the nature of IO that much of the effort to achieve IO related effects can be detracted from or confused by other IO related activity. For example, thematic based message efforts such as deception, PINFO, OPSEC, and PSYOPS often conflict. Therefore, the IO planner will be required to ensure that each effort works to achieve suitable outcomes in accordance with set priorities. Moreover, IO efforts can often conflict with other efforts such as targeting, manoeuvre and the desires of subordinate commanders. Again the IO planner will seek to plan for and avoid such confliction. Deconfliction is discussed further in the following chapter.

(2) **Synchronisation**. As well as being deconflicted, each IO effort must be synchronised with other IO efforts and wider operations efforts to achieve maximum effects. This process is fundamental to IO and is captured on a synchronisation matrix or on a time/event-sequenced chart. Further detail is at Annex C.

d. **Developing IO contingencies for possible branches, vulnerabilities or crises that may arise**. The utility of wargaming is that it allows for the exploitation of a previously unaddressed or unseen vulnerability, and the preparation for commander's decision points within the battlespace. The identification of the possible circumstances in which the commander will be required to decide how, when and where to shape the battlespace, has direct IO implications for the speed of friendly decision-making by preparing the commander. These circumstances require offensive and defensive IO plans, and also lead to a requirement for contingency plans.

Decision and Execution

4.22 **Approval**. The commander will be presented with IO plans as part of each COA developed and analysed in the preceding stages of the JMAP. The commander will then decide the COA to followed as the plan and approve the IO components of the plan.

4.23 **Plans**. There are three general ways in which IO plans are produced:

a. The general concept for IO (including objectives and means) is included in the main text of the operations order (OPORD) or operations instruction (OPINSTR) while the details of each of the capabilities employed in achieving IO are the subject of separate annexes. This system would normally be used in major conflict, where there is a requirement for large, discrete, highly controlled annexes on deception, PSYOPS, OPSEC, EW, and so on. If used, an IO Annex would simply contain the IO synchronisation matrix that displays the links between capability employment described in other annexes.

b. The general concept for IO is included in the main text while the details of activities are included in a single IO Annex. Caveat or limited distribution material may be the subject of appendices to that annex. This system is of use where the detail of capability employment and policy is not lengthy or involved, and where logically a single annex is all that is required.

c. The IO Plan is released as a separate document. As an inseparable part of the operations plan, IO will rarely be released separately at or below the operational level. However, IO planning guidance and inter-departmental IO efforts may be the subject of individual strategic level IO publications.

Execution of IO and the management of IO in current operations is considered in the next chapter.

SECTION 4: IO AND STAFF ORGANISATIONS

4.24 **Staff responsibilities**. IO has the following staff responsibilities:

a. **Operations**:

(1) inclusion of IO in current operations plans;

(2) policy on IO;

(3) deconfliction and synchronisation of IO;

(4) direction of IO related assets on behalf of the commander; and

(5) providing friendly force updates for the commander's situational awareness.

b. **Plans**. Inclusion of IO in future plans and contingencies.

c. **Intelligence** - through JIPB provide:

(1) intelligence on adversary critical vulnerabilities that may be exploited by IO;

(2) advice on the threat from IO and countermeasures;

(3) targeting intelligence on the specific characteristics of selected targets; and

(4) technical control of intelligence collection operations and activity (including counterintelligence operations).

d. **Communications**:

(1) electromagnetic spectrum management;

(2) management of friendly communications architecture;

(3) technical control over communications assets and their security;

(4) technical control of information assurance measures; and

(5) advice on the vulnerability of friendly information systems, given input from J IPB.

e. **Logistics**:

(1) provision of IO related assets and resources; and

(2) advice on logistics infrastructure and plans, given input from JIPB.

f. **IO Staff** (if formed):

(1) the prioritisation, synchronisation and deconfliction functions of IO management;

(2) evaluation of measures of effectiveness (MOE);

(3) steerage of intelligence collection relative to MOE;

(4) liaising with specialists on the effectiveness and utility of IO capability;

(5) preparing IO aspects of operational plans;

(6) advising on IO issues; and

(7) preparing IO policy and procedures.

IO and targeting cells/boards

4.25 In incorporating IO into operations, planners are offered an expanded range of options which may include an ability to deceive, degrade, destroy, manipulate, or confuse an adversary's information and information systems. Hence, IO forms part of the wider operations process that feeds targeting related processes and activity.

4.26 While recognising the IO input to operations planning, the majority of the IO planners' daily work is related to current operations and hence such staff officers usually reside in the operations area of headquarters. In some cases, an IO cell of specialists and involved parties is required to regularly meet to assist in the prosecution of IO staff responsibilities noted above. Figure 2 diagrammatically displays this process.

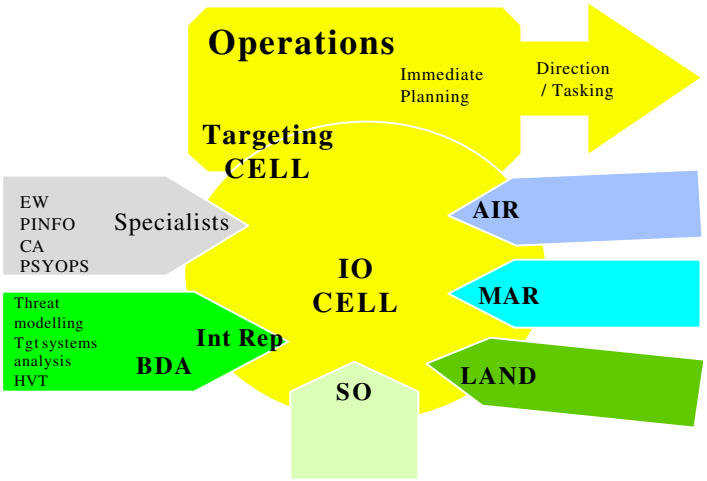


Figure 3 - The IO Cell and Operations

Annexes:
A. Assessing the Environment
B. Nodal Analysis
C. Synchronisation

ASSESSING THE ENVIRONMENT

The Equity Matrix

1. The equity matrix is an analytical product completed by intelligence staff to assist the planning of information operations (IO). In simple terms it states the objectives and/or endstates stakeholders desire. The matrix also provides an overview of stakeholder capacity to conduct or sustain IO. This analysis may be divided into offensive and defensive capability and/or actual and potential capability. It may also be used to address vulnerabilities to offensive IO.

2. All potential stakeholders that impact on the commander's intent should be included on one axis, including non-state actors. The other axis of the matrix is formed from the categories of capability or systems relevant to a situation. Example 1 is a strategic level matrix using elements of national power. Example 2 is an operational level matrix with other elements added. In joint operations the categories may be related more to military characteristics of the environment such as military manoeuvre objectives, sustainment, local support (may be represented by a number of factions), command, intelligence, communications, and so on. A written statement expressing the interest or endstate of the stakeholder in regard to the selected system is added in the blocks formed by the intersection of the axes. Some objectives/endstates have been included in the following matrices as examples only.

Example 1:

Stakeholder	Endstates/Objectives by Capability or Category				IO		
	Political	Economic	Social	Military	Offensive capability	Defensive capability	Vulnerability
AS							
AS Pop							
Adv							
Adv Pop							
Other Stakeholder							
Other Stakeholder							

Example 2:

Stakeholder or capability	Objectives and Requirements					IO		
	Political	Mil Obj	Sustain	C2	Int	Off	Def	Vuln
ADF								
Theatre								
EN Comd								
Clan 1								
Clan 2								
Other Govt 1								
EN AIR								

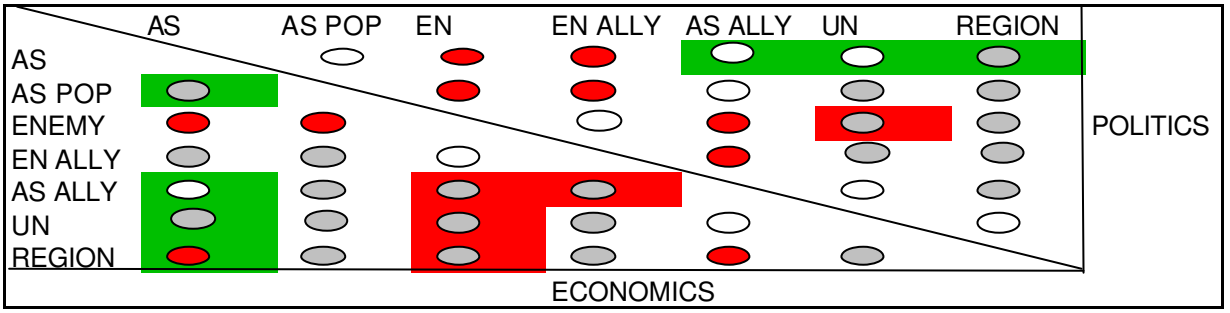
EN LAND								
EN MAR								
EN SF								
FR AIR								
FR MAR								
FR LAND								
FR SF								

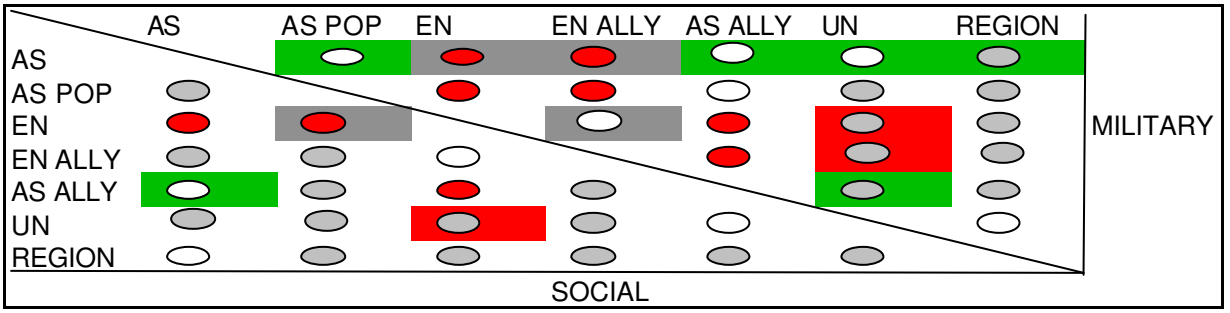
Comparing equity

3. IO planners in operations planning cells will take the above information and analyse and compare objectives to determine potential vulnerabilities and lines of exploitation. These will be linked to the operations plan as it develops in the JMAP.

Equity comparison matrix

4. The comparison of equity can be displayed diagrammatically as shown below. A separate table is established for each category. The example is organised by the categories of politics, economics, social and military. A coloured or shaded button may then be added to represent the level of conflicting or supportive aims of stakeholders. An indication can then be made from the friendly force planning perspective as to whether each of these points could be exploited in support of the commander's intent. In the example, this process is displayed by adding a different type of shaded background to indicate whether the relationship should be made to conflict or be more supportive.





Key:

Circles: White = Of like aims

Red (dark) = Discordant aims

Grey (light) = Unknown / Unassessed

Coloured Background: Green (Vert Stripes) = Change/reinforce to concordant aims

Red (Dark Background) = Create/reinforce discord

Grey (Horiz Stripes) = Mute concord or discord as applicable

NODAL ANALYSIS

1. Nodal analysis has two applications. In conducting offensive IO, it is the methodical examination and evaluation of an adversary's systems to identify nodes that may be exploited to contribute to the attainment of the commander's mission. In conducting defensive IO, it is the systematic examination and evaluation of own force systems to identify nodes that may be exploited by an adversary. This analysis of both the adversary and own forces should result in a list of critical, vulnerable nodes that can either be exploited or should be protected, in supports of the overall operational plan.

2. Nodal analysis is primarily conducted at the operational level. During peacetime, nodal analysis should be routinely conducted as part of the development of campaign plans, operations plans, and contingency plans, all based on strategic plans and guidance.

RELATIONSHIP OF NODAL ANALYSIS TO THE OPERATIONAL PLANNING PROCESS

3. Nodal analysis is part of IO planning which is conducted in parallel and in support of the operational planning process. This approach facilitates the exploitation or protection of nodes contributing to the successful conduct of operations. IO planning is guided by operational planning. An understanding of operational art terms used in the operational planning process is therefore necessary. A more thorough treatment of the operational planning process and operational art terminology can be found in ADFP 1 and ADFP 6.

TARGET DEVELOPMENT RELATED TERMINOLOGY

Centre of gravity

4. A centre of gravity (COG) is that characteristic, capability or locality from which a military force, nation or alliance derives its freedom of action, strength or will to fight at that level of conflict. The centre of gravity may consist of a number of key elements. Typically, the military operations planning process will be primarily focussed through the operational art on efforts to attack, destroy, neutralise or influence, directly or indirectly, an enemy centre of gravity and its key elements. In their broadest sense, the centre of gravity and its supporting elements constitute target systems. Therefore, to gain a clearer perspective of targeting, the ADF views it as the process by which a joint headquarters centrally manages those scarce assets that can affect specific elements of these systems.

Critical vulnerability

5. A critical vulnerability is that characteristic or key element of a force that if destroyed, captured or neutralised will significantly undermine the fighting capability of the force and its centre of gravity. A critical vulnerability is not necessarily a weakness but any source of strength or power that is capable of being attacked or neutralised. Additionally, critical vulnerabilities may be tangible or intangible. An adversary's critical vulnerabilities are initially identified in the ongoing intelligence process. The subsequent critical vulnerability analysis within operations planning identifies the types of target systems that need to be effected to achieve the commander's intent. Hence the critical vulnerability analysis conducted by operations planners is aided by target system analysis process detailed below.

Targets

6. Targets are defined as any geographic area, complex, installation, platform, object, capability or entity planned for capture, neutralisation, exploitation, or destruction by military forces. A platform may be air, sea, land, or space based, and an entity may be a person, government, organisation or body. Capability may be related to systems, training, knowledge, force element, and so on.

Target characteristics. Every target has distinct characteristics. These characteristics form the basis for target detection, location, identification and classification for analysis and strike. Target characteristics include:

Inherent characteristics. The initial, original or essential characteristics of a target object or area that are generally immediately obvious and which are used to identify, detect and categorise the target (for example, the spans, piers, abutments and superstructure of a bridge, or the ethnicity of a target group).

Acquired characteristics. Elements which modify, enhance or augment the inherent characteristics of a target (for example, the internal modifications to a fertiliser plant enabling the production of explosives, or the attitudes and behaviour of individuals relative to specific situations).

Functional characteristics. The organisational characteristics that describe the operations and activity levels of a target and are important in determining target value.

Physical characteristics. Definition of a target by size and shape, physical complexity, composition and construction, reflectivity and absorbency, electromagnetic energy propagation and/or vulnerability.

Mobility characteristics. Characteristics that define the target's ability to move or be moved (that is, targets may be fixed, mobile or transportable).

Environmental characteristics. Constant or man-made conditions that may include atmospheric, geographic, economic characteristics, countermeasures, and accessibility.

Target system

7. A target system is a group or set of targets that are functionally related. 'Functionally' means that all targets in the system contribute towards the function of the system, or each plays a part in the final product. Normally, a target system equates to a measure of capability that is a key element of a force and hence may be considered a critical vulnerability. Systems require an interrelationship between personnel, equipment and procedures.

8. A commander will depend on a number of systems to complete a mission. For example, supply and distribution systems, air defence systems, pay and personnel management systems. Examples of strategic target systems include components of national infrastructure (such as power and communications), political leadership, education/knowledge, utilities, military command and control hierarchy, and offensive/defensive capability. While an individual target may be important or significant based on its own characteristics, its worth usually derives from its relative importance within a target system.

