National Defence / Défense Nationale

B-GJ-005-200/FP-000

Joint Doctrine Manual

JOINT INTELLIGENCE DOCTRINE

(Supersedes B-GG-005-004/AF-008 dated 1995-05-24)

(ENGLISH)

Issued on Authority of the Chief of Defence Staff

Custodian: J2 PLANS POL **2003-05-21**

CANADIAN FORCES
FORCES CANADIENNES
WWW.FORCES.GC.CA

Canada

LIST OF EFFECTIVE PAGES

1. Insert latest changed pages, dispose of superseded pages in accordance with applicable orders.

2. Dates of issue for original and changed pages are:

Original	0	2003-02-13	Change	3	
Change	1		Change	4	
Change	2		Change	5	

3. Zero in Change No. Column indicates an original page. Total number of pages in this publication is 100 consisting of the following:

Page No.	Change No.
Title	0
A	0
i to vi	0
1-1 to 1-8	0
2-1 to 2-18	0
3-1 to 3-12	0
3A-1 to 3A-2	0
3B-1 to 3B-2	0
4-1 to 4-12	0
4A-1 to 4A-2	0
4B-1 to 4B-4	0
5-1 to 5-10	0
5-1 to 5-10	0
6-1 to 6-8	0
GL-1 to GL-4	0
LA-1 to LA-4	0
REF-1 to REF-2	0
INDEX-1 to INDEX-6	0

PREFACE

1. Intelligence is fundamental to success in military operations. The aim of this publication is to provide a national doctrine for the use of intelligence in support of CF operations. It can be used in the training of personnel in the principles and practice of intelligence; by operational staffs wishing to know how intelligence can support their operations; and as guidance for intelligence staffs in the performance of their duties. As with all doctrine, it should be read in the spirit in which it was written: that is to say, as *guidance* and *suggestions* as to how intelligence should work and be used, rather than as a set of rules to be slavishly followed in all instances.

2. This keystone publication is subordinate to the CF capstone doctrine publication - “Canadian Forces Doctrine” (B-GJ-005-000/AF-000). Joint Intelligence Doctrine provides guidance and principles, which amplify the doctrine on intelligence described in outline in the CF Operations manual (B-GG-005-004/AF-000). This publication will supplement manuals produced by Environmental Commands and formations describing intelligence doctrine specific to single-service operations. In any joint or nationally directed operation, the intelligence doctrine described in this publication will take precedence over single-service doctrine.

FOREWORD

1. This publication is a guide for all those involved in the intelligence process. This includes those responsible for directing and resourcing the intelligence effort and those using intelligence products (commanders and their staffs), as well as intelligence staffs and organizations involved in executing the intelligence function. This manual does not address domestic operations. Specific guidance regarding the employment of intelligence resources of the CF in domestic operations is contained in NDHQ Instruction DCDS Directive 2/98.[1]

2. *Joint Intelligence Doctrine* is organized as follows:

   a. Chapter 1 – The Nature of Intelligence;

   b. Chapter 2 – The Intelligence Process;

   c. Chapter 3 – Intelligence Practice;

   d. Chapter 4 – Intelligence Support to Planning;

   e. Chapter 5 – Operational Intelligence; and

   f. Chapter 6 – Guidelines for Joint Intelligence Practice.

3. To promote interoperability and to ensure consistency to the maximum extent possible with the doctrine of our principal allies, this publication draws upon related US, NATO, UK and AUS publications, which are recorded in the List of References. AJP 2.0 – Allied Joint Intelligence, Counter-Intelligence and Security Doctrine is the NATO publication that provides similar guidance to that contained in this publication.

4. Recommendations for amendments to this publication are welcome and should be forwarded to National Defence Headquarters, attention J2 Plans Pol 3.

5. The Joint Capability Requirements Board is the ratification (approval) authority for this publication

[1] See 3301-1 (DCDS) dated 10 Jul 98 DCDS 2/98 (Guidance for the Conduct of Domestic Operations), paragraph 75, page 20.

