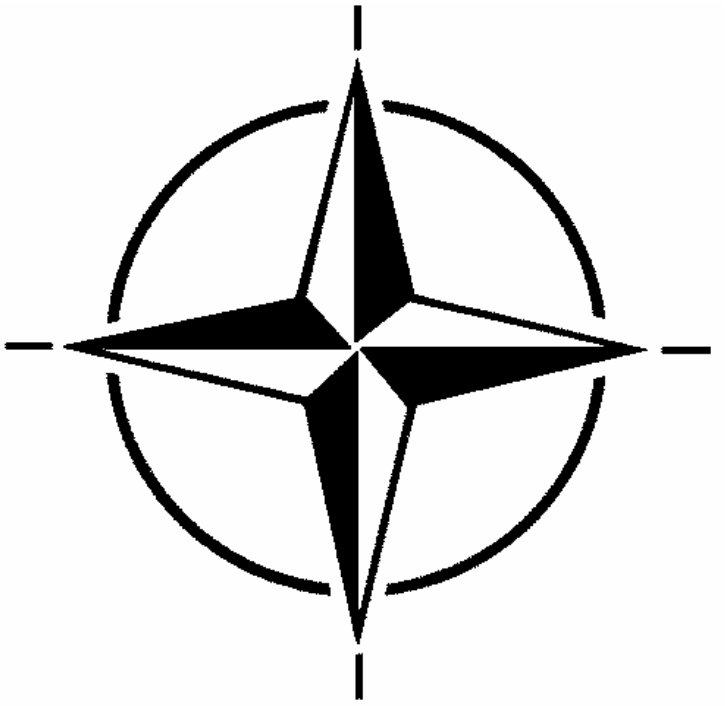
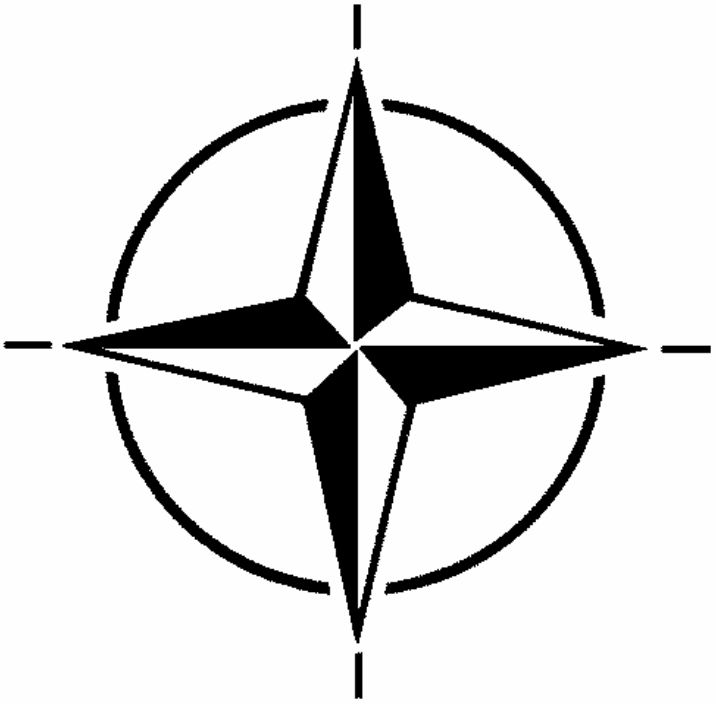


AJP-3.10

ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS

(INTENTIONALLY BLANK)



ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS

AJP-3.10

NOVEMBER 2009

(INTENTIONALLY BLANK)

NORTH ATLANTIC TREATY ORGANIZATION

NATO STANDARDIZATION AGENCY (NSA)

NATO LETTER OF PROMULGATION

23 November 2009

1. AJP-3.10 – ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS is a NATO/PfP UNCLASSIFIED publication. The agreement of NATO nations to use this publication is recorded in STANAG 2518.

2. AJP-3.10 is effective on receipt.

Juan A. MORENO
Vice Admiral ESP(N)
Director, NATO Standardization Agency

(INTENTIONALLY BLANK)

RESERVED FOR NATIONAL LETTER OF PROMULGATION

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change Date	Date Entered	Effective Date	By whom entered

(INTENTIONALLY BLANK)

RECORD OF RESERVATIONS

Chapter/Annex	Record of Reservation By Nations
Genral	DEU
1	USA
2	ITA
3	USA
Annex 1A	USA

(INTENTIONALLY BLANK)

RECORD OF SPECIFIC RESERVATIONS

Nation	Specific Reservations
DEU	1. Effects-Based Approach is not a NATO agreed term, not ratified and shall therefore not be used. Especially the use of the abbreviations EBA / EBAO / EBO shall be avoided in accordance with discussions related to the Combined Custodial Project (CCP) re-working the capstone and Keystone documents AJP-01, 03 and -05 and decision taken in the last AJOD-WG from October 2008. 2. The AJP insufficiently emphasizes the requirement for mission-specific strategic and political guidance for information activities, e.g. , in the format of a multinational Information Strategy. 3. The used term "Critical Vulnerability" is insufficiently described and does not reflect dependency on "Critical Requirement" and "Critical Capability". It therefore should be replaced by the definition given in the GOP. Critical Vulnerability. A critical vulnerability exists when a critical requirement is deficient, degraded or missing and exposes a critical capability to damage or loss. The ability to exploit critical vulnerabilities provides the potential to achieve significant or even decisive results disproportionate to the military resources applied. Operational art looks to gain leverage by applying own strengths against critical vulnerabilities of opposing forces. 4. The legal limitations and constrains as mentioned in the AJP-3.10 repeatedly should refer not only to the conduct of information activities but also to he effects created just by the co-ordination of such activities.
ITA	Considering the three InfoOps staff options (para. 208), ITA will apply option c. normally centralised Info Ops branch at ACOS level under a Chief InfoOps). In some cases ITA will consider acceptable another staff option: a Info Ops section as part of the specialist J3/5 branches.
USA	a. The United States does not subscribe to how the term “effects” is described in paragraphs 0110 and 0313. Rationale. AJP-01(C) supports an “effects-based approach to operations” to “achieving results that will contribute to attaining objectives and the strategic end-state." AJP 3-10 use of the term “effects” is contrary to AJP-01(C). Effects are not capabilities to be delivered, but the result of the employment of capabilities. The use of effects in AJP 3-10 must be consistent with AJP-01. The text from these paragraphs should read as follows: (1) 0110. **Effects-Based Approach <u>to Operations</u>**. ~~Alliance operations are likely to be more efficiently conducted by adopting an effects-based approach~~ <u>The Alliance’s focus should increasingly be on ensuring that activities contribute to creating the</u> ~~effects~~ <u>outcomes to achieve strategic campaign objectives.</u> The individual elements that comprise an effects-based approach are not new; it is a philosophical change in the way to <u>view</u>, plan, conduct and assess operations. It ~~puts a stronger focus on cause and effect versus target-centric attrition~~ <u>places emphasis on achieving desired outcomes and mitigating undesired ones.</u> It involves the coherent planning~~,~~ execution and assessment of actions by all involved organizations, together with the use of modern technology<u>.</u> ~~and novel approaches to enhance situational understanding, that brings new possibilities to the way future operations will be conducted.~~ (2) 0313. Info Ops assist in the targeting process by identifying where information activities could be applied to achieve ~~specific~~ <u>desired</u> ~~effects~~ <u>outcomes</u> in support of the JFC’s mission objectives. b. The US does not subscribe to the use of kinetic and non-kinetic language in paragraphs 0103, 0110, 0115 and 1A1. Rationale. Kinetic and non-kinetic activities have no defined meaning in NATO doctrine. Kinetic is a scientific idea commonly applied to motion and energy related descriptions. Kinetic and non-kinetic (non-motion or non-energy activities) do not fit the context of the publication. In contrast,

paragraph 0125 of AJP-01(C) references lethal and non-lethal "effects in order to achieve operational objectives." The precedent established in this *capstone* document provides an alliance agreed upon concept that can be applied to the use of information operations to achieve campaign objectives.

(1) 0103. **Non-~~Kinetic~~ Lethal Activities**. While information operations may be accomplished through ~~kinetic or non-kinetic~~ lethal or non-lethal means, ~~as effects-based thinking is applied,~~ there is likely to be an increased focus on non-~~kinetic~~ lethal activity. A large element of Info Ops is non-~~kinetic~~ lethal, and recent operations have shown its significance by increasing the commander's choice of means, by which effects can be ~~achieved~~ created or generated at all stages of a crisis to support achievement of objectives. ~~However, it is not only the movement towards an Effects-Based Approach (EBA) that has brought about this new emphasis on non-kinetic activity.~~

(2) 0110. This approach can be adopted at all levels of command and across the spectrum of conflict. Info Ops is an integrating function focused on the information environment that involves the selective combination of lethal and non-lethal ~~effects, kinetic and non-kinetic~~ means to achieve campaign objectives.

(3) 0115. Military information activities may include a wide range of actions (see Annex 1A – Information ~~Operations Critical Terminology~~ Activities Actions) and will be achieved by ~~kinetic and/or non-kinetic means delivering~~ lethal and/or non-lethal means ~~effects~~.

(4) 1A1 changes are as follows:

ANNEX 1A – INFORMATION ACTIVITIES ACTIONS ~~OPERATIONS CRITICAL TERMINOLOGY~~

Compel	To force someone to undertake a desired course of action. (Similar to convince and mislead but not limited to perceptions and generally ~~more kinetic~~ lethal ~~in its overtone~~.)
Diminish	To make less or cause less to appear to reduce the effectiveness of an activity. (This is similar to degrade, without the ~~kinetic~~ lethal overtones.)
Disrupt	To break or interrupt the flow of information. To use force or other non-lethal ~~kinetic~~ means to shatter the cohesion of a (target) audience and prevent them from functioning effectively. (Damage done to the function is temporary, and only portions of the function were affected. A function's operation is impaired over the short term and the damage does not extend to all facets of the function's operation.)

c. The US does not subscribe to the idea that Civil-Military Cooperation (CIMIC) as discussed in paragraphs 0130-0131, Section V, *Capabilities, Tools, and Techniques Used in Support of Information Objectives*, is a capability.

Rationale. The United States believes the current placement of paragraphs 0130-0131 could mislead readers as to the actual doctrinal relationship between information activities and CIMIC. These paragraphs would be better served if placed into a separate section entitled *Relationship to Civil-Military Cooperation* which describes how information activities support CIMIC operations.

d. The United States does not subscribe to Annex 1A labeled as critical terminology or the second column header labeled "DEFINITION".

	Rationale. The table is described as an "illustrative overview of the possible range of actions that could be involved in military information activities" and should not be interpreted as defining those actions. 1A1 changes are as follows: ACTION | ~~DEFINITIONS~~ DESCRIPTION e. The United States does not recognize the terms and definitions included in the text and glossary as being NATO agreed terms that have been identified for inclusion into the NATO Terminology Data Base and/or for inclusion into AAP-6: *combined joint task force, computer network operations, critical vulnerability, information activities, information environment, information objectives, information operations, information security, information systems* and *public affairs*.

(INTENTIONALLY BLANK)

PREFACE

1. Doctrine consists of fundamental principles by which military forces guide their actions in support of objectives. It is authoritative but requires judgement in application. The planning, execution and support of military operations require a clearly understood and widely accepted doctrine. This is especially important when combined, multinational or coalition forces conduct operations. Joint doctrine applies when two or more components operate together.

2. North Atlantic Treaty Organisation (NATO) military Information Operations (Info Ops) doctrine is intended primarily for use by NATO forces, and provides a useful framework for operations conducted by a coalition of NATO partners, non-NATO nations and other organisations. Interoperability between NATO nations is based upon NATO standardisation agreements and publications; many of the subjects covered in these may have to be reconsidered in the planning of Info Ops with non-NATO forces in accordance with North Atlantic Council (NAC) agreed decisions and procedures. This doctrine, therefore, provides a common baseline for achieving Info Ops interoperability, rather than trying to encompass each nation's Info Ops approach.

3. The purpose of Allied Joint Publication (AJP)-3.10 *Allied Joint Doctrine for Information Operations* is to explain how Info Ops support the planning, conduct and assessment of operations. The provenance for AJP-3.10 is MC 422/3 *NATO Military Policy on Information Operations*, which clearly acknowledges the primacy of civil/political direction on information issues and that the policy and subordinate doctrine applies to the military lever of power only. AJP-3.10 is focused on the operational level. It defines and discusses principles of Info Ops, and highlights those particular Info Ops considerations relevant to the conduct of operations, such as the sensitivity to political factors, and the role of non-military entities and emerging technological capabilities in the information environment, both within and external to NATO.

4. The ongoing debate about the span of Info Ops has fuelled doctrine development based on real world necessity. AJP-3.10 must be seen as a living document, centred on how Info Ops supports the Joint Force Commander's (JFC's) mission.

5. AJP-3.10 is intended principally for use by a JFC, Combined Joint Task Force (CJTF) commander, Deployable Joint Task Force (DJTF) commander and those of their staff with Info Ops responsibilities. It addresses the roles, links, responsibilities and required products from the strategic, operational and tactical commands. Each echelon of command will be responsible for developing specific Standing Operating Procedures (SOPs) to reflect Headquarters (HQ)/command specifics, as appropriate.

6. Within the overall NATO publication hierarchy, AJP-3.10 is directly subordinate to AJP-3 *Joint Operations*, which is one of NATO's keystone publications focused on staff functions. AJP-3 describes the fundamental operational aspects of joint operations and provides guidance on their conduct. Furthermore, AJP-3.10 links directly to AJP-01 and the available policy documents containing Info Ops content.