9. An example of a target system is an air defence system, an example of which is at Figure 1. Identification of the air defence system's key components would form a necessary foundation to efforts to gain air superiority within a course of action. Analysis of the air defence system would start with the target system organisation and then analyse the command and control linkages and communications nets, the fighting elements, sensors and the resulting inter-relationships, dependencies and weaknesses.

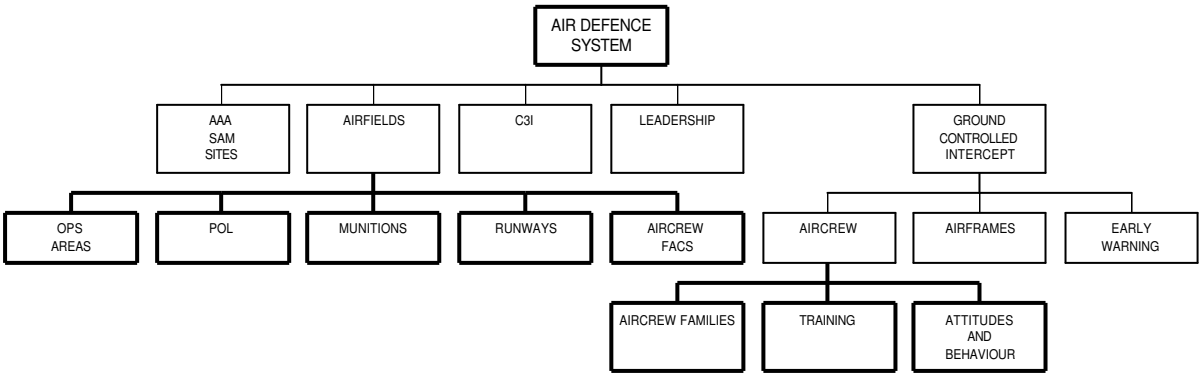


Figure 1 - Representative Target System

Target system components

10. A target system may be broken down into smaller units called target system components that assist or orientate the system to achieve its goal, objective, or purpose. Moreover, each system is a component of a larger, more inclusive system, and hence the definition of systems to be targeted is peculiar to each level of command. Systems can be complex and components are interdependent; a change in one component affects other components. Additionally, systems can be modified to overcome damage to their components.

11. For example, the air defence system's components at Figure 1 include leadership, ground-controlled intercept, anti-aircraft artillery (AAA) and surface to air missile (SAM) sites, airfields, and command and control (C2). Target system components can also refer to component services (for example power, water and lines of communication).

Target system elements

12. Target system elements are smaller parts of the target system than the components and are necessary to the operation of the component as a whole. For example, target system elements of the airfield at Figure 1 include operations areas, petroleum, oil and lubricant (POL) supplies, munitions, runways, aircrew facilities, and aircraft, as well as communications links, refuelling tankers or bowsers, or air traffic control (ATC) facilities. Further levels of analysis may derive the training of aircrew as an element of the target system. Where derived elements are tactical assets fundamental to the achievement of operational level outcomes, they are referred to in joint planning as High Value Targets (HVT). An example of HVT in the system at Figure 1 is the combat air patrol airframes.

Nodes

13. A node is the point where human and machine sensors, processors, decision-makers, databases and the interconnecting communication systems converge. Nodes are normally considered as the junction between elements, components or systems. However, nodes may be considered as elements of a target system in their own right.

14. In the example above, the sector headquarters that coordinates the effect of the AD system or the communications links into the headquarters could be considered nodes. Degrading the headquarters performance will have a disproportionate effect on the system.

15. To be vulnerable a node must satisfy three criteria:

Susceptible. There must be a weakness to exploit.

Accessible. There must be scope and resources to exploit or degrade the node.

Feasible. The exploitation must be worth the risk. This will not only include security and LOAC considerations, but will measure the ability of the node to recover its function.

Target system activities

16. Target system activities encompass those actions or functions performed by the target system components and elements in pursuit of system goals. The target development process should not focus on the system nor its components, but rather on their activities. Once the critical vulnerability that must be modified or defeated has been identified, nodes within key target systems, components, or elements that should be attacked, degraded, or exploited to produce the desired effects can be determined.

Target system linkages

17. An understanding of the linkage between target system components and their interdependence is imperative for accurate analysis. Linkage is the connection between installations performing identical, similar, related, or complementary activities or functions. Interdependence describes the mutual relationships among installations so that the activity of one is contingent upon, influenced, controlled, or determined by another. For example, some industries are dependent upon

the products (such as capital goods, equipment, components and expendable supplies) of other industries to manufacture their own products.

Target systems analysis

18. Target systems analysis process (TSA) examines the following aspects of a target system:

Target system characteristics. Identify the dimensions of the target system in space, time and effect, determining the general components and elements that comprise the system.

Target system activities. Determine the key activities and functional outcomes of components and elements to assign relative importance to the system.

Target system linkages. Develop an understanding of the linkage between target system components and their interdependence.

Nodes. Identify those key points where target systems, system components and target elements are linked and dependent upon each other. TSA focuses on identifying the critical nodes within key target systems that will satisfy objectives and conform to guidance. Critical nodes are also assessed to identify the implications resulting from their damage, exploitation or destruction.

Critical elements. Important nodes are analysed to identify their critical elements (CE) for destruction or exploitation. Every target has at least one CE that, if damaged or destroyed, will prevent the target from performing its designed function for some period of time. For example, the CE of a sector headquarters in an enemy air defence system would comprise the operators, the commander, the operations room, the communications room, communications feeds, external communications facilities or main and emergency power supplies. The particular CE to be attacked will be determined in the light of:

(6) command guidance,

(7) weapon type availability and accessibility,

(8) the reliability of perception management strategies, and

(9) the protective characteristics of the CE.

Recovery times. Selected nodes are also analysed to identify recovery times associated with their exploitation or destruction. Recovery time is a measurement of the time and cost required for a system to regain the ability to function after being disrupted. Recovery effort is a key indicator of how critical a target is to the enemy. Assessments on the time and cost required for an opponent to respond to counter the exploitation or to repair or replace damaged elements, allow operations planners to determine the timing or necessity for re-attack in concert with the wider scheme of manoeuvre. The time required to restore a degraded function depends on many factors. These may include the sensitivity of the adversary's intelligence system to perception management activity and the adversary's defensive information operations capability. It may also include the level of damage inflicted, power, energy and materials for repairs. The availability of alternative locations to substitute for damaged or destroyed functions should also be considered when analysing an entire target system's ability to recover.

ROLE OF INTELLIGENCE STAFF IN NODAL ANALYSIS

19. In most circumstances, identification and analysis of systems to determine critical nodes requires the skills of specialist analysts. This effort is conducted by the Intelligence staff. Of note, however, is that intelligence analysts conduct TSA from an adversary perspective, that is, consider targets from an adversary perspective. There remains a requirement for IO planners in the operations planning function to conduct nodal analysis from the perspective of how friendly COA are seeking to shape the battlespace and achieve effects.

20. Nodal analysis depends on highly developed and well maintained databases which provide basic intelligence on potential nodes within an adversary's systems as well as own systems. Intelligence staff will compile a comprehensive database of critical nodes which may be exploited or will require protection during a contingency. The identification of critical nodes and the examination of their vulnerability, is conducted by the IO planner, as part of either deliberate or contingency planning. The IO planner may often require additional information on a node and will task the intelligence staff in accordance with standing operating procedures.

RELATIONSHIP OF NODAL ANALYSIS TO TARGET DEVELOPMENT

21. Target development is part of the targeting process described in detail in ADFP 23 *Targeting*. IO analysis of adversary nodes is integral to this process. IO analysis of friendly nodes is integral to the defensive analysis, and forms part of information assurance (IA) planning coordinated by the J6 or CIS staff.

22. Target development and nodal analysis are both done in support of the operational planner's critical vulnerability analysis. The efforts will be conducted in parallel. Close coordination is essential for the success of both. The IO planner provides input to the targeting process on those offensive IO actions required to be inserted into the Joint Target List (JTL). The JTL includes a statement on the significance of the target relative to the commander's intent and are produced for each COA developed. The list may nominate force capabilities that could be employed, while the IO planner's comments should be included if the target can be affected through IO means. Input will also be made the restricted/protected target list. An example would be an enemy command and control site which is being exploited for deception purposes which outweighs its importance as a target.

23. All the JTL will be reduced to a Joint Prioritised Target List (JPTL) when a decision is made as to which COA is to be enacted as the plan. The IO planner should be a member of any targeting cells or boards designed to validate and prioritise nominated targets.

24. Nodal analysis has similarities with Target Systems Analysis (TSA), conducted as part of target development. TSA is a detailed analysis of an entire target system in order to identify the relative importance of individual target system components, elements or nodes. Nodal analysis examines specific systems, their interrelationship, and assesses the impact of exploitation of critical and vulnerable nodes, both of a particular system, and on other systems which are related through critical nodes.

ADFP 23 includes a thorough treatment of the target development process.

NODAL ANALYSIS DOCUMENTATION

25. Analysis of all identified systems is published in standardised electronic and/or hard copy format. Each individual system analysed will comprise a separate publication, termed a Nodal Analysis Study. Each study should be cross-referenced to the campaign or operational plan it supports. The content of the publication will include textual data, system diagrams, imagery of system components, biographical information, cultural information and possible actions to significance statements and possibly generic weapon solutions.

NODAL ANALYSIS TOOLS

26. Nodal analysis is a complicated and manpower intensive process. The tools provided below are not designed to replicate CIS tools, feeds and inputs that can be harnessed in the nodal analysis process. Instead they graphically represent the 'way' or logical process behind nodal analysis.

27. **Nodal analysis worksheet**. The nodal analysis worksheet provides an audit trail and a graphic representation of the breakdown of target systems and the identification of critical elements of nodes. A separate nodal analysis worksheet should be maintained for defensive and offensive IO.

NODAL ANALYSIS WORKSHEET

CHARACTERISTICS OF TARGET SYSTEM OR STAKEHOLDER	VITAL INTERESTS, COMPONENTS and ELEMENTS	ACTIVITIES AND LINKAGES	POTENTIAL NODES	CRITICAL ELEMENTS OF NODES

28. **Pressure point worksheet**. A pressure point worksheet is a type of nodal analysis wooksheet used in the planning of information campaigns. It examines people as targets and and attempts to define where they can be pressured (in perception terms) given potential future actions.

PRESSURE POINT WORKSHEET

TARGET OF THE INFORMATION CAMPAIGN	VITAL INTERESTS	ACTION(S) TARGET IS EXPECTED TO TAKE TO ACHIEVE VITAL INTERESTS	POSSIBLE PRESSURE POINTS

CLASSIFICATION

29. **Vulnerability**. Identifying the preferred critical elements (or pressure points) to target or protect, a product of conducting the nodal analysis in concert with wider operational planning and

therefore assimilating the command direction and scheme of manoeuvre being developed. The key ingredients of this process can be displayed graphically as shown below.

Critical Elements or pressure points	**Assessment of Vulnerability**				**Relation To COA**	**Priority of Effort**
	Susceptible	Accessible		Feasible		
		Suitable resources	Available resources			

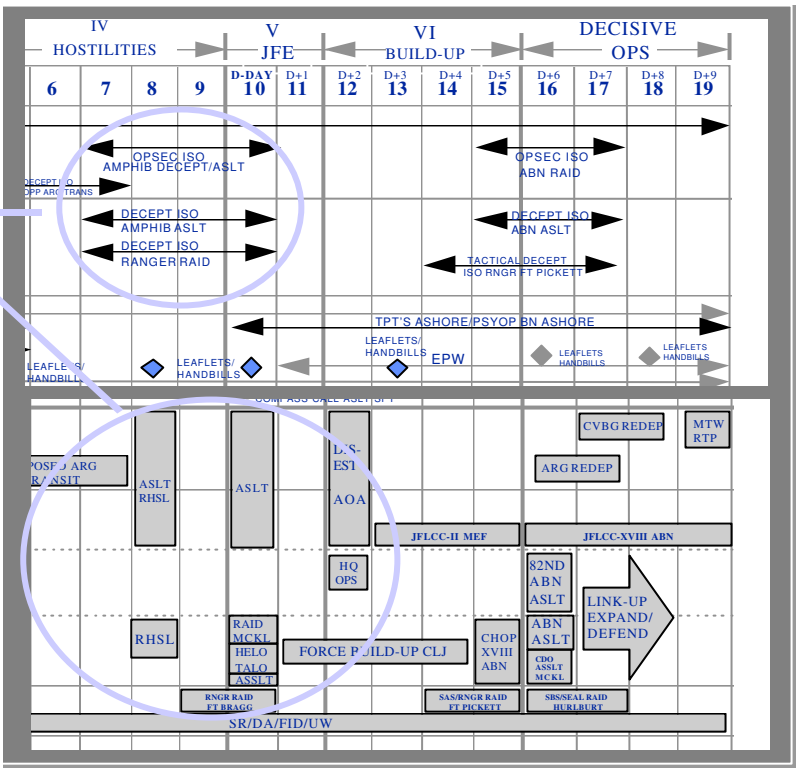
SYNCHRONISATION

1. The diagrams below indicate the process used to develop the IO aspects of the operations planning synchronisation matrix to achieve designated effects and sequence objectives.

Look For Opportunities to Support JTF Objectives

Develop Detailed Plans for Each Capability

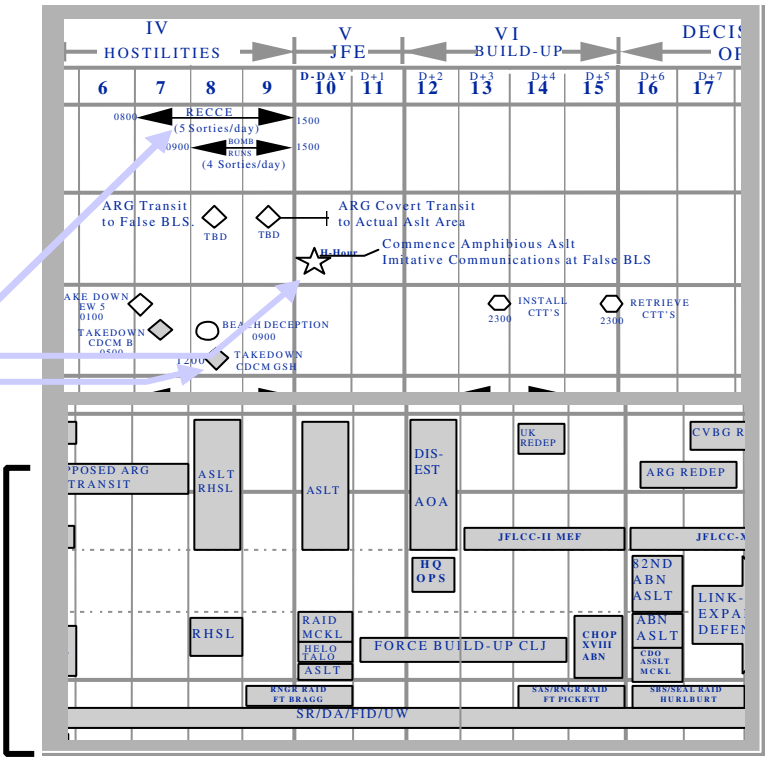
Ensure Each Capability Deconflicted and Synchronised



Elaborate on Details of the Plan

Required Force/Asset Time Lines. Identify Show Stoppers

Continuously Update Campaign Plan



An example format of a synchronisation matrix used during to support NATO operations in Bosnia is shown below.