TABLE OF CONTENTS

List of Effective Pages ..... B
Preface i
Foreword ii

CHAPTER 1 - THE NATURE OF INTELLIGENCE 1-1

SECTION I – INTRODUCTION 1-1

101. The Need for Intelligence 1-1
102. The Role of Intelligence 1-1
103. Aims 1-1
104. Meaning of Intelligence 1-2

SECTION II – OVERVIEW OF KEY INTELLIGENCE FUNCTIONS 1-4

105. Indications and Warning (I&W) 1-4
106. Intelligence Preparation of the Battlespace (IPB) 1-4
107. Common Operational Picture (COP) And Situational Awareness (SA) 1-4
108. Support to Targeting 1-4
109. Force Protection 1-5
110. Counter-Intelligence 1-5
111. Manage Intelligence Effort 1-6

CHAPTER 2 - THE INTELLIGENCE PROCESS 2-1

201. Levels and Types Of Intelligence 2-1
202. Levels of Intelligence 2-1
203. Types of Intelligence 2-1
204. Definitions 2-2
205. The Principles of Intelligence 2-3
206. The Intelligence Cycle 2-3
207. Direction 2-4
208. Collection 2-6
209. Processing 2-8
210. Dissemination 2-12
211. Intelligence Sources and Agencies 2-15

CHAPTER 3 - INTELLIGENCE PRACTICE 3-1

301. Introduction 3-1
302. Joint Intelligence Staff Structures 3-1
303. Liaison 3-2
304. Joint Intelligence Architecture and Planning 3-2
305. Principles 3-2
306. Communications Capability 3-3
307. Planning the Architecture 3-4

308. Intelligence Staff Process 3-4
309. Information Management....3-5
310. Collection Management....3-5
311. Intelligence Requirements Management....3-6
312. Collection Co-Ordination 3-6
313. CCIRM Staff Procedures....3-7
314. Summary 3-7
315. Product Types....3-8
316. Threat and Risk Products....3-8
317. Basic Intelligence Products 3-8
318. Military Capability Assessments and Studies....3-9
319. Operations Specific Products 3-9
320. Reports and Summaries....3-9
321. Intelligence Operations....3-10

ANNEX A - INTELLIGENCE DATABASES....3A-1

3A01. Intelligence Databases 3A-1
3A02. Database Standards....3A-2
3A03. Database Management 3A-2

ANNEX B - FORMAT FOR A COLLECTION PLAN....3B-1

CHAPTER 4 - INTELLIGENCE SUPPORT TO PLANNING....4-1

401. Introduction....4-1
402. Intelligence Staff Responsibilities....4-1
403. The CF Operational Planning Process (CF OPP)....4-1
404. Intelligence Preparation of The Battlespace (IPB) 4-2
405. Use of IPB....4-3
406. The IPB Concept 4-3
407. IPB and the Intelligence Cycle....4-3
408. IPB Process....4-3
409. Application 4-4
410. IPB and the Targeting Process....4-4
411. Information Operations (IO)....4-5
412. Intelligence Support to IO 4-6
413. Intelligence, Surveillance and Reconnaissance 4-6
414. ISR Concept of Operations....4-8
415. Conclusion....4-9
416. The Intelligence Estimate 4-9
417. Methodology for the Estimate....4-9
418. Factors to be Considered 4-10
419. Principles 4-10
420. Additional Guidance 4-10
421. Types of Intelligence Estimates....4-11

ANNEX A - FORMAT FOR AN INTELLIGENCE ESTIMATE 4A-1
ANNEX B - INTELLIGENCE ANNEX FORMAT 4B-1

CHAPTER 5 - OPERATIONAL INTELLIGENCE 5-1

501. Introduction 5-1
502. Joint Operations 5-1
503. Purpose of Intelligence at the Operational Level 5-1
504. Overview of Intelligence Requirements 5-2
505. Intelligence Support To Planning 5-3
506. CF Operational Planning Process (CF OPP) 5-3
507. Joint Intelligence Preparation of the Battlespace (JIPB) 5-4
508. Intelligence Support to Operations 5-4
509. Intelligence, Surveillance and Reconnaissance (ISR) 5-4
510. Joint Targeting 5-4
511. Intelligence and Information Operations (IO) at the Operational Level 5-5
512. Intelligence Support to Post Conflict Operations 5-5
513. Joint Intelligence Architecture 5-5
514. Characteristics 5-5
515. Planning Considerations 5-6
516. Requirements 5-6
517. The Intelligence Task Organization 5-6
518. Joint Intelligence Centre 5-7
519. National Intelligence Cells 5-8
520. Collection Planning 5-8

CHAPTER 6 - GUIDELINES FOR JOINT INTELLIGENCE PRACTICE 6-1

601. Analyse Operational Intelligence in Context 6-1
602. Define Support 6-1
603. Involve the J2 staff 6-2
604. Constitute Joint Intelligence Staffs 6-2
605. Synchronize Effort 6-2
606. Understand Requirement 6-2
607. Establish Capability 6-2
608. Strategic Support 6-3
609. Ensure Unity of Effort 6-3
610. Make all Organic Intelligence Capabilities Available to the Entire Joint Task Force 6-4
611. View the Adversary as Joint or Unified 6-4
612. Keep Operational Intelligence Current 6-4
613. Maintain Flexibility 6-4
614. Ensure Accessibility of Intelligence 6-4
615. Use an All-Source Approach 6-5
616. Distinguish between Fact and Assessment 6-5
617. Use Liaison 6-5