(INTENTIONALLY BLANK)

ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS AJP-3.10

TABLE OF CONTENTS

CHAPTER 1 – INFORMATION OPERATIONS

Section I – Background

0101. **Information in the Global Security Environment**. The changing global security situation has seen a shift in emphasis from the certainties of super-power confrontation towards more complex interactions of state and non-state actors. Globalisation, competition for resources and tensions in political and social structures combine with ideological, religious and cultural distinctions to increase uncertainty. Furthermore, terrorism, along with the spread of weapons of mass destruction, are likely to remain principal threats. There is also an expectation in some societies, reinforced by media exposure of global issues, that conflict and confrontation will be constrained by increasingly moral codes and regulated by progressively more extensive legal obligations. Concurrently, there has been an 'information revolution' (the Internet and mobile telephones) that has ushered in an age of computer-based decision-making. This evolving Information Environment[1] comprises information, actors and systems that enable the use of information. The actors include leaders, decision-makers, individuals, and organizations. Information systems[2] include the materials and systems employed to collect, apply, or disseminate information. The information environment itself is where humans and automated systems observe, orientate, decide and act upon information, and is therefore the principal environment of decision-making. To address both the changing global security situation and the emergence of a new information environment, NATO is in the process of developing concepts, processes and doctrine, including Information Operations (Info Ops), to deal with these new challenges.

0102. **Strategic Guidance**. Military action alone cannot resolve crises, but it can set the conditions for resolution by other actors, including the use of the full suite of national power provided by NATO member states. During planning and throughout operations the military identifies how it may best support, and be supported by, other instruments of Alliance power.[3] As part of this approach, the NAC will provide overall guidance and direction for NATO public diplomacy efforts, as well as mission-specific strategic and political guidance for NATO military information activities.[4] As NATO's political/military situation evolves and matures for a given situation/operation, revised/updated strategic guidance could be provided to adjust the planning and conduct of information activities accordingly.

---

[1] The Information Environment is defined as the virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems. (MC 422/3)

[2] Information systems are socio-technical systems for the collection, processing and dissemination of information. They comprise personnel, technical components, organisational structures and processes that create, collect, perceive, analyse, assess, structure, manipulate, store, retrieve, display, share, transmit and disseminate information. (AJP-3.10)

[3] 'Instruments of power' are the national or organisational means to enforce will or exert influence on others; one framework for this is Diplomacy, Information, Military and Economic elements (DIME).

[4] Information activities are actions designed to affect information and/or information systems, performed by any actor. (AJP-3.10)

0103. **Non-Lethal Activities**. While Information Objectives[5] may be accomplished through lethal or non-lethal means, there is likely to be an increased focus on non-lethal activity. A large element of Info Ops is non-lethal and recent operations have shown its significance by increasing the commander's choice of means, by which effects can be created or generated at all stages of a crisis to support achievement of objectives. Increased attention on Info Ops is also due to the realisation that we now live in an information-dominated environment as described in paragraph 0101. There is an increased reliance on, and desire for, information. In addition, the impact of real-time media coverage of crises, the exploitation and manipulation of the media by some parties and the ever-increasing use of technologies such as the Internet have resulted in a world where information plays an increasingly important role.

0104. **The Importance of Information**. Information awareness and perceptions gained from analysis of collected information and personal observations have long been an integral part of human existence; those with a superior ability to gather, understand, control and use information have gained a substantial advantage. The ability to manage and employ information underpins activities in diplomatic, military, economic and other areas of activity, maintaining Allied freedom of action. From the strategic to the tactical level and across the range of military operations, information plays a vital role in the manner in which decisions are made. In military operations the ability to defeat adversaries or potential adversaries may rest on the perception of all actors involved, particularly the local population. There is therefore considerable benefit to be gained by affecting the flow of information through a decision-maker and his understanding of that information.

0105. **The Impact of the Media**. All crises occur under the spotlight of the international media. The maintenance of understanding and support of public opinion is crucial for democratically accountable governments, and this influences[6] the options they can take, including military action, and the presentation of these options to different audiences. In order to gain and maintain public support, national governments and international organisations/agencies need to show a degree of transparency in their actions, and these actions must be in accordance with international law. The influence of the media has increased as access to regional and international media has increased. This has been brought about by technologies such as satellite broadcasting and global connectivity through the Internet. In addition, the availability of relatively cheap printing and copying equipment has brought newspapers and other printed material to a much wider audience. Consequently, there is a need to be proactive in ensuring that the presentation of NATO actions is accurate and reflects NATO's

[5] Information Objectives provide statements of measurable response that reflect the aspired conditions in the information environment as a result of information activities. They enable analysis, planning, execution/management and assessment/evaluation of related actions and/or effects. (AJP-3.10)

[6] The Concise Oxford English Dictionary defines the term 'influence' as 'the capacity to have an effect on the character or behaviour of someone or something, or the effect itself'. This benign definition provides the meaning of 'influence' throughout this document.

messages, while at the same time countering an adversary's[7] or detractor's attempts to undermine public support.

0106. **The Impact of Technology and the Internet**. In addition to the role played by technology in increasing access to the media, there is an ever-increasing dependence on Information Technology (IT). Computer systems now pervade society; they also form the core of most military systems, especially communications systems/signals support and Intelligence, Surveillance and Reconnaissance (ISR). This increased reliance on computer technology introduces new opportunities that can be exploited, and new vulnerabilities that must be addressed. In addition, technology has provided a new means of direct access to information via the Internet. That information is absorbed without necessarily knowing its validity and source and, in some cases, considerable credence is placed on it; this is particularly so in societies without a free press. The Internet is used to spread or circulate information and opinion, including rumour, with a speed inconceivable a few years ago. The Internet is an unrestricted and unregulated medium, available globally, which an adversary can exploit either to spread his message, as a vehicle to attack friendly systems, or as an open source of intelligence.

Section II – Fundamentals of Information Operations

0107. **Definitions**. The definition of Info Ops and information activities are as follows:[8]

a. Info Ops is a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties[9] in support of Alliance mission objectives.

b. Information activities are actions designed to affect information and or information systems. They can be performed by any actor and include protective measures.

0108. **Focus of Information Operations**. A decision-maker's[10] effectiveness is a function of *will*,[11] *understanding*[12] and *capability*. In other words, a decision-maker must have the will to act, an understanding of the situation to act and possess the capability to act. If any one of these elements is not in place, the decision-maker's ability to act in the way he wants to will

---

[7] Throughout this publication, the term 'adversary' includes potential as well as actual adversary.
[8] Drawn from MC422/3 – *NATO Military Policy on Information Operation.*
[9] NAC approved parties are those identified in top-level political guidance on Alliance information activities. These may include adversaries, potential adversaries, decision makers, cultural groups, elements of the international community and others who may be informed by Alliance information activities.
[10] Decision-maker is used in its broadest sense throughout this document. They include political and other leaders and military commanders, influential individuals, military personnel, armed factions and specific population groups (e.g. ethnic, cultural, religious and political). They may be adversaries, potential adversaries or other NAC approved parties.
[11] Will includes factors such as motivation, intent, attitude, beliefs and values.
[12] In this context, understanding includes an actor's perceptions of a given situation and an actor's situational awareness of that situation.

be affected.[13] Generally conflict focused, the Joint Force Commander (JFC)'s campaign has, in the past, aimed primarily at affecting an adversary's capability, with the secondary aim of affecting his will. Activities coordinated through Info Ops focus directly on influencing will, affecting understanding and on those capabilities that promote understanding or the application of will. They therefore have applicability across the range of military operations. The following are examples of how Info Ops may support mission accomplishment in all military operations:

a. **Will**. Within the direction and goals of wider military operations, and mission specific NATO guidance, military information activities are aimed at decision-makers at any level capable of influencing the situation:

(1) Information activities aim to influence an adversary's will and undermine cohesion. For example, by questioning the legitimacy of leadership and cause, information activities may undermine their moral power base, separating leadership from supporters, political, military and public, thus weakening their desire to continue and affecting their actions. Adversary attempts to influence NATO's will should be countered, in order to isolate the adversary, maintain coalition cohesion and enhance our freedom of action.

(2) Information activities aim to protect those capabilities, for example friendly command, control and communications infrastructure, that allow us to exercise effective command, and to seize and maintain the initiative. NATO may seek to protect approved parties' capabilities proactively by countering adversary information activities.

b. **Understanding**. Military information activities will seek to affect the information available to decision-makers in order to affect their understanding of a given situation:

(1) Information activities seek to deny, degrade, disrupt and manipulate the information available to a decision-maker in order to affect understanding and thereby perception. Manipulation of information in these ways will directly affect the actions of the adversary decision-maker, enabling friendly information-superiority and decision-making.

(2) Information activities are also aimed at ensuring that the information available to friendly decision-makers is safeguarded and assured. In this way, shared understanding between allies will be possible (provided the mechanisms are in place), thus improving NATO decision-making and effectiveness. In addition, NATO may seek to provide factual information to other approved parties to seek their support or to undermine efforts of an adversary attempting to gain support from them.

[13] The term 'to affect' is used throughout the document in a generic sense meaning: 'to have an effect on', without any implied (positive or negative) connotations.

c. **Capability**. Within Rules of Engagement (ROE) and legal constraints, military information activities will seek to affect those capabilities, such as the adversary's command, control and communications infrastructure and propaganda facilities that enable a decision-maker to understand a situation and apply his will:

(1) Information activities seek to degrade, disrupt, deceive, destroy or deny those capabilities that allow adversary decision-makers to increase their understanding; bolster, impose, apply and sustain their will and to exercise effective command. In concert with other military and governmental actions, information activities also seek to attack the source of the adversary decision-maker's power base, splitting internal and external groupings and alliances. The aim is to influence adversary decision-making processes, thereby preventing them from taking the initiative.

(2) Information activities also aim to protect those capabilities, for example friendly command, control and communication infrastructure, that allow us to exercise effective command, seize and maintain the initiative. NATO may seek to protect approved parties' capabilities directly by providing materiel and advice, or indirectly by targeting those adversary capabilities that could be used to attack an approved party's capability.

Section III – Principles of Information Operations

0109. **Principles**. The planning and conduct of military information activities should be based on certain principles. These principles will also shape how Info Ops are integrated into the joint targeting process and direct the way in which information activities support the full range of NATO military operations.

0110. **Effects-Based Approach to Operations**. Alliance operations are likely to be more efficiently conducted by adopting an effects-based approach. The individual elements that comprise an effects-based approach are not new; it is a philosophical change in the way to plan, conduct and assess operations. It puts a stronger focus on cause and effect versus target-centric attrition. It involves the coherent planning, execution and assessment of actions by all involved organisations, together with the use of modern technology and novel approaches to enhance situational understanding, that brings new possibilities to the way future operations will be conducted. This approach can be adopted at all levels of command and across the spectrum of conflict. Info Ops is an integrating function focused on the information environment that involves the selective combination of lethal and non-lethal means to achieve campaign objectives.

0111. **Commander's Direction and Personal Involvement**. The commander's personal involvement drives Info Ops, and exercises control over all Info Ops activity within a framework of timely decision-making and consultation up and down the chain of command. Following mission analysis, the commander formulates his initial intent, which reflects higher guidance. Tactical level planning is based on that intent, which must have a clearly

defined military end state and identify the effects required to achieve the relevant objectives. Without this guidance, the Info Ops effort will lack focus and will not create the desired effects.

0112. **Close Coordination and Sequencing**. The very nature of Info Ops and the large, diverse target set means that there needs to be very close integration within a command, and consistency with mission-specific strategic and political guidance for NATO information activities. All plans and activities must be coordinated, de-conflicted and synchronised up, down and across the chain of command with other military, political and civil activities in order that one activity does not compromise, negate or diminish the desired effect of another. This is the responsibility of the commander, assisted by the Chief Info Ops.

0113. **Accurate Intelligence and Information**. Successful military information activities must be founded on effective Intelligence **(**INTEL) support. Attributes of effective INTEL include timely, accurate, and relevant intelligence about adversaries, other NAC approved parties, and the operational environment. The Info Ops staff should coordinate with the INTEL staff to define those INTEL requirements necessary to plan, execute and assess the effectiveness of military information activities. Joint Intelligence Preparation of the Battlespace (JIPB) should include analysis of human factors, IT, decision-making infrastructure and processes, and network vulnerabilities. This portion of JIPB needs to be compiled from various contributions of functional/capability expertise and forms the basis of the Info Ops input to the command estimate. The Info Ops staff will provide feedback to the INTEL staff (e.g., by submitting additional/adjusted requirements) and coordinate analysis contributions and assessments from capabilities conducting information activities. The Info Ops staff will not perform any INTEL collection or analysis function itself.

0114. **Centralised Planning and Decentralised Execution**. Due to the requirement for full integration of the Info Ops function, the principles of centralised planning and decentralised execution apply at all command levels. However, centralised execution may be required for certain types of targeted information activities, when all involved force elements are required to adhere rigidly to a plan, or where strategic assets are used.

0115. **Input to Joint Targeting**. Targeting starts with a detailed understanding of the operational environment and the JFC's objectives. The relevant functional/capability experts and the Info Ops staff identify effects in the information environment required to achieve the JFC's objectives and a range of actions that, when integrated into the overall operation plan, will achieve those objectives. Military information activities may include a wide range of actions (see Annex 1A – Information Operations Critical Terminology) and will be achieved by lethal and/or non-lethal means. Concerning human factors, it is important to realise that any element of targeting activity may influence a range of audiences and may create other unintended effects. The Info Ops staffs will coordinate assessment of the (possible) impact of such activity and propose appropriate actions.

0116. **Early Involvement and Timely Preparation**. Info Ops involvement in planning must start early, because both planning and execution take time and results can be slow to emerge.

Hence, a commander's Info Ops intent and direction, as part of the planning process, must be given at the earliest opportunity. Info Ops staffs need to be fully involved in the operational planning process to integrate Info Ops within the JFC's overall campaign plan.

0117. **Continuity**. The Info Ops function must be able to be performed continuously throughout peace, crisis, conflict and the post-conflict phase.

0118. **Monitoring and Assessment**. The successful prosecution of Info Ops relies on continuous monitoring and assessment of the short and long-term effects of interrelated activities, directed towards objectives. This is achieved by collection of all-source INTEL and other feedback on military information activities. Measurement of Effect (MOE) must be integrated in the INTEL collection activities led by J2. Particular attention should be paid to changes in the adversary's behaviour and such other items as changes in the attitude of the civilian population, political activity, and expressions of unrest. Also, changes in an adversary's capability may be used as a MOE, for example reduced efficiency, disorganisation and slower reactions to events and specific actions in response to deception.