TIME LINE →	**PHASE I** (Projected Timeframe)	**PHASE II** (Projected Timeframe)	**PHASE III** (Projected Timeframe)	**PHASE IV** (Projected Timeframe)
Trigger/Decision Points				
Anticipated Opponent Action(s)				
Air Defense				
Aviation				
Command & Control				
Command Information				
Communications				
Electronic Warfare				
Engineers				
Fire Support				
Intelligence				
JMC				
Logistics				

Manoeuver				
Medical				
Military Deception				
OPSEC				
Personnel				
Political Advisor				
PSYOP				
Public Affairs				
Special Operations				
S Judge Advocate				

CHAPTER 5

INFORMATION OPERATIONS AND CURRENT OPERATIONS

SECTION 1: INTRODUCTION

General

5.1 The majority of information operations (IO) staff effort is directed towards the conduct of current operations. This effort is discussed in this chapter in two broad areas:

a. **IO management**. The focus of this IO management in this chapter will be on deconfliction of IO activity and those tools available to assist in daily management and forecasting of IO activity.

b. **Analysing and monitoring effects.** This includes establishing and evaluating measures of effectiveness (MOE), maintaining an effective reporting system to identify a degradation in information assurance, and steering the Battle Damage Assessment (BDA) efforts of the intelligence system.

IO management

5.2 IO management includes the prioritisation, synchronisation and deconfliction functions of IO staff effort. Prioritisation and synchronisation was discussed in the previous chapter. Deconfliction is discussed below. IO management also addresses the need to monitor IO efforts against the effects to be achieved. Specialist advice will be required to assess the effectiveness of weapon systems, policy and other activity in achieving the desired effects. This assessment leads to advice to operations planners on the success of that approach, whether renewed effort is required, whether a different measure or approach is required, or whether the activity is concluded.

5.3 Some tools available in the management and forecasting of IO activity are discussed at Annex A.

SECTION 2: DECONFLICTION

Psychological Operations and IO

5.4 Psychological operations (PSYOPS) is the primary means of affecting attitudes and behaviour within IO and has also a secondary impact in all military operations. The psychological impact of military activities can be planned for and exploited. The categories of PSYOPS are:

a. **Psychological action**. The planned use of support activities to reduce an adversary's prestige and influence, and to increase friendly influence and attitudes in potentially hostile or neutral countries.

b. **Psychological consolidation**. Those activities designed to foster the establishment or maintenance of order and security, and gaining the support of a local population in order to advance political and military objectives.

c. **Psychological warfare**. Efforts designed to bring psychological pressure to bear on an enemy and to influence attitudes and behaviour of hostile groups and target audiences in areas under enemy control.

5.5 Each category of PSYOPS effort requires deconfliction with other PSYOPS categories, other IO efforts, and wider military operations. Aspects of this deconfliction are as follows:

a. **PSYOPS at various levels of command**. PSYOPS guidance, direction and plans are generated from the 'top down'. In this way tactical level efforts will not undermine operational level objectives and so on. However, this process must ensure that subordinate commanders' flexibility and manoeuvre is not unduly constrained.

b. **PSYOPS and public information**. Psychological consolidation and public information (PINFO) processes appear to overlap in their attempts to influence friendly and sometimes neutral target audiences. In fact, PINFO releases messages through accredited Media resources. PINFO deals in themes, with the content of the message largely construed by the media form. PSYOPS avoids accredited Media, and deals in specifically formatted propaganda for which the medium used is only a vehicle. Moreover, PSYOPS seeks to alter attitudes and behaviour, which is not the pure focus of PINFO.

c. **PSYOPS and operations security**. PSYOPS is heavily influenced by operations security (OPSEC) planning in that OPSEC may seek to deny information to an adversary that would be a significant benefit to PSYOPS. Due to the significance of the essential elements of friendly information (EEFI) that drive OPSEC, OPSEC considerations will normally override PSYOPS requirements.

d. **PSYOPS and deception**. In psychological warfare terms, PSYOPS may seek to influence attitudes and behaviour of key players in the adversary's command decision system. However, deception seeks only to shift perceptions for a given period of time. Deception does not, therefore, deal in altering attitudes and behaviour, but rather seeks to exploit weaknesses in existing attitudes and behaviour patterns. Due to the transient nature of deception objectives, PSYOPS will not normally be involved in releasing deceptive material due to the potential loss of credibility to the more enduring PSYOPS campaign. However, PSYOPS material must not conflict with the deception story.

e. **PSYOPS and civil affairs**. Psychological consolidation activities will normally form a vital link in the conduct of civil affairs (CA). This is especially the case in efforts to foster and maintain order and security.

f. **Counter PSYOPS and defensive IO**. The counter PSYOPS effort designed to counter an adversary's PSYOPS attacks on friendly and neutral audiences forms an integral part of defensive IO. Countering an adversary's covert propaganda effort (that is the adversary's use of black propaganda – which purports to emanate from another source) is linked directly to the counterintelligence (CI) counter subversion effort. More broadly, the counter PSYOPS effort will be linked to information assurance (IA) efforts to secure personnel within information systems and processes supporting decision-making, from subversive messages.

Deception and IO

5.6 **General**. Deception is a fundamental part of IO in that it complicates the adversary's decision cycle by causing the deception target to estimate the situation incorrectly. While normally considered part of offensive IO, deception also forms part of defensive IO by acting as a tool in the OPSEC process and in CI activity. Security requirements generated by the use of deception will normally drive or be allocated priority over other IO activity or measures.

5.7 **Deception and OPSEC**. OPSEC is discussed in more detail in the following chapter. Of note is that there is a symbiotic relationship between OPSEC and deception. The truth must be protected if the false is to be revealed. Moreover, an OPSEC measure can be to deceive an adversary collection system. The planning and execution of OPSEC measures that are needed to secure the real operation are not a direct responsibility of the deception planners. However, the OPSEC measures taken to protect the real operation have to be coordinated with the measures needed to insure against the compromise of the deception operation by the discovery of the real activities. Additionally the deception plan could require the disclosure of some real activity, to the adversary. So it is necessary to ensure that the OPSEC measures associated with the real plan are not so effective that they preclude the adversary from discovering the elements of information required to be released under the deception plan.

5.8 **Coordination of electronic activity.** In planning and conducting electronic deception, the intelligence and deception staffs must work closely with communications and electronic warfare (EW) staffs and units. Effective electronic deception requires coordination:

a. **With electronic warfare.** The full range of EW activities has to be coordinated with the deception plan. Electronic support measures (ES) are required to gain intelligence about the deception target, including knowledge, intentions and expectations. Electronic protection measures (EP) and electronic attack measures (EA) are required to degrade the target's ability to gain visibility of real activity. For example, jamming can be used to screen or confuse surveillance of activities whose concealment may be an essential part of the deception operation. Moreover, drawing the adversary's attention to an activity can be a useful way of ensuring a false ploy is noticed and given priority in the target's intelligence collection plan. However, EA and EP must be constrained to ensure they do not interfere with the portrayal of the deception story through electronic means.

b. **With non-electronic deception measures.** Deception is unlikely to be achieved by the use of electronic measures alone, since the target, who is attracted to a situation by what he sees through the electronic spectrum, will seek confirming evidence through other means. Careful integration of electronic deception with visual, sonic and olfactory measures is critical to the successful projection of a deception story.

c. **With real communications and non-communications activity.** It is also important that the full range of EW activities and the real communications and non-communications activities of the force are coordinated with the deception operation. Close control and integration of the communications and non-communications activities in support of the real and the deception operation will be essential to their success. Both communications and non-communications electronic measures are needed to convey the deception story to a wide range of sources that will influence the target.

d. **Communications security**. Successful electronic deception (and deception in general) requires a very high level of communications security (COMSEC) and communications discipline in the force. Units have to appear to be acting normally, to only reveal what the deception plan says they should, and give no other indicators to the target. Special controls may need to be implemented, however these in themselves should not indicate that something special is occurring.

e. **Effect on signals intelligence**. The projection of the deception story using electronic means can and should be reflected in friendly signals intelligence (SIGINT). This closed loop effect will be particularly important if the deception includes the introduction of imitative electronic deception into the adversary communications system. SIGINT may well be collected by agencies not operating in the same command as the deception authority. Therefore, close coordination between all the agencies handling SIGINT and intelligence processing staffs is required to ensure imitative false intelligence is identified, filtered out and not allowed to influence the assessments of those who may not be fully aware of the deception operation.

Electronic warfare and IO

5.9 EW contributes to IO in three ways:

EA – concerned with denying an adversary commander use of the electromagnetic spectrum to effectively command and control forces (usually associated with offensive IO);

EP – involved with guaranteeing the use of the electromagnetic spectrum for the commander to command and control friendly forces (usually associated with defensive IO); and

ES – contributes to the commander's accurate estimate of the situation in the operational area (usually associated with the intelligence support function to IO).

Each element of EW is interdependent with the other elements and will often require deconfliction. For example the fulfilment of information requirements via ES may conflict with a desire to jam adversary frequencies. Specialists will usually address such deconfliction, leaving IO staff and

operations planning staff to ensure wider systems are working in concert to achieve desired outcomes. An example of the wider deconfliction effort is noted in the deception section above.

Operations security and IO

5.10 OPSEC is covered in more detail in Chapter 6. The IA focus on assuring information for command decision-making and the OPSEC focus on denying EEFI to an adversary are the two cornerstones of defensive IO. IA and OPSEC are therefore essentially linked and need to be strictly coordinated.

5.11 Denying adversary covert attack options is a role of CI (part of the intelligence function) and hence CI counter-espionage operations will need to act in concert with OPSEC measures designed to deny overt and clandestine threats to key elements of information.

Physical destruction and IO

5.12 Physical destruction in IO terms relates to the use of lethal weapons (or clinical strike) to affect designated nodes as part of an integrated IO and targeting effort. The effect required is not necessarily 'destruction' as such but rather may be selective degradation of capability including will to resist. Deconfliction needs to occur as follows:

a. The targeting process, especially the Joint Targeting Coordination Board, will need to prioritise targets, as well as deconflict and synchronise assets available for missions.

b. Physical destruction always has psychological effects and must be deconflicted with, supported by, or subject to, PSYOPS planning and action.

SECTION 3: MONITORING EFFECTIVENESS

General

5.13 Monitoring effectiveness includes establishing MOE and linking the assessment of MOE to the combat assessment aspects of the targeting process and to the security validation and reporting process.

5.14 During planning, the MOE for each IO element will need to be defined. These will be further developed and monitored as part of current operations. MOE are considered in an offensive context (for the targeting outcomes of offensive IO) and in a defensive context for the security aspects of defensive IO. These determinations ideally rely on such data as mathematical models, ongoing practical weapons testing and historical analysis, all of which combine to enable staff to predict the effectiveness of IO activity. In PSYOPS this process may include 'pre-testing' types of product to guarantee an appropriate effect.

Offensive IO - measures of effectiveness

5.15 **Lethal weapons (physical destruction).** Methodologies published in the Joint Munitions Effectiveness Manuals (JMEM) facilitate the development of MOE for air delivered weapons and special operations by formalising the known characteristics of particular weapons and their effects against different types of target. For other force capabilities, staff tables may be used to conduct this analysis. In either case, these data sources enable the development of specific MOE based on the known effects and signatures of the weapon used. Such MOE may include parameters for assessing whether a bridge may be destroyed or sustain only light damage, or whether a runway may be cratered or interdicted.

5.16 **Perception management weapons and risk**. The effects of perception management weapons, such as deception and PSYOPS, are inherently less definite than those achieved by lethal weapons. These effects may be trends, activities or altered patterns of activity. MOE are, therefore, not as rigid as for lethal weapons. In this case, derivation of MOE requires a clear statement of effect and determination of the events and information that will indicate the desired effect is being achieved. Uncertainty should not preclude the use of such weapons; however, an inability to identify results is a significant risk to operational effectiveness. Hence, commander's approval for perception

management weapons employment will usually be predicated on the provision of feasible MOE. The brief outline of potential MOE provided below is only intended to be indicative, and substantive MOE will need to be developed particular to each target type and circumstance.

5.17 **Perception management MOE**. MOE for the employment of perception management weapons include:

a. **Propaganda MOE.** The use of propaganda as a weapon within the Psychological Warfare category of PSYOPS aims to achieve attitudinal and behavioural change in adversary target audiences, or those in areas under adversary control, in order to achieve a desired result or effect. The desired changes may manifest themselves through population movement, civil unrest, retreat, surrender or cooperation. The MOE for a PSYOPS campaign will be directly related to the desired effect, the accessibility of the target audience, the type of propaganda campaign, the themes and symbols used and the types of media selected.

b. **Deception MOE.** The objective of a deception operation is stated in terms of what the adversary commander is to do, or not to do, within the battlespace, within a given time frame. Therefore, successful deception will require an intelligence focus on adversary indicators that prove or disprove the deception plan is working. As deception can be employed through targeting a number of sensors (olfactory, electronic, sonic, and visual) the MOE can focus on adversary sensor analysis and/or adversary reaction.

c. **Electronic Attack MOE**. Electronic attack (EA) depends on Electronic support (ES) measures for cuing and to assess its effectiveness. Signatures may include the cessation of transmission, an adversary's inability to detect or react to hostile forces, the use of alternative or redundant systems, or changed operating procedures or parameters.

Defensive IO – measures of effectiveness

5.18 **Security**. Security MOE are dictated by commanders, in the designation of the level of damage or degradation (often referred to as harm) they are willing to accept on their information, personnel and materiel. MOE on passive security measures may be defined by the category of security control used. That is, passive controls include:

a. military security – the controls imposed by Defence, within Defence, to protect its information, materiel and personnel; and

b. civil security – the controls imposed on the civil population, either by the civil authorities through legislation, or in a theatre of war or emergency by the military authorities on behalf of the civil power.

5.19 Security MOE will seek to evaluate the effectiveness of such controls' success in:

a. deterring threats from penetrating defences;

b. highlighting hostile attack by forcing threat sources into relief;

c. increasing the level of security awareness; and

d. providing suitable response, investigation and repair capability.

5.20 **Information assurance**. IA MOE will include those systems, procedures and training developed to ensure confidentiality, data integrity, transaction non-repudiation, system availability and user identification and authentication. For example, system availability may be evaluated as a product of survivability (tolerance and restoration) and reliability. Such assessments when reviewed against shifting or emerging threats, dictate the level of protective measures, alarms and response measures that need to be installed. In turn these measures become part of the collective IA effort that require MOE. Measures and response mechanisms include:

a. an ability to increase awareness of risk;

b. an ability to identify and patch systems at risk;

c. installation of intruder detection systems on key nodes;

d. assessment and analysis capability on the level of threats;

e. emergency response teams;

f. 'Red Teams' to reverse engineer attacks; and

g. plans for degradation or loss of networks.

Combat assessment

5.21 Combat assessment (CA) provides the feedback necessary to ensure the continuing validity of the targeting process, and recommends future targeting priorities. Commanders must be cognisant of the fact that CA is resource intensive and will divert assets from other operational or intelligence tasks. There are four aspects to CA:

a. **battle damage assessment** (BDA), in which intelligence personnel analyse the effects of weapons employed against a target;

b. **weapons effectiveness assessment** (WEA), in which weapon specialists compare the actual performance of the selected weapon with that expected from data contained in planning manuals;

c. **re-attack recommendations** (RR), in which a collective staff effort conducts a reactive examination of the results of completed missions and makes an assessment for operations staff of whether a target should be re-attacked immediately to facilitate future missions against related targets; and

d. **mission assessment** (MA), in which operations planners address the effectiveness of the overall operation in light of command guidance.

5.22 The most critical ingredient for effective CA is a comprehensive understanding of the commander's guidance and how it relates to a specific target, as well as intelligence input on the overall impact of operations against the adversary.

5.23 Thorough CA greatly assists a commander in determining future mission guidance. All components, all commands, and all sources contribute to and rely on CA. Figure 1 shows the interaction and coordination between those with functional responsibilities, and the four elements of CA.