618. Prioritise Component Information Requirements 6-6
619. Recognise Counter-Intelligence as a Source of Information....6-6
620. Employ All Deployed Forces as Sources 6-6
621. Use the Chain of Command to Satisfy Requests for Information....6-6
622. Structure for Continuous Operations....6-6
623. Use Intelligence Lessons Identified....6-7

GLOSSARY GL-1

LIST OF ABBREVIATIONS....LA-1

LIST OF REFERENCES REF-1

INDEX INDEX-3

LIST OF FIGURES

Figure 1-1 Information and Intelligence Relationship 1-3
Figure 2-1 The Relationship between AO, AIR and AII 2-3
Figure 2-2 The Intelligence Cycle 2-4
Figure 3-1 The CCIRM Process....3-5
Figure 4-1 Information and Intelligence Flows in an ISR system....4-9

LIST OF TABLES

Table 2-1 Reliability Ratings 2-10

CHAPTER 1

THE NATURE OF INTELLIGENCE

"By 'intelligence' we mean every sort of information about the enemy and his country - the basis, in short, of our plans and operations."

Karl von Clausewitz, On War, 1832

SECTION I – INTRODUCTION

101. THE NEED FOR INTELLIGENCE

1. Intelligence is an essential component of military capability. It exists at all levels of command to support commanders and their staffs in making effective decisions by providing them with a timely and accurate understanding of the adversary and operational environment. No operation can be planned with real hope of success until sufficient information on the adversary and environment has been obtained and converted into intelligence. No less important is the need to counter adversaries' similar efforts by depriving them of knowledge of our own actions, dispositions, capabilities and intentions.

2. Intelligence, in a military context, is the product of our knowledge and understanding of the physical environment; weather, demographics and culture of the operational area, the activities, capabilities and intentions of an actual or potential threat, or any other entity or situation with which the Canadian Forces is concerned. Intelligence is fundamental to the planning and conduct of operations, and to force protection, through all dimensions of conflict as it allows the commander to gain control of the threat or situation and mastery of the environment.

3. Intelligence provides the commander with an assessment of the adversary's capability and activities as well as an estimate of the adversary's probable courses of action, centres of gravity and vulnerabilities. The possession of intelligence may afford a critical advantage over the adversary in that the commander, by getting inside the adversary's decision cycle, may be able to act or react more quickly than the opponent. A commander can therefore plan actions based on this knowledge, which will decrease the risks inherent in operational activity and increase the likelihood of success.

4. Intelligence is "command led", which means that the Commander must drive the intelligence process and, while he has his Intelligence staff to advise him, he must have a firm understanding of the intelligence process, its strengths and its limitations. He must have the capability to frame his intelligence requirements succinctly and to interpret the intelligence derived in response to his requirements in the context of his mission.

102. THE ROLE OF INTELLIGENCE

1. The role of intelligence is to assist in the Commander's visualization of the joint battlespace, which will involve the assessment of adversary capabilities, centres of gravity and probable intent. In order to fulfill this role the intelligence system must be able to attain the following objectives:

a. Provide warning;

b. Inform decision making via predictive analysis;

c. Contribute to situational awareness and to attaining the "knowledge edge" over an opponent; and

d. Counter the adversary's intelligence effort.

103. AIMS

1. Intelligence seeks to provide the commander:

a. Warning of threats in time to take effective (preventive, pre-emptive or protective) counter action.

b. A knowledge and understanding of the capabilities, intentions, actions and vulnerabilities of an adversary.

c. A knowledge and understanding of the environment and situation.

d. An insight into friendly vulnerabilities to enemy action including intelligence collection, psychological operations and deception.

104. MEANING OF INTELLIGENCE.

1. In different contexts the term *intelligence* can refer to the organization performing the intelligence function, the activity associated with the conduct of the intelligence function or, more commonly, the product or output which fulfils the role and aims of the function. There is an inherent distinction between information and intelligence.

2. **Information.** Information consists of a single item of data or a series or group of items of data, which is captured by a sensor and is subsequently collected by one means or another from that sensor. It is a statement of a state of affairs that exists, or has existed, at some point in time and space. It is unequivocal in nature and can relate to events in the past or the present; being historical or current. It is defined as "unprocessed data of every description which may be used in the production of intelligence[2]"

3. In operations, the commander will have access to very large amounts of information relating to every aspect of the operational environment. Information will be available to him covering an extremely wide range of matters relating to both his own and his opponent's forces; their numbers, identity, equipment, location, state of re-supply, numbers of casualties, state of reinforcement, fuel states, ammunition states and many other facts. There will also be an equally large volume of information concerning the battlespace environment, the climate, the weather, the terrain, socio-political influences and other aspects of the battlespace.