Section IV – Information Operations Activity Areas

0119. Information activities coordinated through Info Ops are an integral part of the campaign plan aimed specifically at affecting the will and understanding of decision-makers and affecting those capabilities that directly enable the application of their will or aid their understanding. Effects in the information environment can be created by a variety of military activities, the close coordination of which will contribute to the achievement of the overall objective. Info Ops comprises three inter-related activity areas:

a. Information activities that focus on changing, influencing, or reinforcing perceptions and attitudes of adversaries and other NAC approved parties.

b. Information activities that focus on preserving and protecting Alliance freedom of manoeuvre in the information environment by defending the data and information that supports Alliance decision-makers and decision-making processes.

c. Information activities that focus on countering command functions and capabilities, by affecting the data and information that support adversaries and other NAC approved parties, and are used in command and control, intelligence, surveillance and target acquisition, and weapon systems.

While information operations focussing on preserving and protecting Alliance freedom of manoeuvre in the information environment should take place at all times, information operations activities focussed on influence (paragraph 0119 a) and counter command (paragraph 0119 c) may only take place as part of an OPLAN and thus with NAC approval, including definition by the NAC of adversaries and potential adversaries.

Section V – Capabilities, Tools and Techniques Used in Support of Information Objectives

0120. **Key Tools and Techniques**. Info Ops is an integrating function focused on the information environment rather than a capability in its own right. The 3 inter-related activity areas described in Section IV can make use of all or any capability or activity that can exert influence, affect understanding or have a counter-command effect; the extent is only limited by imagination, availability, policy, doctrine and legal constraints. However, there are several capabilities, tools and techniques that form the basis of most Info Ops activity. Information Objectives can be achieved by the planned coordination and synchronisation of military capabilities, tools and techniques affecting information or information systems (such as direct and indirect communication, and by using the electromagnetic spectrum or computer networks). The use of force (such as coercion and destruction) may also combine with those means, e.g., by delivery of specifically targeted fires, which can create considerable effects in the information environment. Clearly, many of these tools and techniques have a much wider application than Info Ops (and when not used to support Info Ops the potential unintended information effects of such activity must be considered), but can be drawn upon by Info Ops. The following paragraphs provide examples of capabilities, tools and techniques used in support of Information Objectives.

0121. **Psychological Operations**. The primary purpose of Psychological Operations (PSYOPS) is to influence the perceptions, attitudes and behaviour of selected individuals or groups in accordance with NAC approved PSYOPS objectives, to induce or reinforce behaviours favourable to overall Alliance objectives. PSYOPS plans and activities have to be in accordance with strategic guidance on information activities and Information Objectives determined in the Operation Plan (OPLAN) (See Annex 3B). Unlike Public Affairs (PA), PSYOPS retains direct control over contents, dissemination and audience. Effective PSYOPS requires timely provision of intelligence, resources such as linguistic support, graphics and print capability, broadcasting capability and other delivery mechanisms. Message presentation methods include print, radio, television, loudspeakers, face-to-face contact, the Internet, faxes, pagers and telephone. Besides the employment of own assets local media services may be contracted. Special support through reach-back can increase planning depth and production output.

0122. **Presence, Posture and Profile**. The impact that the mere presence of a force may have on perceptions can be significant. Deploying even limited capability to the right place at the right time can add substantial credibility to messages being delivered through other channels and provide a major contribution to deterrence. The posture of troops on the ground can demonstrate both commitment and intent and must be considered and balanced with the requirements of force protection. The decision to wear berets instead of combat helmets and body armour can make a considerable difference to the perceptions of both the adversary and local people. The public profile of commanders at all levels will impact on perceptions and therefore the public role of the commander must be carefully analysed and opportunities used to transmit key messages.

0123. **Operations Security**. Operations Security (OPSEC) is the process which gives a military operation appropriate security, using passive or active means, to deny an adversary knowledge of the dispositions, capabilities or intentions of friendly forces. In particular, OPSEC is used to identify and protect information that is critical to the success of the campaign, described as Essential Elements of Friendly Information (EEFI). It aims to deny EEFI to the adversary decision-maker, thereby affecting understanding. EEFI will need to be protected throughout their lifecycle and throughout the range of military operations. Adversarial will, understanding and capability will be targeted to maintain the security of EEFI, using a combination of passive and active techniques.

0124. **Information Security**. As part of OPSEC the goal of Information Security (INFOSEC) is to protect information (stored, processed or transmitted), as well as the host systems, against a loss of confidentiality, integrity and availability through a variety of procedural, technical and administrative controls. INFOSEC includes a range of measures that are applied on a routine basis under the auspices of security policy to protect information. However, it is driven by the generic classification of data, not the criticality of information to a particular activity. Info Ops provides guidance on the application, or waiving, of INFOSEC measures in order to protect friendly decision-makers from adversarial Info Ops, to deny access to EEFI and to support influence or deception. This must be balanced with the need to maintain friendly decision tempo. INFOSEC is an integral element of all military operations and encompasses Communications Security (COMSEC), Computer Security (COMPUSEC), Computer Network Defence (CND), an integral part of Computer Network Operations (CNO), and together with personnel, document, physical and procedural security, it must be considered at the earliest conceptual stages and throughout the planning of an operation.

0125. **Deception**. Deception involves measures designed to mislead adversaries by manipulation, distortion or falsification. Deception is a complex art, which demands considerable effort, a high level of security and a sound understanding of an adversary's way of thinking. In operations, it can directly contribute to the achievement of surprise and, indirectly, to security and economy of effort. Within a deception plan both information and traditional physical means and methods (such as demonstrations and show of force) can be applied. Consequently, deception is not considered exclusively an Info Ops responsibility, but coordinated information activities can contribute to deception operations at all levels, for example, by influencing perceptions of adversary audiences. Info Ops planners must be involved in deception planning in order to ensure that deception objectives and information activities are employed in support of Information Objectives.

0126. **Electronic Warfare**. Electronic Warfare (EW) has wide application in military operations. The effect of EW activity can be temporary or permanent and it has the potential to minimise the use of force, hence avoiding unnecessary casualties and collateral damage. Electronic attack enables both the countering of command functions and attacks on IT. It also supports other information activities by enabling deception and PSYOPS, including broadcasts to target audiences. Electronic protective measures, in conjunction with spectrum management, contributes by helping to counter an adversary’s hostile information capabilities and protecting friendly use of the electromagnetic spectrum. Electronic support measures are an

integral part of information gathering and provide the commander with a wide variety of information from measures of effectiveness to targeting solutions. EW can support operations so that critical information on which an adversary will make a decision, or the information systems for carrying such information, can be affected to NATO advantage.

0127. **Physical Destruction**. There are 2 main aspects to the use of physical destruction for creating information effects. First, through attacks on command and control systems, physical destruction will play a large part in affecting the understanding of an adversary and in affecting his ability to apply will. Second, while the primary effect sought through the use of physical destruction will often lie outside Info Ops, the use of force sends a strong message and consequently the direct application of force through physical destruction will have significant psychological impact. Carefully applied force can play a major role in coercion and deterrence and in reducing an adversary's ability to exercise command. However, undue collateral damage and unnecessary casualties will have an adverse effect on public support. If physical destruction is required to create the desired effect, the JFC must consider and balance the potential negative impact (e.g. secondary effects and reconstruction requirements) that it may cause with the expected benefits.

0128. **Key Leader Engagement**. As part of the Info Ops contribution to an operation it is vital that all key actors and their inter-relationships are identified. Having detailed knowledge of key leaders' personalities, leadership styles, ambitions, motivations, objectives (short and long term), current stances, dependencies, psychological profiles and personal histories will be essential to provide the context to plan appropriate information activities. A vital component in all plans will be to recognise the complex, adaptive relationships and dependencies that exist between actors. The Info Ops staff will coordinate the commander's Key Leaders Engagement Plan (KLEP) that *inter alia* contains information on the situational context (planning milestones), critical events, planned contacts of the command group and special staff (key leaders) with relevant actors, objectives, main themes or issues to be addressed, desired effects and MOE. Figure 1.1 provides a schematic diagram that shows a possible graphic depiction of a KLEP.

Key Leaders Engagement Plan

(Example)

MILESTONES	*TOA* —— *Op XXXXXXX* ⟶					Pres. Elections	
DATE	D+	D+	D+39	D+	D+45	D+	D+
ACTORS							
CTF CDR			BILAT w/ COS ANA-SA				
CTF Deputy CDR					Regional Governors' Conference		
CFLCC CDR							Coordination w/ Local Police

Themes: Humanitarian Assistance | Security Support | Government Initiatives | Counter ACM

Figure 1.1 – Key Leaders Engagement Plan: Schematic Diagram

0129. **Computer Network Operations**. The opportunity for, and effectiveness of, CNO is proportional to the adversary's dependence on IT. CNO comprises 3 integrated elements: Computer Network Attack (CNA), Computer Network Exploitation (CNE) and CND:

a. **Computer Network Attack**. Software and hardware vulnerabilities allow computers, storage devices and networking equipments to be attacked through insertion of malicious code, such as viruses, or through more subtle manipulation of data, changing the characteristics and performance of the devices or the expression and display of the information contained therein. This capability is enhanced by the increasing use of commercial off-the-shelf software in military systems.

b. **Computer Network Exploitation**. CNE supports Info Ops by the ability to get information about computers and computer networks, by gaining access to information hosted on those and the ability to make use of the information and the computers/computer networks.

c. **Computer Network Defence**. The purpose of CND is to protect against CNA and CNE. CND is action taken to protect against disruption, denial, degradation or destruction of information resident in computers and computer networks or the computers and networks themselves. CND is essential to maintain decision-making capability; as well as maintaining a defensive posture, it will use monitoring and

penetration protection techniques to detect, characterise, and respond to an attack, instigating containment and recovery action as required.

0130. **Civil-Military Cooperation**. Although Civil-Military Cooperation (CIMIC) is a capability that can be used to achieve Information Objectives, it is unique in that it seeks to create a meaningful relationship between the military, civilian agencies and the local population. Indeed, CIMIC is the coordination and cooperation, in support of the mission, between military and civil actors, including national population and local authorities, as well as international, national and non-governmental organisations and agencies. CIMIC facilitates cooperation and coordinates activities between a military force and all parts of the civilian environment within the Joint Operations Area (JOA) by:

a. Liaison and coordination with civil actors, e.g. International Organisations (IOs) and Non-Governmental Organisations (NGOs).

b. Considering political, economic, environmental and humanitarian factors when planning and conducting military operations.

c. Building an effective relationship between the military and civilian authorities, organisations, agencies and populations within the JOA.

0131. In addition to the tasks of liaison, reconnaissance, provision of an advisory service and coordinating the management of infrastructure projects, direct relief operations can also be undertaken. The CIMIC staff need to establish relationships with a variety of civilian authorities and agencies and thereby establish a valuable source of information to assist in the planning of information activities. However, due care must be taken to avoid CIMIC activities being perceived as intelligence gathering by partner agencies such as IOs or NGOs. This can be achieved by CIMIC coordinating with other capabilities that consider civil audiences and information systems to create and sustain the conditions needed to support the achievement of Alliance objectives. Depending on the situation and mission requirements, CIMIC activities, within the scope of CIMIC tasks, may directly contribute to influencing key decision-makers.

Section VI – Relationship to Public Affairs

0132. **Public Affairs**. The aim of PA is to protect the credibility of NATO and promote widespread understanding, thereby gaining support for military operations while not compromising EEFI. NATO military PA is the function responsible for promoting NATO's military aims and objectives to audiences in order to enhance awareness and understanding of military aspects of the Alliance. This includes planning and conducting media relations, internal communications and community relations. An important facet of any military operation is to communicate the principal themes and messages while providing a clear and complete understanding of the operation, while maintaining OPSEC. Although PA is primarily focused on the need to inform and educate audiences, which results in maintaining NATO public support and hence freedom of action, its impact is much wider. It is therefore

essential that PA staff and Info Ops staff work closely together to ensure that a coordinated message is delivered to the intended audiences. Particular attention must be paid to local and regional media within the JOA and to other media sources that are influential within the JOA as media reports will have an influence on all parties and must be taken into account. While PA and Info Ops have different audiences and delivery channels, coordination of the message and delivery timing is necessary and appropriate. Effective PA provides a commander freedom of action and supports Info Ops in countering adversary propaganda with the truth about operational activities, while protecting OPSEC. The credibility of PA spokespersons as sources of timely and truthful information must not be jeopardised. Under no circumstances is it permissible to lie to the media. To avoid giving the false impression that the media are being manipulated in any way, a clear distinction must be maintained between Info Ops and PA.

0133. PA and Info Ops are separate, but related functions. They directly support military objectives, counter adversary disinformation and deter adversary actions. However, the efforts of PA and Info Ops differ with respect to audience, scope and intent. Therefore, coordination between PA and Info Ops must be assured at all times and at all levels to ensure consistency in the message released by the military to outside audiences and to promote overall effectiveness and credibility of the campaign. Beyond coordination of efforts and messages, PA will have no role in performing the Info Ops function.

Section VII – Roles of Information Operations at the Strategic, Operational and Tactical Levels

0134. **General**. Operations by NATO forces are directed, planned and conducted at three levels of command; direction and guidance are obtained from NATO HQ via the strategic commander, while planning and execution are largely achieved at the operational and tactical levels. The distinction between activities conducted by forces at the different levels is clear, but the effects of political, strategic, operational and tactical levels of joint operations will seldom remain only at one level. This requires special consideration for Info Ops, where interconnected information systems and the psychology of decision-making mean that action at the tactical level can have strategic implication and vice versa. Particular attention must be paid to local and regional media so as to influence local and regional populations. Although a clear distinction between PA and Info Ops must be made, their goals must be coordinated to ensure maximum effect.