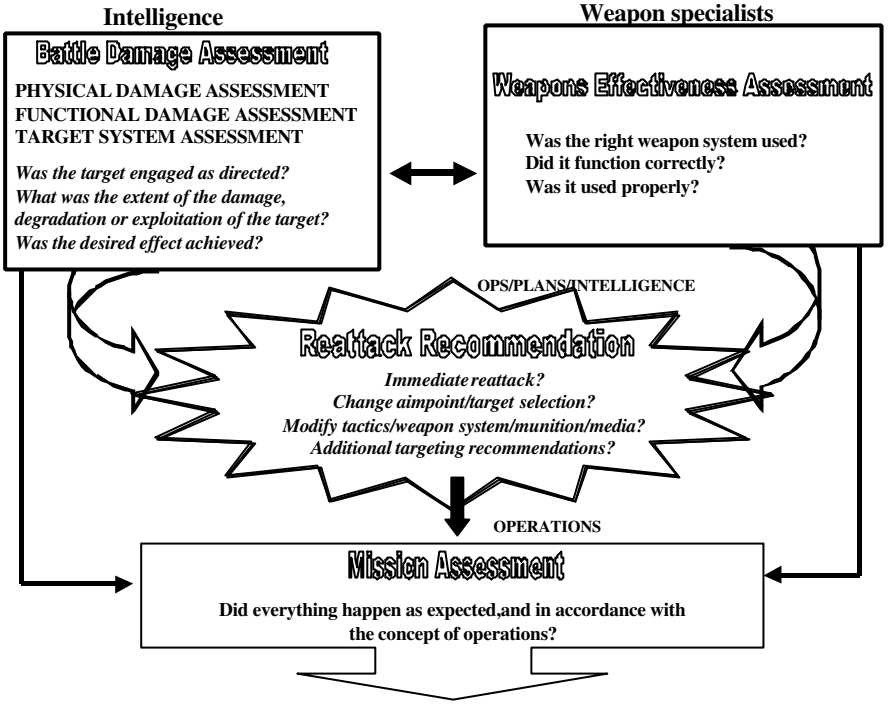


Figure 4 - Combat assessment - coordination and integration

Battle damage assessment

5.24 Battle damage assessment (BDA) is a core aspect of CA and is central to the effective performance of subsequent aspects of CA. BDA is the estimate of the effect on targets resulting from the application of force or perception management activity. BDA also forms part of the intelligence system's estimate of residual adversary capabilities. Timely BDA influences current and future military operations and allows the commander to quickly allocate or redirect forces in their most efficient configuration.

5.25 Separate processes are used for assessing the outcomes of targeting by lethal weapons and perception management tools. However, generically BDA comprises:

a. physical damage or perception influence assessment,

b. functional damage or degradation assessment, and

c. target system assessment.

5.26 **Physical Damage Assessment**. Physical damage assessment is an estimate of the extent of physical damage to a target based on observed or interpreted damage. This post-attack target analysis is a coordinated effort among combat units, component commands, joint task forces, theatre command and national agencies. Information needed to make a physical damage assessment may be derived from mission reports, imagery, aircraft cockpit and weapon system video, personnel debriefings, artillery target surveillance reports, and the various categories of intelligence.

5.27 **Perception influence assessment**. Measures of effectiveness (MOE) for perception management strategies focus on trends, activities, or altered patterns of activity. Hence BDA is often more complex than for the employment of lethal weapons. The perception influence assessment examines the behaviour or functionality of a target against the criteria defined in these MOE. The results of this assessment will necessarily be more qualitative than those for BDA of lethal weapons, but this should be viewed as a characteristic of the weapons themselves and not preclude their use.

a. **Deception**. Intelligence has a special relationship with operations staff in the conduct of deception planning. The MOE for deception relates to the deception objective,

which is stated simply as what the deception target is to do, or not to do, within a given time frame, over a given space. To establish a BDA architecture, intelligence staff fulfil the following functions:

(1) **Know the deception target**. Determine what the target is doing, capable of doing and what the target intends to do. This requires extensive biographical related assessments on the targets decision-making profile and the foibles, attitudes and capability of staff and advisers. In BDA terms, this allows the intelligence staff to predict the likely target reaction to the deception and the reaction if the target detects the deception. Such analysis allows the intelligence staff to determine indicators of target activity and behaviour that prove or disprove the effectiveness of the deception story.

(2) **Know the deception target's intelligence system**. Deception requires intelligence staffs know and be in a position to control the information inputs to the deception target's decision-making process. Such knowledge and capability allow intelligence staff to target those parts of the deception target's intelligence system that will achieve best carriage of the deception story. This analysis leads to decisions about sources that have to be destroyed or neutralised and those that should be targeted for manipulation as a matter of priority.

b. **Psychological operations**. BDA in psychological operations (PSYOPS) forms part of the post-testing process. Results are collection through intelligence channels, observable reactions, or specific PSYOPS post-testing activity such as survey samples, panels of experts, and panels of representatives. The results of PSYOPS product are checked against indicators determined during the planning process. There are two types of indicators:

(1) **Direct indicators**. A direct indicator occurs when the target audience displays activity in accordance with the psychological objective. For example, if the psychological objective was to encourage the local population to report enemy movements, a direct indicator would be a substantial rise in the number of reports received.

(2) **Indirect indicators**. Indirect indicators are events that appear to be the result of PSYOPS activity but cannot be conclusively tied to the material. They may include physical actions by an adversary to deny the PSYOPS product from the target audience or may be an increase in counter-PSYOPS activity by the adversary.

c. **Electronic Warfare**. Electronic attack (EA) crosses the bounds of both lethal and perception management weapons. Indicators of the effectiveness of EA will be examined through intelligence channels, and especially through electronic support (ES). BDA considerations for elements of EA are as follows:

(1) **Jamming.** A target suffering jamming may switch off emitters, reveal emergency or silent frequencies or activate alternative systems or reserve modes of operation that are more susceptible to friendly ES. Jamming may also interfere with friendly electronic systems and will deny the target frequency as a source of ES information. This may effect BDA collection architecture. Consideration of an adversary's ability to employ lethal weapons against jammers is considered in the planning for their use.

(2) **Deception.** An adversary's ES is the target of manipulative EW deception and is subject to the same BDA requirements as noted for deception above.

(3) **Neutralisation.** The assessment of the level of damage to target emitters due to neutralisation by electro-magnetic means is usually conducted via indirect indicators of damage. Unless technical expertise is available on the sight of the emitter, historical data of neutralisation is the main direct assessment tool.

Indirect indicators of damage may be change in operational procedures, loss of power to observable assets, and so on.

d. **Computer network attack**. BDA requirements for computer network attack are the same as for EA neutralisation noted above.

5.28 **Functional damage or degradation assessment**. Functional damage or degradation assessment estimates the remaining functional or operational capability of a targeted facility, object, audience or person. Functional assessments are inferred from physical damage assessments or perception influence assessments. They include estimates of the recovery or replacement time required for the target to resume normal operations. Such analysis is typically conducted in intelligence all-source centres or designated BDA fusion cells and is conducted in conjunction with support from higher level assets.

5.29 **Target recovery time.** As part of the functional damage assessment, a recovery time to repair, replace or recondition the target's critical element(s) or node(s) is also determined. This time is an estimate based on type, degree and location of the degradation relative to the strength, will and resources required to recover. The availability of spares, reserves or alternate elements, campaign tempo and the expected duration of hostilities, as well the adversary's determination to repair, recondition or replace the degraded element are all factors used to calculate recovery times.

5.30 **Target system assessment**. Target system assessment is an estimate of the overall impact of force employment or perception management techniques against an adversary target system. In this assessment the analyst uses the same criteria as used to determine the individual target's functional damage or degradation. These assessments are typically conducted in intelligence all-source centres or designated BDA fusion cells and is conducted in conjunction with support from higher level assets providing additional target system analysis. These centres compile all BDA reporting on physical and functional damage to targets within a target system and assess the overall impact on that system's capabilities. This lays the groundwork for future recommendations for military operations in support of operational objectives

5.31 **Reporting**. Central to the effective conduct of BDA is the timely reporting of the results of these assessments to higher command. BDA reporting consists of three phases by which physical, functional and target system damage assessments are conveyed to all levels of command. The analysis contained in the reports must be read in conjunction with intelligence assessments on the likely adversary response. BDA reports attempt to answer to the following questions:

What were the actual levels of damage or exploitation to the target?

What residual capability remains?

What level of collateral damage was inflicted?

Were there any unpredicted results or adverse impact on adversary activity or operations?

How long will it take the adversary to repair the damage, or recover from exploitation and resume pre-targeting levels of activity?

Where is the adversary now most vulnerable to targeting, in nodal and critical element terms?

What would be the likely result of, or response to, re-attack?

Weapons effectiveness assessment

5.32 Weapons effectiveness assessments (WEA) allow commanders to receive specialist advice on the effectiveness of employed weapons. WEA information is useful in choosing more effective weapons, or fine tuning weapons for continued operations. The results of WEA from specialists in IO related capability may include the shifting of jamming aimpoint (in frequency terms), or a change in PSYOPS media, themes or symbols.

5.33 WEA is conducted in concert with BDA since the same signatures used to determine the level of physical or functional damage also provide information as to the weapons' effectiveness. The difference is that BDA is conducted from largely the adversary perspective, whereas WEA is conducted from the friendly weaponeering perspective. Hence WEA is primarily the responsibility of operations staff and specialist advisers with inputs from intelligence staff. WEA analysts seek to identify any deficiencies in the performance of the weapon and weapon system, including the tactics and procedures used to conduct the targeting activity.

WEA answers the question; "Did the force employed perform as expected?"

5.34 Once a deficiency is identified, analysts can make recommendations for procedural changes, different tactics, system modifications, or new system development. After the same weapon attacks several targets of a specific type, WEA should be used to evaluate weapon performance.

5.35 Targeted installations that are captured by friendly forces will yield detailed information on the effectiveness of weapons employed to WEA teams. Similarly human intelligence exploitation of individuals will validate the effectiveness of PSYOPS, deception and other offensive information operations. Such information could have a crucial impact on future operations and the quality of future CA.

5.36 WEA continue after conflict resolution and during weapons trials during peace to establish MOE baselines.

Re-attack recommendations

5.37 Re-attack recommendations follow directly from BDA and WEA efforts and are incorporated as part of current operations planning. They are a combined staff effort incorporating intelligence BDA outcomes, specialist WEA, legal advice, logistic and communications implications, and, most significantly, commander's direction. Operations staffs are ultimately responsible for re-attack recommendations to the commander for initiation by the relevant actioning agencies.

5.38 Re-attack recommendations provide inputs for modification of the targeting process through updates to target development, weapons selection, force application, execution and combat assessment activities. Evolving objectives, target selection, vulnerabilities, tactics and weapons are all factors in the new recommendations. Re-attack recommendations can also drive requirements for further capability acquisition or research and development.

Mission assessment

5.39 Mission assessment (MA) is an evaluation of the effectiveness of all preceding steps in the targeting process in the light of overall command guidance. MA gives commanders at all levels a broad understanding of the impact and success of targeting operations against an adversary and provides the commander scope to review, renew or re-direct targeting efforts within command guidance.

5.40 Operations staffs are responsible for MA. The questions they will answer through MA are:

Did the targeting mission achieve its objective? Was the effect on the adversary the desired effect?

Was the adversary response expected and planned for?

Does the adversary response require a shift in future targeting activity?

Did the targeting objective add to the commander's intent?

Do outstanding targeting objectives require modification?

Do the measures of performance require modification?

What changes in operational posture are now required to shape the battlespace to achieve the commander's intent?

Does a particular adversary target system require more or less emphasis in future missions?

Were there any unintended consequences such as additional or collateral damage?

Annexes:

A. IO Management Tools

IO MANAGEMENT TOOLS

IO implementation graph

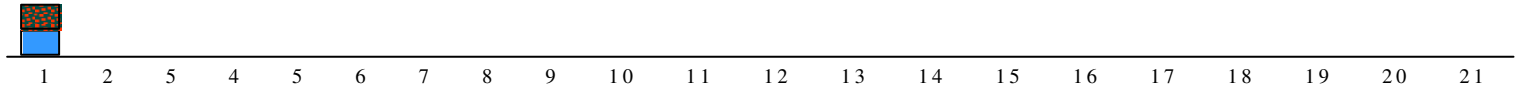
IO implementation graphs can be used to visually portray rates of effort and sequence of action. An example from NATO action in Bosnia is displayed below. Such graphs can also indicate what has happened, as opposed to what was intended to occur.

CLASSIFICATION

Name of Problem Set & Timeframe

Instructions: Copy the appropriate box from the menu below. Place the copy on the time line, above the date of the scheduled execution. Boxes can be stacked in a column to represent multiple executions on the same day. The draw/align function can be used to form straight columns.

Example



PSYOP Radio
PSYOP TV
PSYOP Print
PSYOP Loud-speaker
PA Press Con-ference
Press Release
Press Guidance
PA Radio
PA TV
POLAD Meeting
CA Contact w/Locals
CA Contact w/PVOs
CA Contact w/GOs
CA Contact w/NGOs
CA Contact w/IOs
JMC BILAT
JMC Conference
JMC Inspection
MF Town Hall Meetings
MF Contact w/ local officials
MF Contact w/local population
MF Liaison w/Foreign Military
MF on Radio/TV
MF Show of Force
SF Contact w/local officials
SF w/local population
SF w/Foreign Military

CLASSIFICATION

IOSPM

IO implementation matrix

Each element of the IO implementation graph can have explanatory notes displayed in an implementation matrix that assist in the monitoring of activity and assessment of measures of effectiveness, and can also be used to display unplanned activity as it occurs.

Category	When (Date)	Target(s)	Primary Themes (Refer to the List of Approved Themes)	Objective(s)
PSYOP - Radio Message				
PSYOP - TV Message				
PSYOP Handbill/Leaflet/Poster				
PSYOP - Loudspeaker				
Public Affairs - Press Conference				

IOSPM

Public Affairs - Press Release				
Public Affairs - Press Guidance				
Public Affairs - Radio Message				
Public Affairs - TV Message				
POLAD - Meeting				
Civil Affairs - Contact w/Local Officials				
Civil Affairs - Contact w/PVOs				

IOSPM

Civil Affairs - Contact w/Gov't Organizations				
Civil Affairs - Contact w/Non-Gov't Organizations				
Civil Affairs - Contact with International Org				
Joint Military Council - BILAT				
JMC - Conference				
JMC - Inspection				
Manoeuver Forces - Town Hall Meeting				

IOSPM

Manoeuver Forces - Contact w/Local Officials				
Manoeuver Forces - Contact w/Local Population				
Manoeuver Forces - Liaison w/Foreign Military				
Manoeuver Forces - Appearance on Local Radio/TV				
Manoeuver Forces - Show of Force				
Special Forces - Contact w/Local Officials				

IOSPM

Special Forces - Contact w/Local Population				
Special Forces - Contact w/Foreign Military				

CHAPTER 6

OPERATIONS SECURITY

INTRODUCTION

Background

6.1 Operations Security (OPSEC) is the process which gives a military operation or exercise appropriate security, using passive or active means, to **deny knowledge** of the dispositions, capabilities and intentions of friendly forces. It is a command function that involves those collective measures taken by the operational force to maintain security from generally overt and clandestine intelligence collection. It is therefore controlled and coordinated by operations staff with input from CI and other staffs. OPSEC depends on an understanding of the adversary's ability to collect information, the way information is processed, and the decision-action cycle that results from it.