4. In preparing to conduct his decision making process, the commander will be able to identify, from the outset, what information, relating to both the adversary and friendly forces, he requires to be able to reach a decision and make his plan.

5. **Intelligence.** Information is of great value when a deduction of some sort can be drawn from it. Information on its own is a fact or a series of facts but when it is related to other information already known, and when it is considered in the light of past experience, it will give rise to a new set of facts, which is called intelligence. Intelligence differs from information in that, being the result of a process of subjective *judgement*, it is not unequivocal and is open to challenge. The relating of one set of information to another or the judgement of information against a data base of knowledge already held and the drawing of conclusions by an analyst, is the analytical "process" which is at the root of the production of intelligence from information. The relationship between data, information and intelligence is shown diagrammatically in Figure 1-1 below.

[2] NATO, Glossary of Terms and Definitions (AAP-6 (2002))

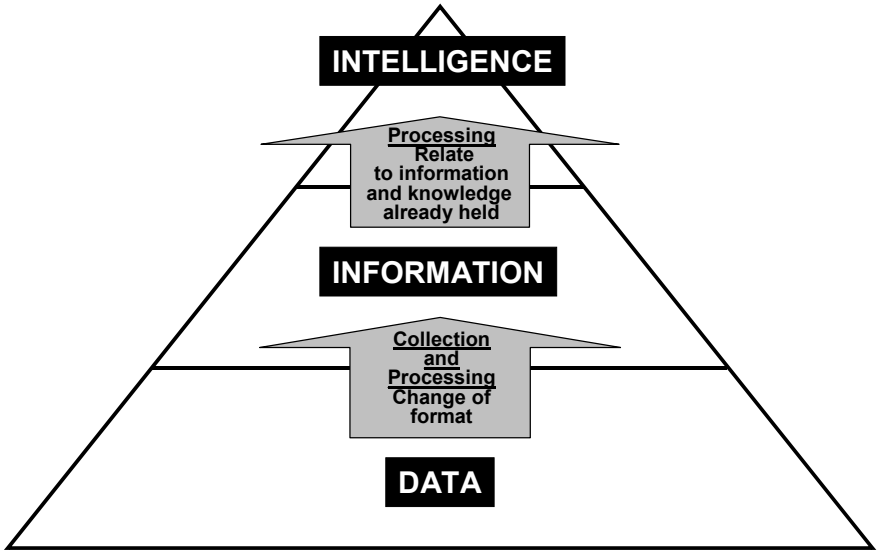

Figure 1-1 Information and Intelligence Relationship

6. Intelligence provides the commander with a *prediction* of his adversary's likely tactics or an *assessment* of his capabilities and intentions. The possession of intelligence affords him a critical advantage over the adversary in that he is able to 'get inside' his opponent's mind and form an insight into what the adversary's actions or reactions are likely to be. The commander can therefore plan his own actions based on this knowledge thus decreasing the risks inherent in combat and increasing the likelihood of success.

7. Intelligence is defined as "The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements or areas of actual or potential operations.[3]"The term is also applied to the activity which gives rise to intelligence and as a generic title, to those who carry out the process, which leads to its production.

[3] Ibid

SECTION II – OVERVIEW OF KEY INTELLIGENCE FUNCTIONS

105. INDICATIONS AND WARNING (I&W)

1. An I&W system is based on the identification of a series of specific activities or indicators which are relatively easily recognised and which are linked either individually or together to a less easily identifiable activity which is being carried out by an adversary. A range of indicators is identified in advance of an operation and forms Information Requirements (IRs) that lead to the tasking of sources and agencies. As the operation develops, the range of indicators is expanded to cover all the options open to an opponent. Wherever possible, multiple indicators are developed for each case to prevent deception and increase collateral for the identification of the activity to which the indicators are linked. I&W systems in peacetime may use a variety of triggers in addition to those normally used in time of war. These will include amongst others, political, social, religious and economic triggers.

106. INTELLIGENCE PREPARATION OF THE BATTLESPACE (IPB)

1. IPB is a graphical analytical methodology that is conducted by intelligence organizations to produce intelligence products in support of the commander's decision-making process. It is a continuous process[4] that involves:

a. Defining the battlespace environment.

b. Describing the battlespace's effects.

c. Evaluating the adversary.

d. Determining the adversary's potential Courses of Action (COA).