0135. **Political and Strategic Level**. At this level, armed forces are used within an overarching political framework and in a synchronised fashion. The Military Committee (MC) considers the contribution that Info Ops can make to the achievement of Alliance overall objectives and provides military advice to the NAC. In forming Info Ops advice as outlined in MC 422/3 '*NATO Military Policy on Information Operations*', the International Military Staff (IMS) on behalf of the MC would consult with the strategic commander to:

a. Recognise any political or legal limitations on the conduct of military information activities, with particular regard to international law, custom and practice, Host Nation agreements/arrangements, support by other nations or other sensitivities.

b. Consider the impact of NAC approved ROE on the application of information activities.

c. Regularly update and inform the Strategic Command (SC) on the focus and progress of the overall Information Objectives, which will include an update of the coordinated messages and themes with non-military activities. This is vital in order to guide and facilitate the planning and execution of military information activities.

d. Ensure coordination of strategic level targeting, including information activities. This applies especially to sensitive targeting such as against computer networks and information technology, population groups or individuals.

0136. Overall Info Ops strategic guidance will be outlined in Annex O to the strategic level OPLAN, if developed. Strategic guidance, under MC133, will usually include available political guidance, strategic goals, directives and limitations. The main body of the OPLAN should address the strategic commander's overall intent. It is the responsibility of the strategic level Info Ops staff to ensure that military coordination with the higher-level political and media aspects of the operation takes place regularly. This feedback loop is crucial in order to ensure that the targeted activities in support of Info Ops at the strategic and operational level are synchronised with other activities.

0137. After the initial coordination process has been established and strategic planning guidance has been issued, the SC Info Ops staff will contribute to further refinement of the OPLAN, Contingency Plan (CONPLAN) or Standing Defence Plan (SDP), taking into account issues from multinational and joint operational planning. Given the scope of the tasks described above and the potential sensitivity of information activities, every consideration should be given to ensure that the strategic level Info Ops staff is established on a full-time basis. This will require sufficient manpower to cope with the information demands from the operational level as well as the requirements of the higher political and military bodies.

0138. **Operational Level Information Operations**. At the operational level, armed forces are deployed, sustained, employed, and redeployed to attain strategic objectives through the conduct of major operations and campaigns without compromising the mission. The JFC is normally responsible for:

a. Identifying the Information Objectives necessary to achieve the CJTF's objectives.

b. Establishing the priorities for achieving the Information Objectives.

c. Providing guidance for allocating forces and resources as necessary for subordinate commanders to execute their tasks. The JFC will maintain the capability to change

the emphasis of information activities at the operational level for the joint campaign to react to developments.

d. Providing military advice on Info Ops to the strategic commander in order to ensure that the objectives given in the strategic commander's OPLAN are met, by conducting Info Ops assessments.

e. Providing guidance to tactical level commanders to enable them to create the desired effects depicted in the OPLAN.

f. Implementation of NATO Crisis Response System (NCRS) measures as required.

0139. **Tactical Level Information Operations**. At the tactical level, armed forces conduct military activity to achieve military objectives assigned to tactical forces. At this level, Info Ops focuses on creating an effect on key local decision-makers and groups by affecting their will, decision-making processes and capabilities. Coordination of information activities to create these effects is vital to the success of the joint campaign. At the same time, activities to protect one's own information and information systems must be conducted.

0140. The component commands and Graduated Readiness Force (GRF) HQs must conduct a mission analysis based on the JFC's campaign and relevant plans and integrate information activities in their plans. The level of planning will be more detailed and localised to the operational environment following guidance and direction from the higher command. At this level, information activities carried out in support of the joint campaign may create a desired effect against decision-makers, their systems and processes, targeted in support of a higher commander's objectives.

Section VIII – Summary

0141. Figure 1.2 offers a pictorial summary of this Chapter's primary theme by showing the top-down relationship between mission specific guidance that provides the context for the selection of appropriate information activities which, in turn, influence the information environment to affect adversaries and other NAC approved targets/audiences.

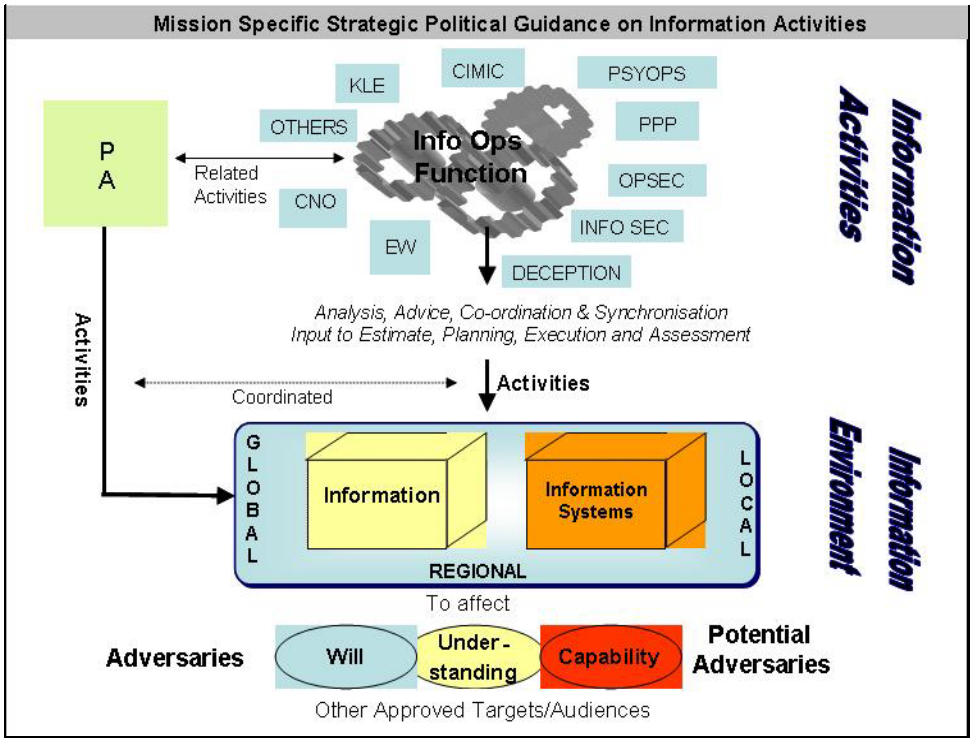


Fig 1.2 Summary of Info Ops Approach

ANNEX 1A – INFORMATION OPERATIONS CRITICAL TERMINOLOGY

1A1. **General**. The purpose of this annex is to provide an illustrative overview of the possible range of actions that could be involved in military information activities (i.e., actions designed to affect information and/or information systems, performed by any actor).

ACTION	DEFINITION
Assess	To pose a judgement after comparing measured performances against a standard.
Canalize	To force someone to take a desired direction in its actions to gain an advantage. To orient the perception of a situation or event toward a desired outcome.
Coerce	To use force or the threat of force or other potentially prejudicial means to persuade a party to adopt a certain pattern of behaviour against his wishes.
Collect, Gather	To assemble, accumulate data or information. To develop knowledge by gradually acquiring data or information.
Compel	To force someone to undertake a desired course of action. (Similar to convince and mislead but not limited to perceptions and generally more lethal in its overtone.)
Contain	To stop, hold, or restrain the spread of information, a message or an effect in a media or (target) audience or on an information system.
Convince	To overcome by argument. To bring to belief, consent, or a course of action.
Coordinate	To bring functions, systems or entities operating in the same environment in proper relation in order to avoid counter-productive results such as duplication of effort or mutually-negating actions.
Corrupt	To alter from the original or correct form or version.
Deceive	To cause a person to believe what is not true. (Deception seeks to mislead adversary decision makers by manipulating their perception of reality.)
Degrade	To reduce the effectiveness or efficiency. (...of an adversary C2 or communications systems, and information collection efforts or means. Info Ops can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions. Damage done the function is permanent, but only portions of the function were affected; that is, the function still operates, but not fully. A function's operation is permanently impaired, but the damage does not extend to all facets of the functions operation.)
Deny	To prevent someone from accessing and using critical information, systems, and services. (Damage done to the function is only temporary, but all aspects of the function were affected. A function's operation is impaired over the short term, but the damage extends to all facets of the function's operation.)
Destroy	To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.

ACTION	DEFINITION
	(Damage done to the function is permanent, and all aspects of the function have been affected. A function's operation is permanently impaired, and the damage extends to all facets of the function's operation.)
Detect	To discover or discern the existence, presence, or fact of an intrusion into information systems.
Deter	To turn aside, discourage, or prevent a potential or actual adversary or other target audience from taking actions that threaten coalition interests
Diminish	To make less or cause less to appear. To reduce the effectiveness of an activity. (This is similar to degrade, without the lethal overtones.)
Disrupt	To break or interrupt the flow of information. To use force or other non-lethal means to shatter the cohesion of a (target) audience and prevent them from functioning effectively. (Damage done to the function is temporary, and only portions of the function were affected. A function's operation is impaired over the short term and the damage does not extend to all facets of the function's operation.)
Exploit	Attempts to gather information that will enable the ability to conduct operations to induce other effects. To gain access to adversary systems to collect information or to plant false or misleading information.
Expose	To make known or cause to be visible to the public eye. To make visible, to reveal something undesirable or injurious.
Influence	To cause a change in the character, thought, or action of a particular entity. (Selected projection or distortion of the truth to persuade the opposition to act in a manner detrimental to their mission accomplishment while benefiting accomplishment of friendly objectives.)
Inform	To impart information or knowledge.
Manipulate	To handle or treat (especially with skill). To manage by dextrous (especially unfair) use of influence.
Mask	To conceal. To cover or keep in check while an action detrimental to mission accomplishment by the opposition is being carried out.
Mislead	To create a false perception that leads someone to act in a manner detrimental to mission accomplishment while benefiting accomplishment of friendly objectives.
Negate, Neutralize	To render ineffective, invalid or unable to perform a particular task or function. To counteract the activity or effect of.
Prevent	To deprive of hope or power of acting or succeeding. To keep from happening, to avert.
Probe	To examine closely in order to evaluate a system or entity to gain an understanding of its general layout and/or perception.
Promote	To contribute to the progress or growth of; further.
Protect, Safeguard	To cover or shield from exposure, damage, or destruction. To keep from harm, attack, injury or exploitation.

ACTION	DEFINITION
	To maintain the status or integrity of. To take action to guard against espionage or capture of sensitive equipment and information.
Shape	To determine or direct the course of events. To modify behaviour by rewarding changes that lend toward a desired response. To cause to conform to a particular form or pattern.
Support	To keep from weakening or failing; strengthen.
Usurp	To take the place of, by or as if by force.

(INTENTIONALLY BLANK)

CHAPTER 2 – INFORMATION OPERATIONS COORDINATION PROCESS AND STAFF REQUIREMENTS

Section I – Introduction

0201. **General**. To achieve success and meet the commanders' objectives, Information Operations (Info Ops) must be fully integrated and coordinated with all other Joint Force actions. To create the desired effects, a coherent and synchronised approach among Headquarters (HQs), adjacent and subordinate commands, and the strategic-political level must be achieved. One of the keys to success is thorough coordination of Information Objectives and related military actions from the strategic to the tactical level. Commanders should ensure that any information activity likely to affect other areas is implemented with prior coordination and notification.

0202. **Information Operations Process**. Figure 1.1 summarised the Info Ops military function as providing advice and coordination of military information activities to meet mission-specific Alliance guidance. To achieve this, Info Ops personnel undertake four major staff activities:

a. Evaluate results from systems analysis of the information environment.

b. Provide advice on the planning and execution of operations in the information environment.

c. Develop Info Ops contributions to planning and assessment from a generalist's perspective.

d. Coordinate the contributions of military capabilities to planning, execution and assessment of activities in the information environment and the resultant effects.

0203. **The Role of the Information Operations Coordination Board**. The Info Ops process is put into effect through the existing HQ coordination processes via an Info Ops Coordination Board (IOCB), which prepares inputs to relevant HQ internal and external processes including the joint targeting processes,[1] the INTEL process[2] and the joint coordination process. A wide range of staff functions play a role in the Info Ops process, as outlined in Annex 2A. Functional area participation in the IOCB is essential in order that their input and subject matter expertise can be applied to the Info Ops coordination process. There needs to be a structured Info Ops coordination process, which allows the Chief Info Ops, chairman of the IOCB, to outline current and future information activities. Of particular importance is the need for all activity to be consistent with mission-specific strategic guidance and a view taken on the potential impact.

[1] This may include a Joint Targeting Working Group (JTWG), a Joint Coordination Board (JCB), a Joint Defence Assets (JDA) Working Group as well as other similar targeting meetings. Time Sensitive Targets (TST) are a particular subset of interest to Info Ops as their effects need to be properly defined and potential unintended effects should be pre-analysed if possible. Details are contained in AJP-3.9 '*Allied Joint for Targeting*'.
[2] In accordance with AJP-2.1 '*Intelligence Procedures*'.

0204. **Planning**. Info Ops staffs should be directly involved from the start as part of the Joint Operations Planning Group (JOPG) and should take part in early discussion including mission analysis.[3] An Info Ops presence on the JOPG is essential, as it is the Info Ops staff who provide input to the overall estimate process in close coordination with the INTEL and other staffs (Further details in Chapter 3).

0205. **Operations**. The IOCB is integrated into the HQ's battle rhythm and meets regularly within the HQ, attended by all relevant staff and Liaison Officers (LOs) from subordinate or superior commands to plan, coordinate and synchronise military information activities. As Info Ops is also relevant in day-to-day business, the IOCB may function as a smaller group and a think-tank for the commander.

0206. **Inter-Command Level Coordination**. Given the potentially wide-ranging effect of military information activities, a coordinated approach is necessary across all command levels and Alliance and host nation political institutions. Thus a system of coordination and liaison processes between commands and supporting agencies that allows staffs to communicate with, send reports to, and receive guidance from, superior and subordinate commands is required.

Section II – Headquarters Internal Coordination and Staff Requirements

0207. **The Information Operations Staff**. The Info Ops staff's (comprising a Chief Info Ops and sufficient supporting staff relative to the HQ size and function) primary role, is to assist the commander in planning, coordinating and directing the implementation of information activities to support the achievement of campaign objectives. HQ staff functions all have Info Ops related requirements that should be included in the planning and conduct of operations. The focus and responsibilities of the Info Ops staff will be determined by the command level and assigned mission. At the operational level, there will be a need for a comprehensive staff to enable planning, operations, INTEL support and specialists to determine targeting and campaign assessment. At the tactical level, the need will focus more on specialists to deliver capability against specified targets. Within the HQ, the Chief Info Ops is responsible for:

a. Providing specific Info Ops input to the development of the commander's direction and guidance.

b. Preparing Info Ops contributions to the commander's plans and orders.

c. Assisting in the determination of the desired effects in support of operational objectives.