6.2 Operations Security (OPSEC) is a process of identifying essential elements of friendly information and subsequently analysing friendly actions attendant to military operations and other activities to:

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

b. determine what indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive essential elements of friendly information in time to be useful to adversaries; and

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

6.3 OPSEC's most important characteristic is that it is a process that can be applied to every operation. The OPSEC process consists of five distinct actions: identification of essential elements of friendly information, analysis of threats, analysis of vulnerabilities, assessment of risk, and the application of appropriate OPSEC measures. These actions may be revisited at any time in order to update all planning processes. As such, the process is not a collection of specific rules and instructions, but more a tool for the management of the perceptions of an adversary.

6.4 In information operations (IO), the threat to OPSEC is ultimately the adversary decision-maker. Denial of essential elements of friendly information about friendly capabilities and limitations attempt to force an adversary into flawed decisions. The intent of OPSEC in IO should be to force the adversary to make decisions based upon insufficient information and/or to retard the decision-making process due to a lack of information.

6.5 Joint OPSEC planning and execution occurs as part of the command or organisation's IO effort. The commander's objectives for IO are the basis for OPSEC planning. OPSEC is an operational function, and works towards attaining the ultimate condition of Security, an ADF warfighting concept and principle of war. This relationship is displayed at Figure 5.1. Planning must focus on identifying and protecting essential elements of friendly information as articulated by the commander.

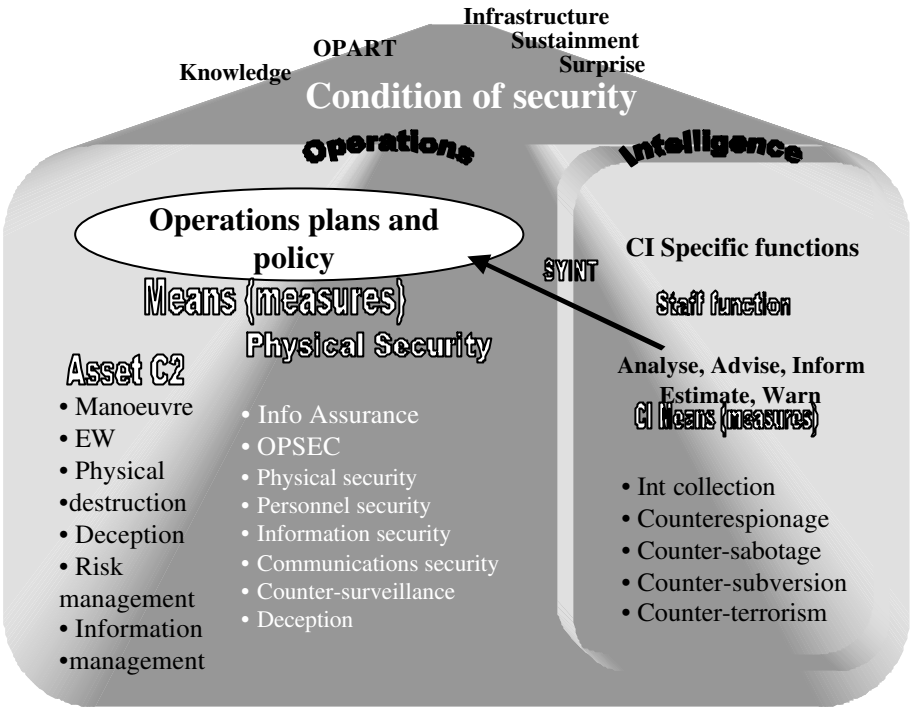


Figure 1.5 - OPSEC and the condition of security

OPSEC is a process of identifying essential elements of friendly information and denying such information to an adversary by controlling unclassified indicators that will divulge that information.

6.6 **Essential elements of friendly information**. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

a. **OPSEC Indicators**. Friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive essential elements of friendly information.

b. **OPSEC Vulnerability**. A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated in time to provide a basis for effective adversary decision-making.

Counterintelligence

6.7 There is a wide range of activities undertaken to counter adversary intelligence systems in order to maintain security or to gain surprise. Information Operations, manoeuvre, legal action, policing, physical destruction, deception, physical security, and counter surveillance all contain examples of measures that can be taken to 'counter' intelligence and are all controlled, staffed, or managed through a variety of functions. Specifically, **counterintelligence (CI) is that part of the intelligence function** devoted supporting these facets of security. It has both offensive and defensive aspects and may be directed against hostile intelligence sources and agencies and/or individuals, groups or organisations capable of conducting espionage, subversion, sabotage[5] or terrorism[6].

[5] Sabotage is used in CI terms in relation to covert attack by 'insiders' and sabotage networks orchestrated by hostile intelligence agencies, organisations, or individuals. It does not normally include external, clandestine attack by special forces and so on.

[6] Counter terrorism relates to the 'force protection' aspects of the CI function. Due to the extent of the covert nature of terrorists' daily existance and sources of supply, the ADF has adapted the British experience of linking counter terrorism to the specialist stream of CI.

6.8 The CI function is normally enacted on two levels: staff and operator. At a staff level, CI personnel will be involved with the provision of security intelligence, protective security policy advice (including input to operations security and deception) and the technical control of CI operations. At an operator level, CI personnel can provide local CI staff advice and will conduct CI operations to gather security intelligence and to counter threats from espionage, sabotage, subversion, and terrorism.

Counterintelligence and OPSEC

6.9 OPSEC is a command function that involves those collective measures taken by the operational force to maintain security. It includes those active and passive measures designed to deny hostile intelligence systems knowledge of the actions of friendly units. It is therefore controlled and coordinated by operations staff with input from CI and other staffs. OPSEC Plans focus on denying an adversary knowledge of Essential Elements of Friendly Information (EEFI) about the friendly plan, and utilise non-specialist measures such as counter-surveillance, electronic protection, physical security, and deception. On the other hand, CI Plans are directed towards the gaining of security intelligence and denying threats from espionage, sabotage, subversion, and terrorism. The CI Estimate provides the foundation for both OPSEC and CI Plans and significantly influences deception planning.

THE OPSEC PROCESS

6.10 The OPSEC planning process consists of five steps that are intrinsically linked within the Joint Military Appreciation Process (JMAP). These actions are applied in a sequential or adaptive manner during OPSEC planning. In dynamic situations, however, select actions may be revisited at any time. New information about the adversary's intelligence collection capabilities, for instance, would require a new analysis of threats.

6.11 **OPSEC planning factors.** The following factors must be considered when conducting OPSEC planning.

a. **The commander plays the critical role.** OPSEC planning guidance must be provided as part of the commander's IO planning guidance to ensure that OPSEC is considered during the development of friendly courses of action (COAs).

b. **OPSEC is an operations function.** Operations planners must do OPSEC planning, with assistance from appropriate planners from other staff elements. Intelligence support is particularly important in determining the threat to friendly operations and in assessing friendly vulnerabilities.

c. **Planning must focus on identifying and protecting only essential elements of friendly information.** Denying all information about a friendly operation or activity is seldom cost effective or realistic.

d. **The ultimate goal of OPSEC is increased mission effectiveness.** By preventing an adversary from determining friendly intentions or capabilities, OPSEC reduces losses to friendly units and increases the likelihood of mission success.

e. **OPSEC should be one of the factors considered during the development and selection of friendly COAs.** COAs will differ in terms of how many OPSEC indicators will be created and how easily those indicators can be managed by OPSEC measures. Depending upon how important maintaining secrecy is to mission success, OPSEC considerations will be a factor in selecting a COA.

f. **OPSEC planning is a continuous process.** During the execution phase of an operation, feedback on the success or failure of OPSEC measures is evaluated and the OPSEC plan is modified accordingly. Friendly intelligence and counterintelligence organisations, communications security (COMSEC) monitoring, and OPSEC surveys are the primary sources for feedback information.

g. **Public affairs officers should participate in** OPSEC planning to provide their assessments on the possible effects of media coverage and for the coordination of OPSEC measures to minimise those effects.

h. **The termination of OPSEC** measures must be addressed in the OPSEC plan to prevent future adversaries from developing countermeasures to successful OPSEC measures. In some situations, it may be necessary for the OPSEC plan to provide guidance on how to prevent the adversary as well as any interested third parties from discovering sensitive information relating to OPSEC during the post-execution phase.

JIPB: Analysis of Threats/Adversary

6.12 As part of the Joint Intelligence Preparation of the Battlespace (JIPB) process the intelligence staff will advise on adversary capability and intent, including adversary and stakeholder intelligence collection capability and potential. Operations planners, working with the intelligence and counterintelligence staffs and assisted by the OPSEC program personnel, will require answers to the following questions:

Who is the adversary? (Who has the intent and capability to take action against the planned operation?)

What are the adversary's intelligence collection capabilities?

What are the adversary's goals? (What does the adversary want to accomplish?)

What is the adversary's strategy for opposing the planned operation? (What actions might the adversary take?)

What essential elements of friendly information does the adversary already know about the operation? (What information is it too late to protect?)

Mission Analysis/COA Development: identification of essential elements of friendly information

6.13 To be effective, OPSEC measures must be considered as early as possible during mission analysis and then be revised to keep pace with any changes in current operations and adversarial threats.

6.14 While assessing and comparing friendly versus adversary capabilities during the planning process for a specific operation or activity, the commander and staff seek to identify the questions that they believe the adversary will ask about friendly intentions, capabilities, and activities. These questions are recommended by intelligence (counterintelligence) staff and extrapolated as EEFI for each course of action under development. It is only that information that is vitally needed by an adversary. The identification of essential elements of friendly information is important in that it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all sensitive information.

COA Analysis: analysis of vulnerabilities

6.15 Identifying the OPSEC vulnerabilities of an operation or activity requires examining each aspect of a course of action under development to identify indicators that could reveal essential elements of friendly information. These indicators are then compared against the adversary's intelligence collection capabilities during course of action analysis (wargaming). A vulnerability exists when the adversary can collect an OPSEC indicator, correctly analyse it, and then exploit it. Continuing to work with the intelligence and counterintelligence staffs, the operations planners seek answers to the following questions:

What indicators of essential elements of friendly information, assessed as unknown to the adversary, will be created by the execution of the course of action?

What indicators can the adversary actually collect?

What indicators can the adversary use to the disadvantage of friendly forces? (Can the adversary analyse the information, make a decision, and take appropriate action in time to interfere with the planned operation?).

Decision and Execution: assessment of risk

6.16 Planning staff analyses the OPSEC vulnerabilities identified in wargaming and determines possible OPSEC measures for each. During the decision and execution phase of planning, the commander must assess the risk to security because of the vulnerabilities and approve the execution of specific OPSEC measures to minimise the risk.

6.17 OPSEC measures reduce the probability of the adversary either collecting the indicators or being able to correctly analyse their meaning. OPSEC measures can be used to:

a. Prevent the adversary from detecting an indicator;

b. Provide an alternative analysis of an indicator; and/or

c. Attack the adversary's collection system.

6.18 OPSEC measures include any action tailored to protect overt indicators and can include such actions as cover, concealment, camouflage, deception, international deviations from normal patterns, and direct strikes against the adversary's intelligence system. More than one possible measure may be identified for each vulnerability. Conversely, a single measure may be used for more than one vulnerability. The most desirable OPSEC measures are those that combine the highest possible protection with the least effect on operational effectiveness. Each of the standard OPSEC measures noted below exist in their own right and may perform other functions. However, they are the most often used to protect the indicators that give away EEFI:

a. personnel security,

b. physical security,

c. information security,

d. EP,

e. counter-surveillance, and

f. deception operations conducted to maintain security.

6.19 Risk assessment requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability. OPSEC measures usually entail some cost in time, resources, personnel, or interference with normal operations. If the cost to mission effectiveness exceeds the harm that an adversary could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires command involvement. Typical questions that might be asked when making this analysis include the following:

a. What risk to effectiveness is likely to occur if a particular OPSEC measure is implemented?

b. What risk to the mission is incurred if an OPSEC measure is not implemented?

c. What risk to the mission is incurred if an OPSEC measure fails to be effective?

6.20 The interaction of OPSEC measures must be analysed. In some situations, certain OPSEC measures may actually create indicators of essential elements of friendly information. For example, the camouflage of previously unprotected facilities could be an indicator of preparations for military action. The selection of measures must be coordinated with the other components of IO. Actions

such as jamming of intelligence nets and physical destruction as well as PSYOP plans may require that OPSEC measures not be applied to certain indicators in order to project a specific message to the adversary. The commander is ultimately responsible for making the decision on how much risk to accept.

Application of appropriate OPSEC measures

6.21 In this step, the command implements the OPSEC measures or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans. During the execution of OPSEC measures, the reaction of adversaries to the measures is monitored to determine their effectiveness and to provide feedback. Current operations planners use that feedback to adjust ongoing activities and for future OPSEC planning. Provisions for feedback must be coordinated with the command's intelligence and counterintelligence staffs to ensure that the requirements to support OPSEC receive the appropriate priority. In addition to intelligence sources providing feedback, OPSEC surveys can provide useful information related to the success of OPSEC measures.

6.22 Feedback between and within each step of the process is vital to effectively protect essential elements of friendly information and eliminating indicators.

SURVEYS

6.23 The purpose of an OPSEC survey is to thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists. Ideally, the operation or activity being surveyed will employ OPSEC measures to protect its essential elements of friendly information. The OPSEC survey is used to assess the effectiveness of the measures. The survey will determine if the essential elements of friendly information identified during the OPSEC planning process are being protected. A survey cannot be conducted until after an operation or activity has at least identified its essential elements of friendly information. Such information is necessary to make a determination that OPSEC vulnerabilities exist.

6.24 In combat, a survey's emphasis must be on identifying operational indicators that signal friendly intentions, capabilities, and/or limitations and that permit the adversary to counter friendly operations or reduce their effectiveness. In peacetime, surveys generally seek to correct weaknesses that disclose information useful to potential adversaries. Many activities, such as operational unit tests, practice alerts, and major exercises, are of great interest to a potential adversary because they provide insight into friendly readiness, plans, crisis procedures, and C2 capabilities. Such insights can contribute to that adversary's long-range planning.

6.25 **Types of surveys**. There are two basic kinds of OPSEC surveys, command and formal. A command survey is performed using only command personnel and concentrates on events within the particular command. A formal survey requires a survey team composed of members from inside and outside the command and will normally cross command lines (after prior coordination). Careful prior planning, thorough data collection, and thoughtful analysis of the results are the key phases of an effective OPSEC survey.

CHAPTER 7

DECEPTION

Though fraud in other activities be detestable, in the management of war it is laudable and glorious. He who overcomes the enemy by fraud is as much to be praised as he who does so by force. Machiavelli

SECTION 7-1 DECEPTION

7.1 Deception has always been a crucial facet of warfare. It is a significant false multiplier, creating doubt and forcing an unwarranted expenditure of resources and effort by an adversary. Deception seeks to influence the mind of the adversary commander. It therefore requires an intimate knowledge of the adversary commander, a clear concept of operations, a clear deception objective, and a high standard of operations security (OPSEC). Recent examples of the successful use of deception show that it still has great utility despite the sophistication of modern surveillance and intelligence collection systems. The human mind is today no less susceptible to deception than in the Stone Age.

7.2 Successful deception invokes two principles of war: security and surprise. The requirement for deception is thus derived from a desire for security or a need to achieve surprise.

Security. Security is a function of command and includes all those measures taken by a command to protect itself from espionage, observation, sabotage, annoyance and surprise. Security denies information to an adversary and retains for the commander the ability to employ his forces more effectively. Deception may be required to assist in the protection of capability and intent from an adversary's collection system.

Surprise. The ultimate objective of deception is the achievement of surprise. It is not essential that an adversary be taken unaware, but only that he becomes aware too late to react effectively. If a commander is to achieve surprise, he must plan to fulfil two requirements: *conceal* the true (security) and *reveal* the false (deception).

SECTION 7-2 THE DECEPTION PLANNING PROCESS

The deception planning process in overview

7.3 The deception planning process commences when the commander is issued with a directive or conceives of the need to undertake an operation. The requirement for deception arises from the commander's appreciation of the need for surprise to shape the battlespace or it may arise from the security needs of emerging courses of action in the Joint Military Appreciation Process (JMAP).

7.4 The steps in the deception planning process (also known as conducting a deception appreciation) are:

a. determine the desirability, feasibility and credibility of a deception operation;

b. determine who to deceive (the deception target);

c. determine the deception objectives (what the deception target is to do or not to do);

d. conduct a deception appreciation to determine what the enemy is to perceive in order to react according to the commander's intent (the deception story);

e. develop the outline plan into a full deception plan by applying resources and systematically analyse operations plans to decide what aspects are to be hidden and what false information is to be presented (deception methods and techniques);

f. incorporate deception requirements into the OPSEC plan, counterintelligence plan, collection plan; and

g. commander approves plan.

7.5 After approval the plan moves to the implementation stage. This involves the:

a. allocation of troops to tasks and preparation of orders;

b. issue of orders;

c. execution of the deception activities;

d. monitoring of the effectiveness of OPSEC measures;

e. monitoring of the effectiveness of the deception;

f. assessing of the need for remedial action;

g. deciding whether to continue, adjust or abandon deception operations; and

h. termination of the deception.

Deception and the joint intelligence preparation of the battlespace process

7.6 The joint intelligence preparation of the battlespace (JIPB) process provides an analysis of the operational environment and an intelligence estimate.

7.7 **The analysis of the operational environment.** The analysis of the operational environment contains analysis of all information related to oceanic, continental, aerospace, littoral, electromagnetic, social, political, cultural, religious and economic factors that influence and constitute the battlespace. The significance of how these factors affect the battlespace on military operations is also assessed. This analysis is applied to deception planning in the consideration of:

a. the effectiveness of each of the available deception techniques and measures; and

b. the channels available for conveying the deception story to the adversary through his intelligence collection and surveillance sources.

7.8 **The intelligence estimate**. The intelligence estimate provides an assessment of the adversary's most likely course of action (COA). It is therefore the nearest available approximation to what the adversary will do in reaction to the friendly force and the adversary's expectation of friendly activities. The estimate will also provide:

a. An assessment of the adversary's strengths and weaknesses.

b. Guidance on the level of adversary commander in position to control the battle. The commander who is the focus of the Estimate will often be the target for any deception activities.

7.9 **The counterintelligence estimate**. The counterintelligence (CI) estimate is a systematic appreciation of the friendly operational plan and its vulnerabilities, relative to the adversary's intelligence collection capabilities and threats from sabotage, terrorism and subversion. It is conducted by the counterintelligence (CI) component of the intelligence staff. Significantly, the CI staff will assess the vulnerability of the adversary's intelligence collection system to manipulation through deception. The enemy's strengths, weaknesses, critical nodes and intelligence acquisition systems will determine the deception means to be covered by the friendly deception plan. The CI estimate will provide the deception planners with detail on:

a. the adversary's intelligence collection and surveillance capabilities;

b. the adversary's employment and deployment of his collection means;

c. the threat these present to the friendly forces and plans and to the detection of their real activities;

d. the threat posed to the deception by the adversary's collection activities; and

e. recommended countermeasures in the form of deception, OPSEC measures, and physical security.

7.10 **Collection planning**. JIPB and commander's intelligence requirements leads to the development of the friendly intelligence collection plan and to a large part of the surveillance plan. The collection plan is designed to collect the indicators of the adversary activity in order to confirm, refute or modify the most likely adversary COA deduced in the estimate. When a deception operation is to also be conducted, the collection plan has to be expanded to include:

a. the collection of the information that is needed to monitor the adversary's receipt of the deception indicators;

b. the collection of indicators that the adversary is reacting, or not reacting, to the deception story in the way desired; and

c. the collection of details about the adversary's intelligence collection and surveillance resources, their operating status, location, reporting systems etc.

Deception and the JMAP

7.11 The JMAP (see Chapter 4) has three important connections with the deception planning process:

a. The JMAP may come up with a most desirable course of action (COA) that cannot be achieved unless the adversary is deceived. It can thus identify the need for deception and the deception objectives.

b. The JMAP will identify a number of feasible COA to the friendly force. Since all of these are feasible they have the essential element of credibility to be used as the basis of the deception story.

c. The JMAP sets the time frame for the deception. Deception planning staff (if formed) act integrally with plans staff. Much of the operations planning deliberations will be directly relevant to the depiction of the deception story as the story takes on the character of the friendly concept of operations.

7.12 The following table shows the concurrent activity and the responsibilities of staff elements whether a special deception staff is created or not.

JMAP	**Operations and intelligence planning**	**Deception Planning**
Mission Analysis and JIPB	Mission and desirability of Deception (Comd) JIPB – AOE Intelligence Estimate (Level of adversary command) (Int) Mission Analysis (ops/plans)	 Potential deception targets. Vulnerabilities in adversary collection systems. Desirability, feasibility and credibility of deception.

	Commander's Guidance (Comd/Ops)	Desired enemy action (deception target and deception objective) (Comd)
COA Development	Critical vulnerability analysis (ops/plans) JIPB – Intelligence estimate development and CI estimate (Int) (adversary collection capabilities) Develop potential COA and lines of operation (ops/plans) Assign available resources to each COA (ops/plans)	Deception target vulnerabilities Deception story for each potential COA (staff) Determine appropriate deception means, measures and technique to propagate deception story.
COA Analysis	Conduct wargame (staff). Determine commander's decision points (ops). Shape collection plan (int).	Determine measures of effectiveness (MOE) of the deception. Plan for potential branches and sequels. Steer collection plan and determination of indicators.
Decision and Execution	Commander's decision on COA. (Comd) Prepare and dispatch orders (Ops)	Deception plan and outline schedule presented. Deception tasks and detailed schedule. Prepare deception orders.

Deception and communications

7.13 In the context of the conduct of a deception operation, communications have to perform five functions:

a. The force has to continue to operate and to prepare for future activities. Communications are required to support the command and control of the force in the normal way.

b. The communications picture that supports the deception story has to be generated.

c. Those communications that would reveal the actual operations, and so compromise the deception operation, have to be concealed.

d. The communications of the friendly force have to be monitored to ensure that the desired electronic indicators are available to the enemy and that indicators that would compromise the deception are denied to him.

e. The adversary's communications have to be intercepted to determine that he is receiving the indicators and reacting to them in the desired manner.

SECTION 7.3: DESIRABILITY, FEASIBILITY AND CREDIBILITY OF DECEPTION

Desirability

7.14 The criteria for employment of deception includes:

Will it lead to surprise?

Will it achieve decisive results?

Will it reduce casualties?

Will it save time?

Feasibility

7.15 Prior to planning, the feasibility of deception is determined by examining the following:

a. the degree to which the commander's plan is dependent on successful deception,

b. the opportunity to achieve deception,

c. the susceptibility of the adversary to deception,

d. the likely enemy reaction to deception,

e. the time available to achieve the deception, and

f. the degree to which resources can be diverted to the deception.

7.16 **Criticality to the commander's plan**. It is often not be desirable to depend on deception for success, but in some situations the only way to achieve the mission with the available resources and in the desired time will be to significantly, alter the balance of forces at a point in the battle. This will form part of the risk the commander is willing to sustain and should be highlighted early in planning. Conversely in a situation where the achievement of surprise will have no material effect on the conduct of the battle, the expenditure of resources on deception may be deemed a waste.

7.17 **Likely adversary reaction and susceptibility to deception.** Deception operations must be tailored in each case to the enemy's unique character and conditions. The consequences of adversary likely response options to the friendly plan must be taken into account before deciding to proceed with deception. If the enemy can react in a way that would place the real friendly plan in jeopardy, the deception may have to be rejected as a dangerous course to follow. From an adversary perspective the intelligence staff will assess:

a. the quality of the enemy's intelligence,

b. the likely intelligence architecture,

c. adversary perceptions,

d. cultural framework,

e. operational situation and flexibility of response,

f. the ways in which the enemy might react to the deception,

7.18 **Opportunity for deception.** To achieve a deception objective, a command must have a number of potential options that the adversary has the capability to assess as likely to occur. The deception story can then be enacted by displaying indicators of an alternative COA that forces the

adversary to react or not react according to the requirements of the deception objective. These multiple, feasible courses of action are derived during the COA Development process.

7.19 **Time available**. There has to be sufficient time for the deception to be planned, prepared and executed and for the adversary to act on it. There must also be time to establish a collection capability to assess the adversary reaction, to collect information on adversary indicators, to process that information and to react to it by the time the deception is achieving the desired effect. Initial planning guidance must determine the key timings in the design for battle and indicate the time available until the deception has to take effect. The intelligence staff can assess the time needed to pass deception indicators to the enemy and for a reaction to occur Thereby planners can conduct a gross check to determine if there is sufficient time for deception. If sufficient time is not available then launching any complex deception is a waste of effort.

7.20 **Resource availability**. Even if the effectiveness of deception is beyond question, the cost of applying it should not be underestimated. Every attempt at deception implies a penalty in terms of manpower time, equipment, training for the specific skills required and the logistic effort needed to support it. The penalty increases as the level of the deception target and duration of the deception increases and the cost effectiveness of the diversion of these resources needs to be carefully assessed. Moreover, the necessary time sensitive coordination and centralised control required for successful deception may make deception difficult in situations where commanders do not have control over all the deception means available.

Credibility and excessive and repetitive use of deception

7.21 While it is laudable to seek to achieve surprise in every military operation, the dogged adherence to the principle can be counter-productive. An adversary who is alert to the possibility of surprise in every operation will proceed cautiously and the enemy commander who has been conditioned to expect surprise all the time will have already overcome the actual shock of the unexpected.

7.22 As a result of the expectation of deception, the adversary may be more cautious and hesitant to act without overwhelming evidence. This may benefit the friendly commander, as a hesitant opponent who delays decisions might be easier to handle. However, a cautious adversary may act with greater certainty and stronger resources. An audacious opponent who takes risks may be easier to defeat than a cautious enemy as he would be easier to deceive.

7.23 As well as the conditioning effect on the enemy of repetitive deception, a constant requirement to produce a deception aspect in every operation will exhaust the flair and inventiveness of the friendly deception planners. Deception stories may become repetitious variations on a few themes, which will become predictable. Reliance on a few deception techniques that have been successful may produce a pattern that is also predictable. And once deception becomes predictable it becomes ineffective and can be turned to the adversary's advantage.

7.24 The repetitive and routine use of deception by the Soviets against the Germans during World War II ran this risk. It was largely the arrogance of the high level German commanders, who tended to follow their own preconceived conclusions, almost without regard for the actual evidence, and the fragmentation of their intelligence systems, that allowed the Russians to continually achieve operational surprise through deception.

SECTION 7.4: THE DECEPTION TARGET

Whom to target

7.25 The determination of who to target with deception is not as simple as it may appear. The level of command that can affect the required response needs to be carefully selected. Often the deception target is the mind of the adversary commander who has the span of responsibility and authority to make the decisions and order the actions that will comply with the deception objectives. On the other hand, the target may not be obvious as, for example, the opposing commander may be significantly constrained by higher authority. Moreover, several targets may be selected to provide the corporate response, or lack of response, required.

Adversary intelligence system

7.26 The principal channel for information to reach the deception target is the adversary intelligence system. Hence a significant piece of the assessment of the target is the accessibility, credibility, reliability and capability of the target's intelligence feeds. If a piece of information does not attract the attention of the adversary intelligence staff it is unlikely to get to the commander in a form that will be seen as sufficiently significant to react to. Moreover, the relationship of the principal intelligence staff officer to the commander and the credibility and reliability of the adversary intelligence staff are also important factors to consider.

SECTION 7.4: DECEPTION OBJECTIVES

7.27 The commander's intent will include direction on how he wants the battlespace shaped, including how adversary action is to be made to conform to the plan. He will therefore provide to his staff a broad statement of what the commander wants the adversary to do or not do. These assessments and requirements will be refined as the JMAP process unfolds. An examination of the likely and desired enemy action, in the context of the proposed friendly operation, will then indicate:

a. what actions will be forced on the adversary by the actual friendly operations,

b. where it would be desirable for the adversary to carry out actions to his disadvantage, and

c. those adversary actions that would place the commander's plan in jeopardy if they were to occur.

7.28 Based on these assessments the deception planner can determine the perceptions that have to be created in the enemy commander's mind in order to influence him along the desired lines. Staff thus develop a statement specifically dictating what actions the deception target is to take or not to take, at a given time and place within the battlespace. This statement is known as the deception objective. Along with the deception objective staff will detail the key aspects of the friendly plan that are to be protected from discovery by the adversary, known as essential elements of friendly information (EEFI).

7.29 Deception objectives should be explicitly stated and agreed by the commander, as they are what deception operations are to be designed to achieve and they are the bases for making judgments on the effectiveness and continuation of the operations once launched. For example, "The Kamarian JTF commander is not to attempt to reinforce the X Island garrison until 18 Oct XX."

SECTION 7.5: THE DECEPTION STORY

The process

7.30 The deception story is the friendly intention, capability, or disposition, which the adversary is to be made to believe is true. It is the picture of reality that the enemy is to conclude, as a result of his intelligence system collecting and processing the false information that is provided. It is the focus for the planning of the deception operation.

7.31 From the derivation of a deception target and objective, deception planners then conceive the deception stories that may achieve the objectives by influencing the target. The preferred deception story will then be selected based on a consideration of factors such as accessibility of the target, time, availability of means, and resources. A deception planning checklist is provided at Annex A to assist this process.

The possible deception stories

7.32 **The Commander's choice.** The commander's consideration of the situation and his design for battle, may enable him to give a clear indication of what he expects the enemy commander to believe is happening. In simple tactical situations where the choice of friendly courses is limited, this may be merely a matter of his indicating what his proposed course will be and that he wants the enemy to believe the friendly intention is to follow the course that is least like the actual plan.

7.33 **Rejected friendly courses.** Examination of the operational appreciation will identify courses of action that are feasible but have been rejected. These will have the advantages of credibility and some work may have been done on the elements of the operation that would be required to put them into effect.

7.34 **Adversary expectations.** The enemy's intentions (as assessed in the Intelligence Estimate) or his dispositions may also indicate the course of action he is most expecting. If this is not the chosen friendly course the deception story can be built around it to exploit the enemy's preconceived idea. If it is the same as the friendly plan then the commander may adjust his plan or it may be necessary to adjust the enemy commander's perceptions through the deception.

Selecting the best story

7.35 **Principle's of deception stories** To be effective a deception story must be:

Realistic. Realism involves ensuring that the story is consistent with the reality of the situation, at least as far as the adversary's perception of the situation can be determined.

Plausible. To be plausible, the story must accurately match the adversary's estimate of the factors that he will consider. It must be logically consistent with the way in which the friendly force normally acts. For example, the environment must appear to provide for the course of action being portrayed. The story must accord with the capabilities and dispositions of the friendly force. These capabilities and dispositions must be as they are assessed by the adversary and be compatible with his background intelligence on the friendly order of battle and his knowledge of recent activity on the battlefield.

Verifiable. The story has to be such that it can be detected by the adversary's intelligence collection means and cross-checked by several sources to determine it to be true. A story, which can only be portrayed through one source, will often be dismissed or overlooked.

Simple. The more complex the deception story, the more time and means will be required to portray it and the more difficult it will be for the adversary to piece it together. The simpler the story can be kept the more likely it is that the enemy will be able to put it together accurately.