[3] Carried out in accordance with the established planning process in Allied Command Operations (ACO) Guidelines for Operational Planning (GOP) Final Revision 1, 4 July 2005 (The ACO GOP is to be replaced in 2010 by a Comprehensive Operations Planning Directive (COPD)). In addition, MC 133/3 Corr 3 dated 18 August 05 and AJP-5 '*Allied Joint Doctrine for Operational Planning*' provides operational planning guidance.

d. Assisting in the determination of all possible military actions to support the attainment Information objectives.

e. Recommending priorities for military information activities.

f. Contributing to the campaign synchronisation and assessment.

g. Coordinating with all principal functional staff areas, special staff and higher and subordinate HQ in support of Info Ops.

h. Chairing the IOCB within the HQ staff.

0208. **Information Operations Staff Structures**. Given the evolving nature of Info Ops and due to command and mission specific requirements, an Info Ops staff can be formed at all levels of command within NATO. Comparable command levels (e.g., JFC, component commander and GRF) should generate similar Info Ops structures within staffs. The structure, number and rank of Info Ops staff will depend on the size, type and complexity of the operation being undertaken, however, the three following example staff structures present possible models, based on a generic NATO command HQ (Figure 2.1), that can be implemented or adapted further depending on the prevailing operational situation:

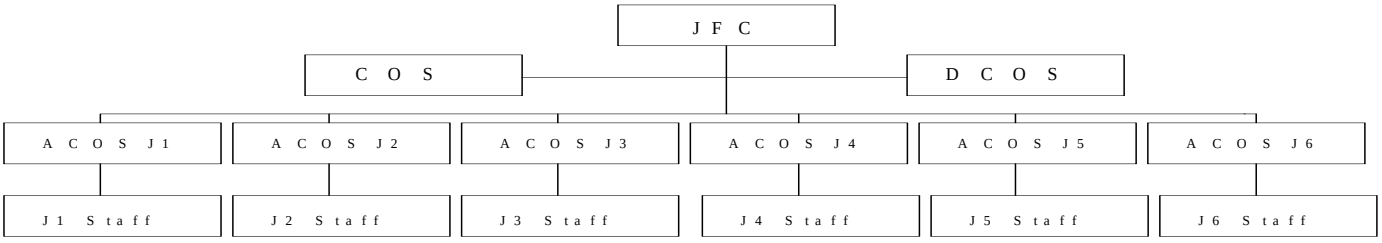


Figure 2.1 Generic NATO HQ

a. Chief Info Ops as member of the HQ's special staff with decentralised Info Ops personnel in J-divisions, probably J2, J3 and J5. This would ensure that Info Ops was fully considered at the highest, decision-making level with close relationships to the command group. Possible disadvantages could result from a reduced involvement of the Chief Info Ops in day-to-day J-staff activities, and from administrative problems inherent in the matrix-type organisation of the Info Ops staff.

b. A centralised Info Ops staff brigaded at Chief of Staff (COS) level under a Chief Info Ops. This would ensure that Info Ops was fully considered at the highest, cross-functional level in planning, execution and assessment of an operation. Possible disadvantages could include a lack of liaison and understanding of the more detailed aspects of the operation, particularly in the J3 and J5 areas.

c. Centralised Info Ops staff at Assistant Chief of Staff (ACOS) COS level under a Chief Info Ops would ensure a greater level of liaison with specialist staffs within the

respective J-division whilst retaining a significant level of senior influence within the HQ, albeit a considerably reduced level compared to the COS construct.

0209. The following should be considered when deciding upon a particular level or structure for Info Ops staff within a command:

a. The core of an Info Ops staff should consist of trained and experienced Info Ops personnel with an understanding of the information environment, aware of available capabilities to conduct information activities, and familiar with general staff procedures.

b. The Info Ops staff should develop and/or improve Info Ops awareness and procedures within their commands, ensuring adequacy to support the planning, conduct and assessment of military information activities.

c. A core Info Ops staff with clearly defined links to other staff elements within the command should be established to ensure Info Ops issues are dealt with adequately. Ideally, the Info Ops staff should include a Chief Info Ops and established personnel to support planning, execution, and assessment, and conduct targeting coordination and external liaison. Info Ops staff must have a clear understanding of the functions of the other staff elements and that there is an exchange of information in a timely manner.

d. Command group understanding of Info Ops is required in order to integrate Info Ops into training, exercises, operations and day-to-day business. Info Ops representation in or close relation to the J3 is needed to ensure sufficient experience and training throughout the HQ.

e. Understanding of the NATO and national capabilities and organisations that conduct information activities is essential. Most, if not all, of these capabilities will come from external organisations. Establishing an ongoing working relationship with these organisations will enable the core Info Ops staff to appropriately contribute to planning, implementation, and assessment of information activities. While some required capabilities are resident within the NATO structure, many of the other required capabilities are only available via the participating nations.

0210. **Targeting Coordination**. To achieve Information Objectives, a coordinated targeting approach is required. This means that the Info Ops staff should participate in both the JTWG and the Joint Targeting Coordination Board (JTCB). All information activities must be closely aligned with the objectives from the JTFC's plans. It is vital that all targeting takes into consideration all possible secondary effects (intended and unintended) that may result in psychological or physical damage. This means the full range of targets affected by military information activities, including adversary decision-making processes, key decision-makers and technical components of information systems, must be coordinated. Info Ops involvement in the joint targeting process is crucial to create required effects in the information environment.

Section III – External Coordination

0211. **General**. To realise desired Information Objectives to meet strategic and political guidance, close coordination of campaign and supporting plans, among strategic, operational and tactical HQs as well as coordination with international and regional political and civil organisations is vital. This coordination up and down the command levels takes the form of formal plans, direction, guidance, doctrine, policy and training.

0212. **Component Commanders/Tactical Level Commanders**. It is important that activity conducted by component commanders and commanders at lower tactical levels are synchronised with activity at higher levels. In addition, commanders at these levels will often be required to conduct activity to support higher level objectives. To ensure synchronisation, proposed information activities may need to be forwarded to superior HQ's Info Ops cells for deconfliction with other ongoing activities. Liaison Officers (LOs) will normally be required during crisis or deployed operations. All LOs must maintain close contact with their command Info Ops staff to ensure they are fully aware of changes and/or requirements to be discussed during the IOCB.

0213. **Information Operations Assessment**. Any viable assessment of information activities requires an inter-command effort as intended and unintended effects can be felt across informational, physical and psychological boundaries. The prerequisite for making an assessment of Info Ops effectiveness is through development of rigorous, measurable and observable Measurements of Effect (MOEs).

(INTENTIONALLY BLANK)

ANNEX 2A – THE INFORMATION OPERATIONS COORDINATION BOARD

2A1. **General**. The IOCB is the forum for the implementation of Info Ops collective coordination and advice. This board, chaired by Chief Info Ops, meets as a subset of the JCB. It will convene as necessary in the HQ decision cycle and as required during non-operational activities.

2A2. **Membership**. Composition of the IOCB is shown in Figure 2A.1. The composition is not fixed and the Chief Info Ops will invite other parties as required to contribute to the mission and the role of Info Ops in accomplishing the commander's objectives. Representatives on the IOCB must have the authority to speak for and make decisions on behalf of their command functional area. IOCB member responsibilities are outlined at paragraph 2A6. If the posts for deception and Operations Security (OPSEC) officers are not established, J3 and/or J5 should cover these areas.

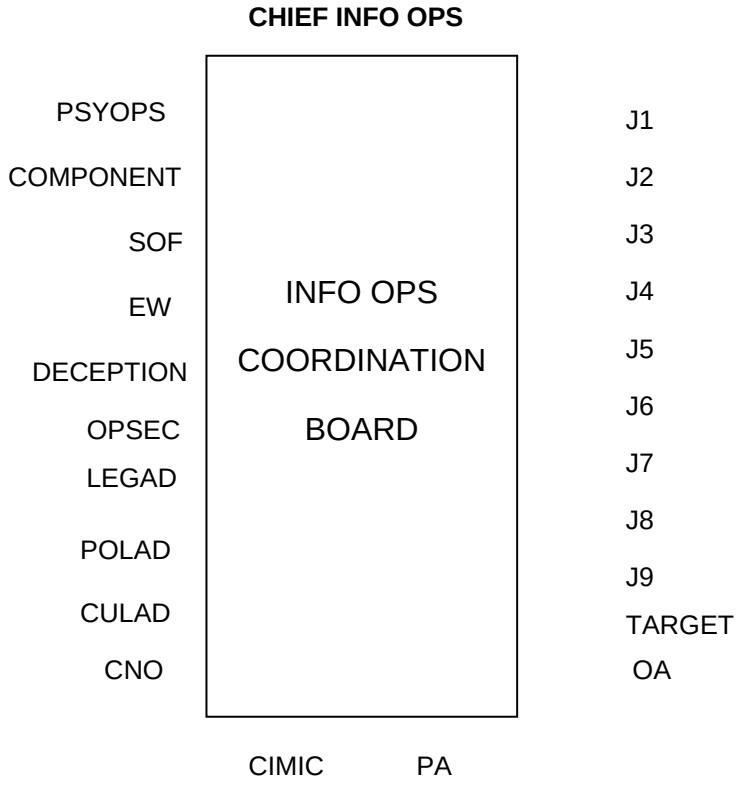


Figure 2A.1 – Information Operations Coordination Board

2A3. **Role**. The role of the IOCB is to ensure that military information activities are coherent and synchronised with other actions (potentially) affecting the information environment. The IOCB provides the forum for collective coordination of the JFC's information activities. Within the scope of its assigned functions, the IOCB will provide initial coordination of

target nominations related to information and information systems to facilitate subsequent harmonisation at the JTCB. It will also provide advice on possible effects in the information environment created by other military actions. The responsible capability representatives, functional advisers or component Liaison Officers (LOs) will present results from IOCB discussions to the JTCB. The Info Ops representative at the JTCB will monitor the selection, harmonisation, nomination and prioritisation process, and advise on over-arching, cross-functional issues, as required. It further provides a forum for coordination, de-confliction and monitoring of Info Ops plans and activities.

2A4. **Responsibility of Representatives**. Representatives provide information on their future intentions and advice on the employment of their assets. Through the IOCB, activities are de-conflicted and intentions amended to ensure coherence before submitting inputs to the JTWG, JCB and, ultimately, the commander for approval. Representatives from the subordinate or component commands, usually Info Ops officers, will provide expertise and act as liaison for Info Ops matters between the higher and subordinate commands. An indication of the contribution of specialist staff, and their requirements of Info Ops staff, is covered in paragraph 2A6.

2A5. **Responsibilities of the Information Operations Coordination Board**. The responsibilities of the IOCB are:

a. Development, revision and assessment of the plans and information activities based on approved Information Objectives.

b. Provision of Info Ops guidance based on commander's guidance and direction.

c. Consideration of activities affecting the information environment.

d. Identification of necessary and available resources and requirements.

e. Recommendations for tasking, coordination and staff action.

f. Review of Info Ops inputs to the main body and annexes to various plans.

g. Development of target nominations for input at the JTWG.

h. Recommendation for approval of the Info Ops Annex O to the OPLAN.

i. Coordination with outside agencies in consultation with other staff areas as required.

2A6. Functional and Special Staff Roles in Support of Information Operations. To maximise the effectiveness of Info Ops, an integrated approach to operations that considers desired effects on the will, capability and understanding of adversaries and other North Atlantic Council (NAC) approved parties must be considered. This requires a coordinated approach to Info Ops across the staff, led by the command group, to achieve a common understanding

of the nature of Info Ops. Specific responsibilities for roles, functional areas and other staffs include:

a. **Commander**. The commander provides direction and guidance to the HQ on Info Ops development and implementation. He[1] also provides advice on Info Ops to the higher levels of command, including assessment of information activities as part of the campaign and for implementation of mission-specific political guidance. The commander is a key Info Ops contributor in his own right, given his ability to influence local events through presence and dialogue, and he also contributes to the wider mission-specific guidance through his direction of all HQ activity.

b. **Chief Information Operations**. The Chief Info Ops at each level is responsible for the overall direction of Info Ops through the HQ coordination and synchronisation process and by chairing the IOCB. The Chief Info Ops leads the coordination process, ensuring prioritisation, de-confliction and unity of purpose for all military information activities undertaken within the command.

c. **Political Adviser**. The Political Adviser (POLAD) advises on policy implications of proposed information activities when required, coordinates the political objectives of information activities with higher HQ counterparts. The POLAD should also coordinate public diplomacy activities with Info Ops staff as part of mission-specific political guidance.

d. **Legal Adviser**. The Legal Adviser (LEGAD) advises on legal implications, including ROE, of proposed information activities, and provides a legal assessment of information activities proposed by the IOCB.

e. **Cultural Adviser**. The Cultural Adviser (CULAD) advises on cultural implications of proposed information activities, including ethnological, religious and social aspects. He also contributes to the assessment of information activities from the cultural perspective.

f. **Operational Analyst**. Using scientific methods, the Operational Analysis (OA) officer provides significant input to all operational and campaign assessments. He is closely associated with Info Ops, advising on and analysing measures of success (Measure of Performance (MOP), Measurement of Effect (MOE), etc) and informing campaign assessments. His advice and output will be applied throughout the iterative planning, execution and review cycle, in particular in relation to the information environment.

g. **Public Affairs**. Public Affairs (PA) is the commander's interface with the media and the public. PA at each level of command directly supports the commander and should

[1] The use of 'he or his' refers to a person of unspecified sex throughout this publication.

not be further delegated or subordinated to other staff functions. The chief, Public Affairs Officer (PAO) directly reports to the commander. Info Ops officers will not be used in a PA role and, conversely, PA officers will not be used in an Info Ops role; there shall be no personnel overlaps during operations in staff designated for Info Ops on the one hand and PAOs on the other. The PAO is responsible to the commander for all media relations, internal communication and community relations plans and activity. He coordinates with Info Ops staff to ensure that PA and other military information activities are mutually consistent.

h. **J1**. J1 participates when personnel matters are included in the information activities. J1 also identifies personnel requirements and shortfalls.

i. **J2**. J2 coordinates INTEL collection requirements and analytical support for Info Ops. INTEL will provide the initial systems analysis, to include a description of the political/military decision-making process and decision-makers, a Communications and Information Systems (CIS) nodal analysis, human/cultural factors and an analysis of other entities' capabilities to affect the information environment. J2 assists in the assessment of activities and the resulting effects and advises on the capability of all-source INTEL support to Info Ops to include targeting.

j. **J3**. J3 plans, advises on and integrates planning of effects and activities in the information environment into the HQ's deliberate short and mid-term planning process. J3 operations provide subject matter expertise in support of the planning and execution of information activities.

k. **J4**. J4 considers the effects of information activity on logistics and support, including any Info Ops requirements. The role of engineers is particularly significant in relation to Info Ops given their vital role in CIMIC activities.

l. **J5**. J5 integrates Info Ops planning into the deliberate long-term planning process (including deception planning). Info Ops is driven by and supports J5 through the Operation Planning Group (OPG) process.

m. **J6**. J6 identifies CIS vulnerabilities and develops procedures and capabilities to protect friendly battle management consultation, command, control, communications and information systems. J6 develops INFOSEC plans and supports the development of OPSEC plans. J6 also assesses the impact of adversary information activities on own systems and maintains a restricted frequency list in conjunction with the Chief Info Ops and J2. J6 coordinates specialist support relating to protection of own CIS to include the coordination of electromagnetic spectrum (i.e., sensors, radars, telemetry devices).

n. **J7**. Training of Info Ops and specialist staff will be an important element in creating the desired information effects in each phase of the operation.

o. **J8**. Financial Management (FM) support enhances the commander's ability to manage and apply available resources at the right time and place in a fiscally responsible manner. FM provides the capability for full spectrum finance and resource management support.

p. **J9**. J9 advises on CIMIC capabilities and assessments that support Information Objectives and coordinates activities with Info Ops staff. J9 can also provide useful feedback on the progress of information activities.

q. **Psychological Operations**. The PSYOPS representative (who may be embedded staff) advises on PSYOPS support and coordinates PSYOPS with other military information activities during the Operational Planning Process (OPP). PSYOPS also initiates PSYOPS plans and the subsequent targeting process and is a key contributor of information activities.

r. **Special Operations Forces**. The Special Operations Force (SOF) representative (who may be embedded staff) provides advice on SOF capabilities and force utilisation in support of information activities.

s. **Liaison Officers**. LOs provide critical linkages between their parent organisation and the JFC HQ, ensuring the activities of both are mutually supportive. Typically, HQ external LOs will be required during crisis or deployed operations. There needs to be a good understanding by LOs of plans, methods and capabilities for information activities available to the command for the operation.

t. **Electronic Warfare Officer**. EW supports information activities by denying, deceiving, exploiting or degrading adversary information and information systems, and at the same time collecting information. It is a capability that requires close coordination to prevent unintended effects to friendly systems. The EW officer should provide advice on EW support to Info Ops and provide feedback on its effectiveness.

u. **Operations Security Officer**. The J3/J5 OPSEC officer is responsible for the identification and protection of EEFI.

v. **Deception Officer**. The J3/J5 deception officer is responsible for recommending deception targets, formulating deception objectives, planning the deception effort, supervising its execution, developing MOE, and controlling termination of the deception effort.

w. **Targeting Officer**. The targeting officer ensures that the IOCB planning activities are synchronised within the targeting matrix and the joint prioritised target list. He also assists in targeting deconfliction and assists in assessment of effects following the conduct of information activities.

x. **Computer Network Operations**. The CNO officer advises on CNO support to proposed information activities, including assessments of effects on computers and computer networks.

CHAPTER 3 – PLANNING

Section I – Overall Planning Considerations for Information Operations

0301. **General**. Info Ops is an integral part of military activity at every level of command. It is therefore critical that Info Ops factors are considered in the Operational Planning Process (OPP) from the beginning. Planning of effects and activities in the information environment must directly support the commander's intent, guidance and desired end-state. Info Ops staff should be core members of relevant staff planning sub-groups, including the Operational Planning Group (OPG), and provide inputs to planning for the Joint Targeting Process (JTP). An Info Ops estimate will usually be conducted (either as a written product or as a less formal process) to ensure that all potential information activities and their intended effects are properly considered and then fed into the commander's estimate process. A summary of plans and outputs for Info Ops is shown at Table 3.1 at the end of this Chapter.

0302. **Inclusion**. Planning of activities to create desired effects in the information environment to support achievement of objectives, provides significant input to advance and crisis response planning and is conducted in accordance with MC 133/3, AJP-5 and the primary planning tool, the ACO Guidelines for Operational Planning (GOP).[1] This planning may be conducted simultaneously at all command levels, depending on the nature of the operation and the scope of the plan being developed. There are important links to be established with the OPG looking at the overall commander's campaign and also with other groups involved in contingency planning and current operations planning. It is imperative that Info Ops is not added on afterwards, but integrated into planning from the beginning while Decisive Points and Centres of Gravity are being identified as a central aspect. It is equally important that planning for Info Ops is considered during the Joint Intelligence Preparation of the Battlespace (JIPB) process.

0303. **Integration**. The Info Ops staff needs to understand the other aspects of the commander's plan and how they may impact on planned activities in the information environment (and supporting plans) and ensure that Info Ops are integrated into the overall plan, without conflict with other elements and functions. This means that the Info Ops planners must maintain a broad perspective with respect to how other operations can impact on Info Ops, taking a protracted amount of time to complete or involving several synchronous operations and activities.

0304. **Planning for Sensitive Issues**. Certain information activities may be considered sensitive due to the nature of the activities, audiences or targets. This type of planning may have to be

[1] ACO's Guidelines for Operational Planning (GOP) Final Revision 1, 4 July 2005 (The ACO GOP is to be replaced in 2010 by a Comprehensive Operations Planning Directive (COPD)). In addition, MC 133/3 '*Operations Planning System*', Corr 3 dated 18 August 2005 and AJP-5 '*Allied Joint Doctrine for Operational Planning*' provide operational planning guidance.

conducted within a sub-group of the OPG. Briefing of sensitive plans or those which are classified above the level of the overall operation will have to be conducted separately on the basis of 'need to know' and should be marked with a Limited Distribution (LIMDIS) caveat. Plans should always be considered for sensitivity marking if they address deception, the use of special information technology, political sensitivities or if plans involve using SOF.

Section II – Detailed Planning

0305. **Initiation**. Once the North Atlantic Council (NAC) initiating directive is issued planning commences.[2] Mission-specific strategic political guidance on information activities should be developed at NATO HQ and this should be analysed by SC planners and Info Ops staff to begin laying the groundwork for mission analysis and JIPB. RFIs can be generated (and special expertise/knowledge requested) to better understand the target spectrum and to determine the vulnerabilities, strengths and weaknesses of potential targets in the information environment.

0306. **Orientation**. During this stage, the Info Ops staff strive to visualise the information environment, understand the adversary and other NAC approved parties, and follow the decision-making processes and systems involved using the detailed JIPB.

a. The Info Ops staff contributes to the development of mission analysis and produce the initial Info Ops contribution to the estimate. This contribution will feed the mission analysis brief, which will lead to the commander's planning guidance. Among other considerations, the Info Ops staff must also understand the threat posed to friendly information systems and decision-making.

b. The Info Ops estimate process ensures that important factors affecting the formulation of planning of effects and activities in the information environment are taken into consideration. It is a collaborative process (involving functional/capability experts through the IOCB and bi-lateral coordination) that provides the foundation on which Courses of Action (COAs) are developed and tasks identified. The overall estimate process, which is built on the JIPB, also helps to identify gaps in knowledge that may be filled by intensified research or the use of RFIs. See Annex 3A for the Info Ops element of the command estimate process.

0307. **Concept Development**. In the concept development stage, Info Ops has to give advice to the JOPG in order to define Decisive Points, which can exist in time, space, forces and the information environment and have to be logically determined from Critical Requirements and Critical Vulnerabilities. Additionally, Info Ops will contribute to development of the COAs, including comparison of different COAs from an Info Ops perspective (both from own forces

[2] MC role for Operational Planning Process according to MC 133/3 '*Operations Planning System*', Corr 3 dated 18 August 2005 refers.

view and adversary) and identification of the COA that Info Ops can best support. During this stage:

a. Info Ops staff will contribute to the development of the commander's Concept of Operations (CONOPS). This will form the basis for the development of the Annex O to the commander's OPLAN.

b. The Info Ops planners will identify the Information Objectives and activities related to the commander's overall objectives and consistent with strategic-political guidance. The Info Ops matrix, with numbering, is initiated at this point. Directly linking the Information Objectives with the commander's objectives will help ensure plan coherency. It should also be aligned with the mission-specific strategic political guidance or higher-level Information Objectives. This linkage will also provide a more precise ability to conduct Info Ops assessment and to address required plan changes.

0308. **Plan Development**. The role of Info Ops may be expressed within the main body of the OPLAN, e.g. in the ('Coordinating Instructions' paragraph) and in the Annex A ('Concept of Operations'). Information Objectives are expressed at Annex O of the OPLAN, including themes and messages from mission-specific strategic political guidance. Also, at this stage, Info Ops staff will contribute to the development of the Commander's Critical Information Requirements (CCIRs). RFIs will be continuously reviewed and submitted during this phase.

a. SUPLANs of military functions/capabilities will focus on creating the desired effects, taking into account Information Objectives listed in the OPLAN Annex O. These SUPLANS will describe the overall sequencing and execution of various information activities, each designed to create specific effects and formulate requirements for determining the measurement of success.

b. Within the JCB process, Info Ops will also contribute to the development of Fragmentary Orders (FRAGOs) that contain coordinating instructions for the conduct of current operations. These FRAGOs should address necessary updates to coordinated information activities and formulate requirements for the measurement of success (e.g. MOPs, MOEs).

0309. **Campaign Plan Review**. Throughout the planning process, the Info Ops staff will continue to conduct theatre assessment focused on the information environment, and contribute to the refinement/adjustment of estimates and plans. This will require constant synchronisation of the planning of information activities with feedback to mission-specific strategic political guidance.

Section III – Outputs from Information Activity Planning

0310. **General**. The functions and processes indicated above will lead to the production of key information activity planning products (Annex O and Objective Matrix) in support of

operational plans and executive papers. The products are applicable for both training and operations. Standard formats should be developed and used as guidance for Info Ops staffs within command standard operating procedures.

0311. **Info Ops Elements of the Operation Plan**. The strategic commander's plan is required to provide overall guidance to the operational planner. It should, as a minimum, cover details concerning strategic political intent and any restraints, constraints or limitations placed on Info Ops planners. The desired effects from information activities, themes and messages generated from the specific Information Objectives distilled from mission-specific guidance will be listed in the Info Ops matrix within Annex O. Subordinate commanders will use this matrix as a basis for their own plans. Info Ops must be developed to support both mission-specific guidance and the overall JFC's campaign plan and consequently Info Ops staff must ensure that the 2 requirements are melded together and potential conflicts of interest highlighted. Info Ops must be integrated in all operational activity; at times it may be the main effort. The Info Ops staff will be responsible for providing the following elements as part of the OPLAN (an outline Info Ops Annex O is at Annex 3B):

a. The commander's intent concerning desired changes in the information environment.

b. Information Objectives derived from mission-specific strategic and political guidance on information activities.

c. HQ internal and external coordinating instructions concerning the implementation of the Info Ops function within their own and subordinate commands.

d. Info Ops considerations concerning INTEL, targeting and assessment of effects in the information environment.

e. Coordination and support to the primary contributors of information activities will be included as cross-references to the appropriate functional annexes. These cross-references are not fixed but will be situation and mission dependent.

0312. **Information Operations Contribution to Fragmentary Orders**. A FRAGO is an abbreviated form of an Operation Order (OPORD), issued as required, that eliminates the need for restating information contained in a basic OPLAN or OPORD. Is serves to adjust ongoing operations to situation developments and/or to changed/updated superior direction and guidance. Within the Joint Coordination Board (JCB) process, Info Ops contributes aspects concerning the information environment that affect the conduct of information activities and require additional coordination effort.

0313. **Information Operations Contribution to Target Nomination**. Info Ops assist in the targeting process by identifying where information activities could be applied to create specific effects in support of the JFC's mission objectives. During planning and continuously as part of implementation, target nominations are required in order to implement information activities. These targets will be coordinated through the Info Ops process (e.g. using the IOCB as a coordination forum) and can include a diverse array of subjects including

decision-making systems, information systems and other linked activities. The cyclic target development process during planning must include Info Ops input, from the strategic to tactical levels.

0314. **Analysis of Adversary Information Activities**. The Info Ops staff will review adversary capabilities and information objectives to identify those that will require countering or exploitation. This systems-of-systems analysis of the adversary provides fundamental information on adversary abilities and own exposed areas. This review is conducted through the IOCB in conjunction with other staff branches as appropriate. The analysis must also consider the impact of any constraints or restraints imposed by higher authority such as:

a. Mission-specific political guidance on information activities and themes.

b. Political, legal and Rules of Engagement (ROE) issues, with particular regard to international law, custom and practice, host nation agreements/arrangements, support by other Nations and other sensitivities.

c. Those arising from social and cultural attitudes which will limit information activity options and lead to development of rules of behaviour, for example:

(1) Alliance or coalition sensitivities.

(2) Ethical and religious issues.

0315. **Force and Capability Coordination**. To ensure that information activities and appropriate staff manning are inserted in good time into the force requirements, a clear analysis must be carried out to determine broadly what activities are needed to support the CONOPS and commander's plan. This is a continuous process and requires regular review.