7.36 **Factors considered in developing the story.** The following factors are considered in developing a deception story:

Factor: The Target. Further examination of the **deception target** and consideration of target characteristics is conducted.

Factor: Adversary's dispositions, intentions and capabilities. This must establish:

(1) what the adversary probably expects the friendly force to do;

(2) what adversarial response is likely as the deception unfolds; and

(3) what the deception target's reaction will be to the discovery that he has been subject to a deception.

Factor: Deception means available. This review ensures that generally the means is available to affect the vulnerabilities in the adversary collection system. Advice will be drawn from basic intelligence material and the counterintelligence (CI) estimate.

Factor: Time. The most important factor is time. The timing of the deception has to be keyed to the timings of the real operation with the sequencing of the deception activity built back from the time by which the deception objectives have to be in effect. In cases where the achievement of the deception is critical to the success of the real operation, it may be necessary to adjust the real operation's timings to allow for the deception to be effective.. Time must be considered from both the friendly and enemy perspective's as follows:

(1) **Friendly.** Consideration of time from the friendly point of view must:

(a) determine the desired duration of the deception;

(b) determine the time to initiate and terminate each deception action;

(c) determine the time at which friendly action will unequivocally compromise the deception;

(d) determine the duration of likely effectiveness of the deception operation; and

(e) determine the time to initiate real activity.

(2) **Target.** Consideration of time from the target point of view must:

(a) determine the time the target will require to collect and process the intelligence;

(b) determine the time for the target's staff and decision cycle to react to the intelligence;

(c) determine the time for the target to enact the desired action; and

(d) determine the time at which the target will be at the most disadvantage.

Factor: Resources available. Consideration of the means of portraying the elements of the deception will indicate what actions are required. Earlier consideration of the availability of resources in relation to the execution of the real operation (during the JMAP) will have identified what is available. These two aspects have to be matched in the outline deception plan. The deception tasks have to be assigned to the forces that can be made available and:

(3) whose ongoing actions can make their deception activity seem a logical continuation of their current activities, and

(4) whose simulated situation at the end of the deception will appear logical and related to their actual situation on the battlefield.

Portraying the Deception Story

7.37 The portrayal of the story is achieved by the conduct of a number of deception activities, both real and simulated, which collectively represent the events that would be necessary to carry out the course chosen as the basis of the story. Each deception event will display an indicator of friendly actions or intentions as an element of the story.

7.38 Portraying the elements of the story, however, is only one part of the conduct of the deception operation. It is equally important that the plan includes those elements that have to be denied to the adversary because they:

a. would reveal the real plan, and/or

b. would discredit the false story.

SECTION 7.6: DECEPTION MEANS

General

7.39 A deception operation consists of one or more deception techniques utilising one or more deception measures to portray indicators of a deception story, through the various deception means, to convince a deception target to carry out the deception objective.

Indicators, patterns and signatures

7.40 **Signatures**. A signature is an object or electromagnetic emission that, singularly or in combination, identifies a military entity. A signature can be an identifier of a generic type of military unit, headquarters, equipment or installation or it may uniquely identify a particular entity. Signatures are detected because equipment's have different physical and operating characteristics. Various units have different equipment, are of different size, emit different electronic emissions, and have different noise and heat sources. A number of signatures when found together can identify a unit or installation or indicate an activity. The types of signatures are:

a. visual,

b. acoustic,

c. infrared,

d. electronic, and

e. chemical.

7.41 **Activity Signatures** In addition to holdings of signature equipment, facilities, units, formations and headquarters can be identified by the way they carry out particular activities. These are often embodied in the unit's Standing Operating Procedures (SOP) and are practiced until they become the routine battle procedure of the unit. They are often unique to a particular unit reflecting the individuality of the unit's commander. When observed, the routines, procedures, layouts, groupings and sequences of activity are signatures of the unit and indicators of the activity it is undertaking or contemplating.

7.42 **Indicators**. An indicator is an object or event that, singularly or in combination, indicates the activities and/or intentions and plans of a military force. In preparing for and conducting military activity it is impossible to avoid generating indicators. In order to use indicators to the advantage of the friendly force it is necessary to recognise what is an indicator and what interpretation can be placed on it. Some indicators or combinations of indicators are directly related to various types of operations. When these are seen it will lead the opposing intelligence staff to put particular interpretations on the events it observes; or thinks it observes.

7.43 **Profiles**. Each unit has a number of signatures and indicators which it displays as it goes about each type of activity. The combination of these provides a picture of the unit, or headquarters or installation, that uniquely identifies it and can point to the activity it is undertaking.

7.44 **Patterns**. Patterns are the way military activities are carried out. Military forces develop standard procedures for most activities which place the various facets of the activity in relation to each other in time and space. Intelligence staffs plot these patterns and develop 'templates' or analytical models and use these as the framework into which they fit the information they receive in order to deduce the activity and intentions of their opponent.

Deception means

7.45 The channel used to provide information from the deceiver to the target is the deception **means**. This channel includes both the adversary's means of intelligence collection and the friendly force's means of conveying the deception. The conduct of deception therefore requires the provision (or denial) of information to the target's intelligence collection resources – the target's sources and agencies - through a channel which consists of:

a. the carrying out of the action or display of the object by the friendly force;

b. the detection of the event or object by the target's intelligence means - agents, surveillance, reconnaissance, and observation systems, and the target's equipment, processes and personnel;

c. the conveying of the report of the observation to the target's intelligence processing staff;

d. the integration of that report into the intelligence being developed by the target intelligence staff; and

e. the reporting of the intelligence assessment to the decision maker/commander.

7.46 **Target sources and agencies**. The adversary or target sources and agencies will be addressed in the CI estimate process and can be further developed by the intelligence staff on direction.

SECTION 7.7: DECEPTION MEASURES

7.47 The deception **measures** are the actions taken to provide the target's intelligence collection means with information in a way that can be received by these senses and sensors, and in the form they are designed to collect. The pieces of information provided to the target should be directed to fulfil the target's intelligence requirements, upon which he will base his assessment of what is the friendly commander's intentions. They may also be information he is not seeking but which has to be brought to his attention in order to convince him of the deception story.

7.48 **Categories of deception measures**. The measures employed to convey elements of the deception story to the target's intelligence / information collection means are:

a. visual,

b. sonic,

c. olfactory,

d. technical sensors,

e. electronic and communications,

f. human, and

g. documentary.

Visual

7.49 Effective visual deception is critical to the projection of the deception story. Visual evidence alone will not usually deceive an adversary, however, its absence will seriously jeopardise the integrity of the other deception measures.

7.50 Much of the adversary's intelligence is based on what is observed on the ground or seen in imagery and, despite technological advances, visual observations and aerial photography continue to be important sources of information. This is especially true at the lower levels of command where sophisticated electronic equipment is not available or is not present in sufficient quantities to cover the area of operations. Examples of visual deception measures include the employment of such things as dummies, decoys, camouflage, and smoke and the portrayal of false positions.

7.51 **Dummies and decoys.** Two items commonly used in visual deception are dummies and decoys. A dummy is a physical representation of something on the battlefield. A decoy is used to draw the attention of the adversary away from a more important area. Dummies can be used as decoys. It is not necessary to have specially made equipment to conduct visual deception. Dummies can be constructed from available stocks, waste materials or salvaged equipment. The distance, both on the ground and from the air, from which the adversary can observe the items or action dictates the degree of realism required. Augmenting dummy with real items also enhances realism. A mix will also add confusion and difficulty to the adversary's attempts to deduce the actual situation, since he has to detect all items in order to determine which are real and which false. Realism is also enhanced by having supporting evidence with the dummies and the scene should be dynamic.

7.52 **Use of camouflage.** As it would be normal to use camouflage, it should appear in a dummy position and on decoys and dummy equipment. Poor camouflage can be used to ensure that the deception is revealed and to add to the realism by making the enemy intelligence analyst 'find' the indicators.

7.53 **Use of smoke.** Smoke may be used with dummies and decoys to simulate activities that would normally produce smoke. Smoke can be used to screen the sites of real activity or installations, to add to the simulation of false activity by screening a probable site without an actual display, and to simulate ground haze or mist when visibility and the tactical situation may unmask decoys.

7.54 **Use of alternative positions.** Previously prepared or alternative positions can provide a ready made basis for depicting an occupied part of the friendly defensive layout. The movement of troops and equipment between alternative positions while leaving dummies in both positions can add to the realism of the depictions. It also indicates a much larger force than actually is in occupation and can cause the enemy confusion as he searches for the true picture.

Sonic

7.55 Sonic deception is the projection of sounds to produce battlefield noises. It is directed against the adversary's sound ranging equipment and the human ear. Sonic measures are used to convey to the adversary the identifiable sounds of a specific activity in accordance with the deception story.

7.56 Sonic measures should be accompanied by visual measures as the adversary will seek to confirm what is heard with other sensors. Sonic measures are generally more effective at night or when the point of origin is obscured by natural terrain or weather or by artificial means such as smoke.

7.57 Sonic deception can be applied to various activities such as vehicle movement, construction work, and defensive digging. It is also possible to use explosives to simulate firing and the fall of fire.

7.58 The following considerations apply to the use of sonic deception:

a. Although a person can recognise several different sounds arriving simultaneously, the estimate of the distance to the source is unreliable. The receiver deduces that a sound rising in pitch is coming towards him and that one lowering is going away.

b. A false sound by itself will seldom be successful. It is necessary to blend true sounds with those reproduced artificially.

c. The less effective the adversary's visual observation, the more effective will be the projection of sonic deception measures.

d. The range of sound depends on climatic conditions, vegetation and topography. Although distances cannot be predicted, conditions in which sound carries best are low temperatures, high humidity, wind in the right direction and across water surfaces.

e. Deception and counter surveillance measures must be integrated, and sounds that will indicate the true operation must be suppressed or swamped with false sonic indicators.

Olfactory

7.59 Olfactory deception is usually aimed at the adversary's collection of intelligence by close human reconnaissance. Applications of olfactory measures are generally limited to a small area where close reconnaissance by the adversary is possible or where adversary agents are likely to gain access. However an adversary may be equipped with special chemical/odour sensing and analysis machines that can extend the range at which he can collect olfactory evidence. In these circumstances a deception that indicated an occupied area could be faulted if it did not also cover the projection of olfactory/chemical indicators.

7.60 Imagination is required to represent the appropriate olfactory signatures. Some considerations for the effective use of battlefield odours are:

a. The smells projected must be consistent with the visual, sonic and electromagnetic measures being used. They will usually be complementary to the main deception measure.

b. Olfactory measures are affected by climatic conditions.

c. The olfactory signatures of true operations must be either controlled or swamped by stronger false odours.

Technical sensors

7.61 What is seen in the visual spectrum must be supported by displays that can be detected by the non-visual surveillance devices. An apparently metal object must display a similar radar picture. A supposed heat source should have an infra-red signature.

Electronic and communications measures

7.62 The array of modern electronic surveillance devices and the interception of the electromagnetic spectrum for the purposes of collecting intelligence make it essential that any deception operation consider the use of electronic measures. Since, military operations are often dependent on the use of communications, the use of appropriate levels of communications activity must be considered in all deception activity. Even if active measures are beyond the resources of the level contemplating the deception, passive measures must be undertaken and what is emitted must be closely controlled.

7.63 **Electronic deception**. Electronic deception is the deliberate radiation, re-radiation, alteration, absorption or reflection of electromagnetic radiation to mislead an adversary in interpreting data received by his electronic equipment, and to present false indications to electronic systems. The projection of false electronic evidence is carried out by technically trained operators working intimately against specific adversary devices and operators. The detail of the specifications of the adversary equipments and their operating procedures will be provided as classified materials for use by the specialist units. Deception planners should be generally aware of the techniques.

7.64 **Categories of electronic deception.** There are three categories of electronic deception:

a. **Manipulative electronic deception.** Manipulative measures are defined as the alteration of real friendly electromagnetic radiation to accomplish deception. Activities include:

(1) **Controlled breach of security.** An apparent breakdown or violation of communications security. This may be introduced as 'operator' chatter, as well as in formal messages.

(2) **Traffic volume manipulation.** False messages can be added to the traffic on a system when the number of real messages is low, and then reduced when the real traffic level increases.

(3) **Traffic direction manipulation.** False messages can be used to adjust the number of apparent messages flowing in particular directions on a net.

(4) **Net signature manipulation.** The movement, or non-movement, of a force can be simulated by the disposition of the unique communications net of that force.

b. **False Order of Battle.** Additional communications facilities can be used (if they can be resourced) to represent a larger and/or more diverse friendly order of battle than actually exists.

c. **Imitative electronic deception.** Imitative measures are defined as the introduction of radiations into adversary channels which imitate the adversary's emissions.

d. **Simulative electronic deception.** Simulation is the creation of electromagnetic emissions to represent friendly notional or actual capabilities in order to mislead hostile forces. Examples are operating false radio nets, generating radar emissions and radar swapping.

7.65 **Non communications.** The enemy uses non communications systems as part of his surveillance, target acquisition and navigation systems. These devices provide information to the adversary's intelligence system and therefore have to be incorporated into any deception operation. Techniques that may be used as part of the deception of these devices and systems are:

Reflection. Deception by reflection is a means of reflecting the electronic illumination of a target (such as by radar) in a way that indicates the signature of a specific equipment or object. This technique is used to indicate the presence of objects that are not actually there and can be very effective in conjunction with dummies of the actual objects.

Repeaters. Repeaters are technical devices that are triggered by the illuminating radar and which emit a return pulse at a different frequency. This introduces a false return to the enemy device and can lead it to mislocate the target.

False target generation - Spoofing. It is possible to use friendly radar emissions to produce false radar readings which indicate the presence of specific equipment such as tanks and aircraft where none actually exist.

Signature manipulation. Non communications electronic equipments are often signature indicators of a particular facility, unit or group, or a particular disposition. The enemy can therefore be led to believe that the force has moved or not moved by observing the actions of the signature equipments. The deceiver can implement this technique by replacing the equipment normally associated the force with a replica thereby, having the signature equipment act independently to portray the deception and marry up with its parent unit(s) later.

Counter targeting techniques. Several technical techniques exist to spoof targeting radars and provide them with false signals that frustrate their ability to accurately locate and track their targets. While essentially self defence devices their use as support to a deception activity, such as with decoys should be considered.

Concealment. Devices such as CHAFF can be utilised to screen actual activity, to confuse enemy surveillance or to inject the impression that something is going on when it is not. Their use in the electromagnetic spectrum is not unlike the use of smoke in the visual spectrum and the two may have to be used together if both visual and electronic surveillance is to be deceived at the same time.

Human source deception

7.66 The use of people to convey elements of the deception story to the adversary involves four types of human sources:

a. the prisoner,

b. the casual source,

c. the agent, and

d. the body.

7.67 **Prisoners.** A friendly soldier who becomes an prisoner is regarded by an adversary as a valuable source of both short term tactical information and information that may be of longer term

operational and strategic importance. The control of the information the prisoner provides to the enemy under interrogation, however, is difficult. The best prisoner source will therefore be one who recounts to his captors what he was doing or saw without knowing it is a deception. Personnel who are aware of the nature of the deception should be protected from capture or exploitation. Although it may be good fiction to plant a prisoner to spread a false story, it would place the integrity and security of the deception in grave jeopardy.

7.68 **Casual Sources.** Non military personnel who are in a position to observe events or objects that are part of the deception and to pass their observations on to the enemy are a valuable corroborating means of supporting the deception story.

7.69 **Agents.** Enemy agents can be important means of conveying elements of the deception story under three circumstances:

a. Where the identity of an agent is unknown, but his presence is suspected, false information can be made readily available so that he is able to collect it in his normal way.

b. Where the agent is known he can be provided with false information in the same way as an unknown agent. In this case there will be a better knowledge of what is actually getting to the enemy.

c. Where the agent is known and turned, into a double agent he can be provided with false information with certainty that it is getting to the enemy in a form and detail under control of the deception director.