0316. **Briefings**. Briefings are an output of planning and must be tailored to the commander and senior staff in order to provide the understanding of the Information Objectives before the details of plans become clear. Incorporation of information activities into plans from the outset will help ensure that Info Ops aspects are included in regular briefings. There will also be a need for further detailed briefings for information activities and for subordinate commands. Sensitive material and subjects may require compartmented or secure briefing facilities and LIMDIS briefs.

STAGE	OPP STAGE STEPS	INFO OPS PLANNING	INFO OPS PRODUCTS/OUTPUT
Initiation	Review NAC Initiating Directive	Initial work on Mission Analysis Activate IOCB Instigate RFIs	Contribute to JIPB Initial Info Ops Estimate
Orientation	Mission Analysis Commander's Planning Guidance	IOCB ongoing: Determine Information Objectives Initial Info Ops Estimate refinement process – Contribute to targeting – Contribute to CCIR – Contribute to Priority Intelligence Requirements (PIR) – Contribute to JIPB	Initial Info Ops Estimate Info Ops contribution to the Mission Analysis briefing (Information Objectives)
Concept Development	Develop COAs Develop CONOPS	IOCB ongoing: Define Info Ops support for each COA Input to targeting matrix Input to decision brief	Info Ops input to CONOPS Info Ops contribution to the decision briefing (effects to support Information Objectives)
Plan Development	Develop and Coordinate Plan	IOCB ongoing: Coordinate and write Info Ops Annex O Contribute to targeting Annex.	OPLAN Annex O: including Info Ops matrix; Info Ops contributions to FRAGOs.
Plan Review	Plan Review/Evaluation Update Plan	Assessment via ongoing IOCB: Updates to Annex O as required	Required Updates to Annex O

Table 3.1 - Info Ops Planning Activity and Outputs

ANNEX 3A – THE INFORMATION OPERATIONS ELEMENT OF THE STAFF ESTIMATE PROCESS

3A1. **General**. Info Ops contribute to the staff estimate throughout the operational planning process and conduct of operations. The following guidance addresses Info Ops considerations at the various stages of the command estimate process, and which can be conducted as either a written Info Ops estimate, or as a thought process that feeds into the overall staff estimate, as required. It should be updated through an iterative process that involves Intelligence (INTEL) systems analysis as well as functional/capability expertise and will contribute to overall situational awareness and understanding.

3A2. **Analysis of Strategic and Political Guidance**. The Info Ops staff will continuously review mission-specific strategic and political guidance for information activities to reaffirm relevancy of Information Objectives, planned desired effects in the information environment and information activities. The Info Ops estimate should contain an updated comparison of strategic guidance (information objectives, themes and messages) and Joint Force Commander's (JFC's) Info Ops intent and plans. Related assessments should be translated as feedback and advice to superior authorities.

3A3. **Description of the Information Environment**. The Info Ops estimate should focus on the description and assessment of the information environment in a systemic context including at least relevant actors, specific information systems, and the media. This description and assessment cannot be done in isolation by the Info Ops staff, but needs to be coordinated and draw from functional/capability expertise without duplicating others' analysis efforts. The resulting product should be considered as a summary of collective situation analysis.

a. **Actors**.

(1) Individuals (e.g., decision-makers and leaders; opinion leaders, opinion formers and spin doctors; journalists, editors, and media publishers).

(2) Groups (population as a whole or in parts; e.g., by region, ethnicity, religion, activity; groups of the above individuals).

(3) Organisations (government agencies & governmental organisations; IOs, NGOs, private volunteer organizations; regional and international enterprises; organisations of the above individuals and groups).

(4) Actors need to be described by relevant characteristics, including their:

(a) Personalities (comprising factors such as: psychological profiles/traits and personal history; culture, motives, interests, values, beliefs, attitudes, and stances; risk aversion, and sensitivities).

(b) Diverse roles – official and unofficial.

(c) Perceptions, images, and opinions (How do actors see themselves and other actors? How do actors want to be seen? To what extent do actors trust the international community, coalition, coalition partners, other actors?).

(d) Information flow and opinion-forming processes, main sources of information and trust in those.

(e) Intent and capabilities for conducting information activities/protecting the information environment against activities.

(f) Balance of power, including military, economic, socio-cultural, and religious aspects; in particular, control over media, communication/information processes and/or related means and infrastructure.

(g) Security situation and its stability, robustness, and sustainability.

(h) Supporters, and followers, and their respective subsistence levels; support-networks; relationships to other actors with regard to politics, security, economy, and psychology.

(i) Possible political, strategic, operational, and tactical short-, mid-, and long-term objectives, as well as their hierarchical schemes and prioritization of objectives (What do the actors want to achieve? How will they act in the information environment?).

(j) Interrelationships and interdependencies between and among actors.

(k) Receptivity, addressing the psychological and technical/physical ability/capability of an actor to perceive/receive messages in any format (e.g., literacy, availability of radio/TV sets); this also includes aspects of external control such as censorship.

(l) Susceptibility, addressing those issues that attract the actors' attention, regardless of the possible resulting effects when consuming; also: 'areas of interest' for the actors (e.g., things they would read in a newspaper or programs they would tune into a radio station); these are often related to attitudes and values.

(m) Vulnerability, addressing those issues that directly affect cognition and emotion of the actors and can be exploited by own actions to create desired effects; assessment is based on results of present social research and refers to anxieties/fears and needs rather than to attitudes.

b. **Specific Information Systems**.

(1) CIS: equipment, methods and procedures and, if necessary, personnel, organised to accomplish information processing and transfer functions.

(2) Command and Control (C2) systems: equipment, methods and procedures (including planning and decision-making tools) and personnel that enable commanders and their staffs to exercise command and control.

(3) Relevant characteristics and components of CIS/C2 systems include:

(a) Personnel (including actors in the above sense).

(b) Command and control philosophy, in terms of decision-making processes, organisation, and communication and information flow patterns (including aspects such as censorship and freedom of opinion).

(c) Technical equipment, techniques, platforms, and organisations used, established, and required to receive, process, and transmit data and information, including their functionality, detailed features, capacity, and level of interoperability, robustness, redundancy, and reliability; this includes system elements and components from (human and technical) sensors throughout the loop to shooters (e.g., IT in weapons systems).

(d) Infrastructure (official and unofficial), including commercial facilities and installations related to telecommunication companies and networks, postal and courier services, broadcast or media dissemination facilities such as fixed and mobile radio stations, platforms.

(e) Support dependencies, such as related to energy, water, transportation, and maintenance.

c. **Media**.

(1) Personnel (e.g., management, owners, financiers, stakeholders, publishers, editors, journalists, employees).

(2) Assets (official and unofficial, open and covert; used or employed by actors for indirect communication, information, entertainment, and other related purposes, including traditional communication, new and emerging media):

(a) Contents (themes and messages).

(b) Reach/area of influence.

(c) Affiliation.

(d) Credibility.

(e) Availability.

(3) Infrastructure (including related industries and media production facilities, e.g., studios and printing shops).

3A4. **Status of Own Information Activities**. The Info Ops estimate should include an overview of available own capabilities, tools and techniques for conducting military information activities, including their current state of readiness, involvement in current operations and principle limitations. This part of the estimate should be contributed to by the responsible capability representatives, functional advisors or component LOs. Chapter 1, Sections V and VI provide initial guidance for structuring this part of the estimate.

3A5. **Status of Adversary Information Activities**. The Info Ops estimate should also include an overview of adversary capabilities, tools and techniques for conducting military information activities, including their (assumed) intent and objectives, current state of readiness, involvement in current operations, principle limitations and vulnerabilities. This part of the estimate should be contributed to by INTEL in coordination with the responsible capability representatives, functional advisors or component LOs.

3A6. **Possible Effects in the Information Environment**. The Info Ops estimate should conclude with a list of possible effects, considering all 3 activity areas outlined in Chapter 1, Section IV. Effects must be formulated in a way that describes the physical and/or behavioural state of a part of the information environment (see Paragraph 3A3) that results from an action or set of actions. They should be characterised as desired or undesired. In addition, the Info Ops staff should consider possible trends (developments, evolutions) that may occur over time without own interference.

ANNEX 3B – OPERATION PLAN ANNEX O FORMAT

ANNEX O TO
OPLAN xxxx
TITLE xxxx
DATED dd mm yyyy

INFORMATION OPERATIONS

References:

1. **(xx)**[1] **SITUATION**.

   a. **General**. See main text.

   b. **Specific**.

      (1) **Information Environment**. Summary of mission-relevant aspects of the information environment, taken from the Info Ops Estimate.

      (2) **Strategic Guidance**. Summary of mission-specific strategic and political guidance on information activities (Information Objectives, themes and messages).

      (3) **Own Information Activities**. Summary of the status of own information activities, taken from the Info Ops Estimate.

      (4) **Adversary Information Activities**. Summary of the status of adversary information activities, taken from the Info Ops Estimate.

2. **(xx) MISSION**.

   a. **Strategic Command**. Statement of the superior commander's intent towards the information environment, taken from the strategic OPLAN, Annex O (if available).

   b. **Joint Force Command**. Statement of the commander's intent towards the information environment, taken from the OPLAN, Paragraph 3a.

3. **(xx) EXECUTION**.

   a. **Information Objectives**. List of Information Objectives that are to be achieved or contributed to by military means, derived from mission-specific strategic and political guidance on information activities and the strategic OPLAN, Annex O (if available).

[1] Abbreviated classification.

b. **Themes and Messages**. Taken from mission-specific strategic and political guidance on information activities and the strategic OPLAN, Annex O (if available).

c. **Desired Effects**. Prioritised list of desired effects in the information environment.

d. **Primary Contributors**. Cross-reference to appropriate functional annexes of capabilities conducting or contributing to information activities.

e. **Key Leaders Engagement**. Guidance on the development of the KLEP.

3. **(xx) COORDINATING INSTRUCTIONS**.

a. **Information Operations Coordination Board**. Guidance on the IOCB composition and process in support of the JCB, taken from the relevant SOPs (if available).

b. **Analysis Support**. Guidance on INTEL/systems analysis support to Info Ops as well as contributions by capabilities conducting or contributing to information activities, with cross-reference to appropriate functional annexes.

c. **Targeting**. Guidance concerning the coordination of target nominations in support of the JTCB, taken from the relevant SOP (if available).

d. **Measurement of Success**. Reference to effects listed in Paragraph 3.c: guidance on the coordinated/collective assessment of MOE.

e. **Info Ops Reporting**. Guidance on contributions to reporting concerning information activities and effects in the information environment, with cross-reference to appropriate functional annexes.

APPENDIX: Info Ops Matrix (Format: see Annex 3C)

ANNEX 3C – INFORMATION OPERATIONS OBJECTIVES MATRIX FORMAT (EXAMPLE)

Serial	Information Objectives (from strat/pol guidance)	Commander's Military Objectives	Priority	Effects	Themes	Messages	MOE	Co-ordination Requirements (information activities)	Remarks

(INTENTIONALLY BLANK)

CHAPTER 4 – COMPETENCIES AND TRAINING

Section I – Information Operations Staff Skills and Competencies

0401. Info Ops staff should be able to contribute to all aspects of the Operational Planning Process (OPP) and coordinate information activities based on a sound knowledge of the information environment. A vital prerequisite for this is an understanding of the functional capabilities contributing to or performing information activities, and experience of general HQ processes at the operational level. Therefore, Info Ops staff require appropriate levels of experience, training and qualifications to discharge the Info Ops staff activities described in Chapters 2 and 3.

0402. Info Ops staff activities include evaluation and interpretation of analysis results, advice to planning and execution, contribution to planning and assessment, and the coordination of contributions by military capabilities. In particular:

a. Evaluation and interpretation of results from Systems Analysis concerning the information environment.

(1) Establishment, development and utilisation of information relationships (Subject Matter Expert (SME) network).

(2) Assessment of the situation:

(a) Description of the operational environment related to information and information systems (considering global/strategic aspects).

(b) Mission analysis/analysis of (strategic) guidance for creating effects in the information environment.

(c) Analysis of limitations (assumptions, constraints and restraints) for information activities.

(d) Identification of own capabilities for creating effects in the information environment.

(e) Identification of others' capabilities for creating effects in the information environment, considering allied, friendly, neutral and (potentially) adversary actors.

(3) Estimate of the situation:

(a) Comparison of the actual and aspired situation in the information environment (variance analysis related to the situation and mission).

(b) Identification and evaluation of possible trends (developments, evolutions) in the information environment.

(c) Identification and evaluation of possible and desired effects in the information environment that can be created by military means.

(d) Identification and evaluation of the vulnerability of own information and information systems and respective protection requirements.

(e) Development of the Info Ops estimate (see Annex 3A).

(4) Development of contributions to situation update and decision briefings.

(5) Development of contributions to the enhancement of situational awareness and understanding, and the development of the Common Operational Picture (COP).

(6) Formulation of (additional) information needs, Requests for Information (RFI), and requirements for systems analysis.

b. Advice to planning and execution of operations regarding effects in the information environment.

(1) Briefing the commander and staff on the situation, possible effects and developments in the information environment.

(2) Identification of possible trade-offs regarding effects in the information environment.

(3) Monitoring of the conduct of information activities and variance analysis concerning planned/desired and actual effects.

(4) Identification of coordination requirements for military and civil actors conducting information activities.

(5) Identification of collaborative opportunities for military and civil actors conducting information activities (description of possible synergetic effects).

(6) Participation in various staff activities related to:

(a) Operational planning (including targeting) and exercise planning.

(b) Conduct of operations (including targeting) and exercises.

(7) Proposal of training programs to promote integration of the information factor in planning and execution of operations.

c. Info Ops contributions to planning and assessment from a general list’s perspective.

(1) Formulation of Information Objectives and requirements for effects in the information environment, including MOEs.

(2) Development of Info Ops contributions to general planning products, including contributions to the development and implementation of mission-specific strategic and political guidance for information activities at appropriate levels of command.

(3) Proposal of activities for key leaders engagement (command group and special staff), and designing the Key Leaders Engagement Plan (KLEP).

(4) Development and proposal of common assessment criteria for information activities.

(5) Identification of differences and commonalities in the assessments of military capabilities regarding information activities.

(6) Analysis of indications and reports, and formulation of Info Ops contributions to Battle Damage Assessment (BDA)/Key Task Accomplishment (KTA)/Combat Assessment (CA).

(7) Formulation of Info Ops contributions to the reporting system.

d. Coordination of contributions by military capabilities to planning, execution and assessment regarding effects in the information environment.

(1) Harmonisation and synchronisation of proposed information activities, including proposals for the KLEP.

(2) Harmonisation and consolidation of individual assessments of military and civil information activities.

(3) Harmonisation of individual contributions to the development of the COP concerning the information environment.

(4) Participation in various staff activities related to:

(a) Operational planning (including targeting) and exercise planning.

(b) Conduct of operations (including targeting) and exercises.

(c) BDA/KTA/CA.

(d) Evaluation of exercises and operations (lessons learned).

0403. Specific Info Ops staff skills and competencies – derived from these staff activities – include:

a. A comprehensive and systemic understanding of the information environment.

(1) Basic principles of complex systems (Systems Theory).

(2) Basic principles of Systems Analysis (systemic analysis).

(3) Basic principles of operations research, and modelling and simulation.

(4) A conceptual model of relevant aspects of the operational environment for information and information systems (see paragraph 3A3):

(a) Recognition of system structures and dynamics.

(b) Balancing complexity reduction vs. complexity management.

(c) Selection and assessment criteria for factors that determine system behaviour.

(5) Procedures and structures for the collaboration with personnel/agencies with assigned Systems Analysis/INTEL functions:

(a) Roles and responsibilities of advisors and analysts vs. planners and operators.

(b) Significance of the focusing of planning and conduct of operations on information and information systems.

(6) Basic principles of intercultural competence and human communication.

b. Basic knowledge about own and others' capabilities for creating effects in the information environment:

(1) Options for providing specific direction and guidance (e.g., mission-specific strategic and political guidance for information activities).

(2) Available and relevant assets/means/methods (military and civil) for creating effects in the information environment, including their capacity and employment principles:

(a) Assets, means and methods for conducting information activities.

(b) Possible effects of mainstream activity in the information environment.

(c) Interfaces and starting-points for synergetic effects and/or trade-offs.

(3) Basic methods and techniques for the measurement of success (MOPs and MOEs).

(4) Legal aspects involved in the employment of above capabilities, including ROE.

c. Process management skills, including components of information management and visualisation techniques:

(1) Deepened knowledge and skills for staff duty:

(a) Possible staff structures (emphasis on particularities of joint and combined headquarters).

(b) Basic staff processes (e.g., JCB, Joint Operations Centre (JOC), JTWG, OPG), including battle rhythm.

(2) Methods and tools:

(a) Info Ops estimate.

(b) KLEP.

(c) Info Ops matrix.

(3) Recognition of the importance of the establishment and development of expert networks, and the collaboration with SMEs.

(4) Preparation, conduct and evaluation of coordination processes:

(a) Information Operations Coordination Board (IOCB) (see Annex 2A).

(b) Details of the coordination with members of the command group and special staff.

(c) Details of the consultation with civil actors.

0404. Furthermore, Info Ops staff should have gained literacy and/or experience in the following areas:

a. Understanding an effects-based approach to operations and the comprehensive approach.

b. Understanding information as an operational factor.

c. Creativity skills (for adapting plans for information activities to specific environments).

d. Holistic and analytical thinking skills.

e. Leadership and moderation skills.

f. Social competence and communication skills.

Section II – Individual and Collective Training for Information Operations Staff

0405. Prior to employment in a NATO context, nominated Info Ops personnel should have undertaken one of the 2 NATO Info Ops courses (senior officers or staff officers) at the NATO School, Oberammergau (NSO) and/or to have undergone a similar level of national training, if possible.

0406. In addition to the formal training courses outlined above, individual training can be undertaken with personnel grouped for training depending on their role and function in a HQ staff. Those involved daily with Info Ops, either by being an integral part of an Info Ops staff or indirectly involved through working in another section, will require a higher level of understanding and training than personnel who will just gain some limited exposure during exercises. Additionally there is a general requirement to train all staff to have a basic understanding of the Info Ops process and to train the command groups to understand how Info Ops can benefit them and how to best employ the resources/capabilities at their disposal.

0407. Personnel augmenting a staff for exercises or operations need to be properly qualified and should have some experience prior to filling the posts. Sufficiently detailed job descriptions for each Info Ops billet should be prepared and posted or distributed during the planning phase for operations or exercises.

0408. Augmentees to HQs must receive the latest policy, doctrine and SOP information concerning Info Ops prior to filling an Info Ops post. This will enable them to properly prepare for their functions. Failure to do this may cause augmentees to spend several days reviewing basic doctrine and policy instead of fulfilling their post. Attending NSO courses in Info Ops and related applications will help provide the augmentees with a basis of knowledge and understanding.

Section III – Training Activities for Key Leaders

0409. It is crucial that the key leaders gain an understanding of the Info Ops function, information activities and the effects that can be created. The training of key leaders in Info Ops will greatly improve their understanding of how Info Ops can contribute to the mission, and thereby enable the Chief Info Ops to gain approval for Info Ops contributions to plans and operations within an environment supportive of Info Ops. Training for key leadership can be provided through attendance at various senior officer courses run at the NSO and through national resources.

0410. Key leader knowledge of Info Ops will also help to ensure that Info Ops becomes central to plans and exercises. The Chief Info Ops should take every opportunity to brief and update key leaders to ensure they understand the importance and central role of Info Ops.

Section IV – Headquarters Functional Area Internal Training

0411. It is important that functional staff divisions and specialist staff also benefit from Info Ops training to enable them to effectively work and integrate with Info Ops staff to maximise the Info Ops contribution to the mission. Training could include lectures, pre-exercise briefings, and mini-exercises to develop aspects of Info Ops, to ensure that the entire HQ staff is aware of the strengths and benefits of Info Ops and that they incorporate them into all unit training.

Section V – Integrating Information Operations within Exercises

0412. Outside structural exercise planning, there is a real need for the Info Ops staff to be fully involved in the preparation of strategic, operational or tactical exercises. Info Ops has many links across the spectrum of exercise training objectives and operational planning. Info Ops should therefore be integrated from the beginning of the exercise planning process through exercise analysis and the identification of lessons learned. Integration of Info Ops is considered particularly relevant for command post exercises, study periods, seminars and map exercises to develop the Info Ops knowledge and understanding of commanders and their key staff.

0413. Equally important are manpower and forces for exercises. Depending on the type of exercise being conducted, serious consideration should be given to the manning of Info Ops staff and the expertise required, especially since much of the staff is often built through augmentation. Other role players and directing staffs, who control, coordinate and synchronise the Info Ops contribution from the adversary's perspective should be considered early in the planning process. There will also be the need for inter-agency coordination and cooperation with civil actors such as International Organisations (IOs), non-Governmental Organisations (NGOs) and other civil representatives involved in exercising Info Ops.

0414. When considering the training objectives of each unit participating in the exercise, the type of training, forces and units required should be determined. Certain manoeuvre operation elements and the more technical aspects of information activities such as Electronic Warfare (EW) and CNO are best trained during a live exercise, which may include everything from providing tactical jamming assets to playing the role of adversary key decision-makers.

0415. Early allocation or request for units is essential together with an understanding of their intended role in the exercise. The limitations and other restrictions for operating those forces need to be resolved in the early stages of planning.

0416. An exercise analysis plan should be created as part of exercise planning to ensure that valuable lessons identified before, during or after the exercise can be addressed. This may be in concert with the Joint Analysis and Lesson Learned Centre or as a stand-alone event dependent on exercise status, size and complexity. Lessons should be captured during exercise runtime so that they can be addressed, changed during the exercise (if necessary) and can also be included in later analysis.

(INTENTIONALLY BLANK)

LEXICON PART 1 – ABBREVIATIONS

ACOS	Assistant Chief of Staff
AJP	Allied Joint Publication
BDA	Battle Damage Assessment
DIME	Diplomacy, Information, Military and Economic
CA	Combat Assessment
CCIR	Commander' Critical Information Requirement
CIMIC	Civil Military Cooperation
CIS	Communications and Information System
CJTF	Combined Joint Task Force
CJTFC	Combined Joint Task Force Commander
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COA	Course of Action
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	Concept of Operations
CONPLAN	Contingency Plan
COS	Chief of Staff
COP	Common Operational Picture
CULAD	Cultural Advisor
C2	Command and Control
DIME	Diplomatic, informational, military and economic
DJTF	Deployed Joint Task Force
EEFI	Essential Elements Friendly Information
EW	Electronic Warfare
FM	Financial Management
FRAGO	Fragmentary Order
GOP	Guidance for Operational Planning (now referred to as Comprehensive Operational Planning Directive (COPD)
GRF	Graduation Readiness Force
HQ	Headquarters

IC	International Community
IER	Information Exchange Requirement
IMS	International Military Staff
INFOSEC	Information Security
Info Ops	Information Operations
INTEL	Intelligence
IO	International Organisation
IOCB	Information Operations Coordination Board
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JCB	Joint Coordination Board
JDA	Joint Defence Asset
JFC	Joint Force Commander
JIPB	Joint Intelligence Preparation of the Battlespace
JOA	Joint Operations Area
JOC	Joint Operations Centre
JOPG	Joint Operations Planning Group
JTFC	Joint Task Force Commander
JTCB	Joint Targeting Coordination Board
JTP	Joint Targeting Process
JTWG	Joint Targeting Working Group
KLEP	Key Leaders Engagement Plan
KTA	Key Task Accomplishment
LEGAD	Legal Advisor
LIMDIS	Limited Distribution
LO	Liaison Officer
MC	Military Committee (NATO)
MOE	Measurement of Effect
MOP	Measure of Performance
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organisation
NCRS	NATO Crisis Response System
NGO	Non-Governmental Organisation
NSO	NATO School Oberammergau
OA	Operational Analysis
OPG	Operational Planning Group
OPLAN	Operational Plan
OPORD	Operational Order

OPP	Operational Planning Process
OPSEC	Operations Security
PA	Public Affairs
PIR	Priority Intelligence Requirement
POLAD	Political Advisor
PSYOPS	Psychological Operations
RFI	Request for Information
ROE	Rules of Engagement
SC	Strategic Command
SDP	Standing Defence Plan
SME	Subject Matter Expert
SOF	Special Operations Force
SOP	Standard Operating Procedure
SUPLAN	Supporting Plan
TST	Time Sensitive Targeting

(INTENTIONALLY BLANK)

LEXICON PART 2 – TERMS AND DEFINITIONS

The primary references for terms and their definitions are indicated in parentheses.[1] Those marked (AJP-3.10) are new and will be incorporated in AAP-6 '*NATO Glossary of Terms and Definitions*' following ratification and agreement of the Military Committee Terminology Conference (MCTC).

Centre of Gravity
Characteristics, capabilities or localities from which a nation, an alliance, a military force or other grouping derives its freedom of action, physical strength or will to fight. (AAP-6)

Combined Joint Task Force
A combined (multinational) and joint (multi-service) deployable task force, tailored to the mission, and formed for the full range of the Alliance's military missions. (MC 389/2)

Computer Network Attack
Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: a computer network attack is a type of cyber attack (2005). (AAP-6)

Computer Network Defence
Actions to protect against disruption, denial, degradation or destruction of information resident in computers and computer networks and the networks themselves. (AAP-6)

Computer Network Exploitation
Action taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage. (AAP-6)

Computer Network Operations
Computer Network Operations (consisting of Computer Network Attack, Exploitation, and Protection) seek to gain access to computer networks to disrupt, deny, degrade or destroy their capability, or alternatively to intercept and utilise their capability, whilst protecting the capability of the joint task force. Success in this aspect is directly proportional to the adversary's dependence on such systems. (AJP-3.10)

Course of Action
In the estimate process, an option that will accomplish or contribute to the accomplishment of a mission or task, and from which a detailed plan is developed. (AAP-6)

Critical Vulnerability
A vulnerability in a fighting force's system which, if destroyed or otherwise controlled, will lead to a dynamic disruption of that force. (AJP-3.10)

[1] AAP-6 '*NATO Glossary of Terms and Definitions*'.

Decisive Point
A point from which a hostile or friendly centre of gravity can be threatened. This point may exist in time, space or the information environment. (AAP-6)

Host Nation
A nation which by agreement:

a. receives forces and materiel of NATO or other nations operating on/from or transiting through its territory;
b. allows materiel and/or NATO organisations to be located on its territory;
c. provides support for these purposes. (AAP-6)

Information Activities
Actions designed to affect information and/or information systems. They can be performed by any actor and include protection measures. (AJP-3.10)

Information Environment
The virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems. (MC 422/3)

Information Objectives
Provide statements of measurable response that reflect the aspired conditions in the information environment as a result of information activities. They enable analysis, planning, execution/management and assessment/evaluation of related actions and/or effects. (AJP-3.10)

Information Operations
Is a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capabilities of adversaries and other NAC approved parties in support of Alliance mission objectives. (AJP-3.10)

Information Security
The protection of information (stored, processed, or transmitted), as well as the host systems, against a loss of confidentiality, integrity and availability through a variety of procedural, technical and administrative controls. (AJP-3.10)

Information Systems
Information systems are socio-technical systems for the collection, processing and dissemination of information. They comprise personnel, technical components, organisational structures and processes that create, collect, perceive, analyse, assess, structure, manipulate, store, retrieve, display, share, transmit and disseminate information. (AJP-3.10)

Joint Operations Area
A temporary area defined by the Supreme Allied Commander Europe, in which a designated joint commander plans and executes a specific mission at the operational level of war. A joint operations area and its defining parameters, such as time, scope of the mission and geographical area, are contingency - or mission-specific and are normally associated with combined joint task force operations. (AAP-6)

Measurement of Effect
Assessment of the realisation of specified effects. (AJP-3-10)

Operations Security
The process which gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities and intentions of friendly forces. (AAP-6)

Public Affairs
NATO military PA is the function responsible to promote NATO's military aims and objectives to audiences in order to enhance awareness and understanding of military aspects of the Alliance. This includes planning and conducting media relations, internal communication and community relations. (MC 457/1)

(INTENTIONALLY BLANK)