7.70 **Bodies.** People have been used as important elements in deception operations when it has been important to enhance the credibility of the deception story with tangible evidence. General Patton was used to give credibility to the existence of the First Army Group. In 1943, the deception operation, Operation Mincemeat (the basis of the story - The Man Who Never Was), involved use of a dead body to give credibility to documentary evidence that the Allies would invade Sardinia, when their real target was Sicily.

Documentary Deception

7.71 A captured document carries high credibility. Above all it must appear genuine and contain information that can be substantiated by other means. The credibility is further enhanced if it comes into the target's hands in a plausible way.

7.72 Considerable care has to be exercised in the use of this type of measure to ensure that the adversary does not get the information too easily. Too gratuitous a provision of a document that contains a large amount of information would be counter productive if it alerted the adversary to look more closely into its authenticity.

Control of Deception Measures

7.73 It may not be practical or appear necessary to use all deception measures in a deception operation. However it is necessary to ensure that all the means that the target has to receive the deception story or to acquire contrary evidence are provided with consistent indicators which collectively provide the whole story. While a mass of conflicting information will confuse the adversary and so assist the friendly commander it is better if the target is able to deduce a consistent and credible picture (albeit the wrong one) in response to the prompts portrayed to him.

SECTION 7.8: DECEPTION TECHNIQUES

7.74 A mix of false and real activities that in total are designed to achieve a specific effect on the target achieves the depiction of a deception. There are a number of patterns or combinations of activities used to achieve these effects. Each specific effect and the way it is achieved are known as a deception **technique**. Deception techniques may be used in combination to present a number of indicators to the enemy.

7.75 There are a number of deception techniques which form the basis of all active deception operations. The recognised techniques are:

a. the feint;

b. the demonstration;

c. the display; and

d. a variety of ruses:

the obvious solution,

the lure,

the false routine,

the mask,

the unintentional mistake,

the piece of bad luck,

the substitution, and

the double bluff.

Feints

7.76 The feint is the most widely used type of active deception operation at the tactical level.

7.77 **Characteristics.** Feints are offensive actions involving actual contact with the enemy. It is the actual contact that distinguishes them from demonstrations. They are usually designed to simulate the launching of an actual main attack, as distinct from supporting or diversionary attacks, which are real attacks with limited objectives.

7.78 **Purpose.** The principal purpose of a feint is to divert the attention and forces of the enemy from the point of the main operation. A feint may be used to cause the enemy to:

a. commit his reserves prematurely or away from the main attack;

b. hold his reserves so that they cannot influence the main attack;

c. reveal the extent and detail of his defence, including such things as his defensive fire plan and positions of support weapons;

d. divert support effort away from the main point of battle; and

e. reveal key technical intelligence (eg electronic characteristics of weapon systems).

7.79 A single feint may not always be the principal deception. A series of recurring feints can be used to harass and confuse the enemy to such an extent that he cannot distinguish the main thrust of the attack. Repetitive feints can also accustom the enemy to a pattern of activity so that he takes no special action; when the main attack occurs, mistaking it for just another feint.

Advantages. Realism is the key advantage of a feint, since the actual contact involved can convince the enemy of the 'truth' of the deception.

Disadvantages. Feints are resource intensive since in order to make them realistic considerable combat power has to be allocated to the task. Contact also brings with it the likelihood of capture of

personnel and documents and the greater risk that the enemy will become aware of the true purpose of the feint. The enemy will also be able to assess the relative strength of the force involved in the feint compared to the rest of the friendly force. Timing is important in minimising this risk by limiting the time between the feint and the actual attack so that they enemy cannot react to the discovery of the deception.

7.80 **Applications.** A feint must be plausible and courses of action considered during the initial appreciation but later rejected, are often suitable for a feint. It must also be capable of achieving the deception objective and the commander must determine that:

a. the area of activity is of sufficient importance to the enemy that he cannot ignore the attack and has to react in the way desired;

b. the feint is conducted sufficiently far from the main point of attack to require the enemy to adjust his dispositions away from positions where they can carry out their original or primary purpose; and

c. the area of the feint is sufficiently displaced from the point of main attack so that the feint does not interfere with the main attack.

7.81 **Time of a feint.** The timing of a feint is critical to its success. It may precede, or be coincident with, the main attack or it may even follow the commencement of the main attack. The timing and duration of the feint has to be such that the enemy commander has time to react and adjust or redeploy his forces before he discovers the nature of the feint or that the other action is the main attack. If he has not reacted then his dispositions will still allow him to meet the main attack with his original plan. A feint may follow a main attack where it is desired to keep the enemy off balance and undecided on the commitment of his reserves thus allowing the main attack time to consolidate and exploit any local opportunities.

Demonstration

7.82 A demonstration is a show of force in an area where a decision is not sought. It is similar to a feint except that no contact with the adversary is intended.

Advantages. The major advantages of using demonstrations are:

the absence of physical contact with the adversary facilitates subsequent employment of the demonstration force elsewhere;

the size of the force can be reduced as its strength is not to be tested by contact with the adversary; and

they permit more use of simulated equipment and actions.

Disavantages. The major disadvantages are:

a demonstration lacks the realism of a feint and it is more difficult to portray the deception story convincingly without contact; and

it is more likely that a demonstration will be identified as deception early in the operation enabling the adversary to divert his intelligence effort and forces to determine and counter the actual operation.

7.83 A demonstration may be used successfully when the factors of time, distance or terrain make a lack of contact realistic. They have application during defensive operations and when the forces are manoeuvring out of contact.

Displays

7.84 To assist in the projection of a deception story, units can be tasked to conduct displays by presenting static productions to the target's intelligence collection resources through the use of:

a. invention,

b. disguise,

c. portrayal, or

d. a combination of the above.

7.85 **Invention.** In an invention, objects or systems are simulated that do not exist. These simulations have varying requirements for authenticity, depending on the type, proximity, and effectiveness of adversary sensors, reconnaissance and observation, and the amount of camouflage used.

7.86 **Disguises.** A disguise is simply altering an object or set of objects to make it look like something else. Since many military objects and installations are difficult to conceal completely, it may be easier and more desirable to disguise their appearance. Disguise can also make targets of high value appear to be of little or no value.

7.87 **Portrayals.** A portrayal presents to the adversary a unit which does not exist, or which is of a different type to that which does actually exist. While portrayal is considered an act in itself, it usually includes disguises and inventions.

7.88 **Use of displays**. Ammunition and supply dumps, vehicle parks, airfields, artillery positions, bridges and field fortifications can be portrayed successfully. The results of some attacks can also be imitated to confuse an adversary's battle damage assessment. For example, airfield runways can be made to appear unusable, or secondary explosions can be initiated in a dump that has been shelled. Portrayal of installations may involve the alteration of existing facilities and adding equipment and activity necessary to provide the desired appearance.

Ruses

7.89 Ruses are tricks of war. They are generally single actions, planned or impromptu. The ruse is characterised by the deliberate placing of false information into the hands of the enemy. The techniques for instigating a ruse and overcoming the suspicion and scepticism of the target are briefly discussed in the following paragraphs.

7.90 **The obvious solution**. In this technique the adversary is encouraged to believe that the obvious way of achieving the objective will be adopted. The JMAP and the adversary deployment pattern can give leads to the identification of what is the most obvious course of action and what the adversary has appreciated is the most likely friendly course.

7.91 **The lure**. In this technique the adversary is presented with a set of apparent circumstances which offer a sudden and ideal opportunity to achieve his objective and which must therefore be seized quickly before it disappears. In fact he is being tempted to take action without the opportunity to fully test the intelligence that has been presented to him and he is heading into a trap.

7.92 **The false routine**. The adversary is conditioned by repetition to believe that the friendly force has a routine of activity that does not lead to any threat. In fact the routine activity is used by the friendly force as a cover for the preparation of hostile action. This may also be known as The Cry Wolf Ploy, where the target is given a number of alerts which result in no substantive action so that he is reluctant to cause yet another unnecessary alert when the real action begins.

7.93 **The mask**. In this technique the friendly forces are disguised as an adversary or neutral element so that the adversary fails to identify them until it is too late and they have a tactical advantage. The use of this technique has to be undertaken with caution however as it is necessary to remove such disguise and reveal the true identity of the force in order not to contravene legal requirements.

7.94 **The unintentional mistake**. The adversary is lead to believe that valuable information has come into his hands by mistake or the incompetence of an individual. This technique most often takes the form of an apparent breach of security or lapse in operational security arising from incorrect use of

document or communications security. Loose talk in the proximity of known or possible enemy agents also comes into this category.

7.95 **The piece of bad luck**. The adversary is lead to believe he has acquired a piece of vitally important information due to friendly force accident or bad luck. The feeding of information to the adversary by having him find such things as marked maps in evacuated headquarters or on prisoners or casualties is such a technique. Faked vehicle or aircraft accidents in which apparently important information falls into the adversary's hands are an example of this technique. The important aspect to using this technique is to ensure that the circumstances are so arranged that the adversary does not suspect the ease with which he receives a critical piece of information.

7.96 **Substitution - false display**. This is an elaborate ploy in which the adversary is shown a display that is obviously a deception or is deliberately exposed to the adversary as not being genuine. Salvaged or dummy equipment and prepared alternative or dummy positions may be used. When the adversary has accepted it as a false situation and dismissed it from his consideration, they can be occupied as real positions or substituted with real capability. A simple example is the dummy defensive position that the adversary discovers to be dummy but the friendly force subsequently occupies as a key part of their defensive plan.

7.97 **The double bluff**. This technique is reliant on an adversary's natural predisposition to expect deception or previous conditioning. Given these circumstances the adversary is presented with the real situation but identifies it as a deception and dismisses it. This technique is extremely risky and requires a highly developed ability to monitor the adversary's intelligence and decision processes. It is vital that the friendly commander knows that the real situation has been dismissed and can proceed with implementation of the real plan without risk.

7.98 **Overload**. Where it is not possible to shift the target's perceptions, it may be possible to:

a. present him with a variety of stories of which all appear equally probable; or

b. present him with so much information that he finds it difficult to reach any conclusion.

7.99 The second situation is one of creating an overload on his intelligence system. The technique of overload is to provide the adversary with an excessive amount of information which he must sort through to make a decision. It is designed to prevent him from producing effective and timely intelligence. If executed effectively it neutralises the adversary's intelligence effort and in the longer term reduces the credibility of the intelligence staff in the eyes of their commander and the operations staff. Such a situation will support future deception, as commanders who have lost faith in their intelligence staff will tend to be their own intelligence officers. They then make themselves more susceptible to believing preconceived ideas or the sources they regard as "best", to the exclusion of a more balanced assessment of the full range of sources.

7.100 The use of overload should not be resorted to lightly. Its effectiveness relies on the incompetence of the adversary intelligence system and its inability to handle volume processing. Faced with a system overload an intelligence officer may fall back on a smaller number of high quality sources or on an almost random selection of the reports available. Equally he might rely more on his detached assessment and be relatively uninfluenced by the incoming information. In these cases the intelligence officer frees himself from being overloaded and can produce a coherent assessment. Such assessments may be wrong but equally they may be right. In either case the friendly deceiver, by using overload, has lost the ability to influence the adversary intelligence officer. Resorting to overload as a ploy therefore still requires the monitoring of the adversary intelligence and command system to determine what the actual effect is and how the overload is being handled.

7.101 The use of overload at the same time as active deception can neutralise the deception. Good deception requires that it attract the attention of the target and intelligence staff and keep them focussed on the information that supports the story. The false information being fed to the adversary to depict the deception story may be lost in the overall volume of the overload.

SECTION 7.9: DECEPTION PLANS

The Deception Plan

7.102 A deception plan consists of the target, the objective, the technique/s, the means, the measures, timings, and the resources required or responsible to achieve the effect.

7.103 **Deriving a plan from the story**. Having decided on the deception story, planners consider which elements of the story can be conveyed by what means, using what technique to the target over what timeframe. The deception planners approach the deception story as if it were the force commander's concept of operations, and detail the actions that the force would have to take to execute the operation.

7.104 **A plan for each COA**. An initial deception plan, prepared for each COA developed within the JMAP, will include a deception target, objective and story, and an overview of the techniques, means, measures, times and resources required. These issues are contested during the wargaming process conducted as part of COA Analayis (see Chapter 4).

7.105 **Deciding on the plan**. In the process of deciding a COA, the commander will select the preferred deception story and provide guidance on the techniques and resources to be used. This is developed into the actual deception plan by matching the available resources to the portrayal of the elements of the deception story they are required to carry out. The preparation of the deception plan converts the visualised deception into the specific actions (deception measures) that have to be carried out. It also finalises who has to carry them out in order to convey the indicators of the deception story to the target's collection means. These then are the basis of the instructions and orders that are subsequently issued.

SECTION 7.10: EXECUTION

Supervision and coordination

7.106 The plan has to include the arrangements for ensuring the deception activities are coordinated and the reporting requirements of the various participants. This should extend to the requirements for monitoring the effectiveness and completeness of the activities and the review and adjustment of the operation.

Concluding a deception

7.107 It is important that, at the planning stage, the way in which the deception is to be concluded is considered and included in the plan. The best deception is one that the adversary does not know has occurred - ever!

7.108 Deception activities should terminate in a logical manner, from the adversary point of view; and it may be necessary to manufacture information in order to make it seem so. The adversary may tend to blame his own intelligence system for failing to provide timely and accurate intelligence rather than see (and acknowledge) that he has been successfully, deceived. This characteristic can be exploited by providing information that shows the real situation but does it too late to be of use.

7.109 The notional order of battle has to be adjusted back to the actual order of battle in a logical way if the adversary is to remain unaware of the deception. If it is intended to utilise 'phantom' units again then they have to be placed in reserve and some continuing deception activities will have to be promulgated to the enemy. Such long-term deception, even at a low level, will require a dedication of resources. Notional units can be disbanded as reinforcements for actual units, however time has to be allocated to achieve this and some briefing and actual movement of personnel may be required if the deception is not to be later compromised by the interrogation of friendly prisoners.

Flexibility

7.110 No battle proceeds as planned. The deception has to be sufficiently flexible to be altered in response to adversary activity that was unexpected or other events that alter the situation. Situations may also arise where the means of channelling the deception story to the adversary become ineffective or are destroyed and alternative measures have to be generated to ensure critical aspects get through to the target.

7.111 The deception must be able to exploit unforeseen opportunities as well as remedy problems. A deception should not be so designed that a critical operational opportunity cannot be exploited because Of the inflexibility of the deception operation. Where exploiting an operational opportunity will compromise the deception the long-term effects on the overall mission will have to be weighed by the commander.

Protection of false activity

7.112 Where it is decided to depict false activity, consideration has to be given to:

a. the provision of protection to the troops who are carrying out the depiction in order to secure them and their deception activities from destruction and discovery; and

b. those OPSEC measures that have to be taken to protect the depiction from compromise.

Concealing the real operation

7.113 The planning and execution of OPSEC measures that are needed to secure the real operation are not a direct responsibility of the deception planners. However the OPSEC measures taken to protect the real operation have to be coordinated with the measures needed to insure against the compromise of the deception operations by the discovery of the real activities. Additionally the deception plan could require the disclosure of some real activity, to the enemy. So it is necessary to ensure that the OPSEC measures associated with the real plan are not so effective that they preclude the enemy from discovering the elements of information required by the deception plan.

7.114 **The Need to Know.** The control arrangements for the distribution of the deception plan and orders has to take into account the extent to which the usual recipients of operational information have a need to know about the deception.