2. IPB products are used by Joint Force and Component staffs in preparing their estimates and are also used in the analysis and selection of friendly COA and generally to direct intelligence operations in support of current and future missions.[5]

107. COMMON OPERATIONAL PICTURE (COP) AND SITUATIONAL AWARENESS (SA)

1. The COP is a snapshot in time of friendly, neutral and adversary forces and of the battlespace environment. It is formed from the output from the database of information and intelligence which is common throughout a level of command and which is disseminated throughout that level of command. The COP informs the commander's SA which is his understanding of the operational environment in the context of his mission. Comprehensive SA is an effective aid to decision making. Intelligence is a primary feed, but not the sole one, to the COP.[6]

108. SUPPORT TO TARGETING

1. Targeting is the process of selecting adversary forces, geographic areas, installations, or activities planned for capture, degradation, destruction or neutralization and matching the appropriate response to them. Targeting includes intelligence, operational and planning functions and involves the use of lethal or non-lethal force, by conventional and unconventional delivery means. The goal of targeting intelligence is to support target analysis and attack recommendations and to assist in mission planning and execution. Targeting intelligence can be broken down into three broad categories: Target System Analysis, Collateral Damage Estimation and Battle Damage Assessment.

---

4 The NATO IPB process consists of three steps, which are described, in detail in NATO AJP 2.1 Intelligence Procedures.

5 For a complete description of the IPB process see the Land Forces Intelligence Field Manual (B-GL-357-001/FP-001) which was derived from ABCA QSTAG 1034 and the definitive US FM 34-130.

6 Additional information on the COP is available in the CF COP CONOPs (revised draft 11 Jul 02)

2. Target System Analysis is the process of identifying and analyzing a target system to identify exploitable vulnerabilities and weaknesses. Target System Analysis is conducted at all levels of command. At the Strategic level, analysis focuses on large national systems such as military campaigns, military-industrial production, transportation, etc. At the Operational/Tactical levels analysis focuses on sub-systems such as an airfield or the POL or munitions storage areas of an airfield.

3. Collateral Damage Estimation (CDE) is the process of determining the unintended results of applying either with lethal or non-lethal force to a predetermined objective. In assessing collateral damage, the proposed weaponeering solution is applied to the target and its surroundings, paying specific attention to local demographics and sensitive civilian objects. Depending on Commander's Direction and Guidance, the results of CDE can cause the commander to request attack authority from higher authorities or to have the targeting staff revise the proposed weaponeering solution.

4. Battle Damage Assessment (BDA) is the process of determining the effects following the application of either lethal or non-lethal force to a predetermined objective. BDA incorporates physical, functional and system damage assessments. BDA along with Munitions Effects Assessment, which is primarily a J3 function, are the key elements in Combat Assessment stage of the targeting cycle.

109. FORCE PROTECTION

1. Effective force protection provides a greater degree for the freedom of movement and action by commanders, which would otherwise be degraded in the event of successful attack. The basic foundation for effective force protection measures rests with the accurate assessment of conventional, asymmetric, environmental, health and hygiene, and accidental threats.

2. Conventional threats are those normally faced by friendly forces in the course of classic military operations. Asymmetric threats are those used to circumvent or undermine an opponent's strength by exploiting weaknesses, using methods that differ significantly from the opponent's usual method of operation. It may include hostile use of information operations, weapons of mass destruction and/or other non-conventional operations. Extreme weather, health and hygiene conditions also exert a threat to a military force requiring effective force protection measures to remove, mitigate, displace or accept risk.

3. From an Intelligence point of view, the effectiveness of a Commander's force protection plan will be dependent upon the *fusion* of multi-source Intelligence to identify and to assess the threat in a timely and accurate manner.

110. COUNTER-INTELLIGENCE

1. Counter-Intelligence (CI) involves those activities that both identify and counteract the threat to security posed by foreign intelligence services or by individual(s) engaged in espionage, sabotage, subversion, terrorism and/or organized crime. The main thrust of the CI effort is directly related to force protection of DND/CF personnel, information, plans and resources, both in Canada and overseas.

2. The conduct of CI operations requires a high degree of functional integration with intelligence operations. Whereas intelligence is aimed at shaping friendly visualisation of the adversary, CI is employed to shape how the adversary perceives and visualises friendly capabilities and intentions. CI creates uncertainty in the mind of an adversary, degrading his decision making capability by denying him information required to conduct effective operations against friendly forces. CI assets constitute much more than mere collection assets and possess the capability of implementing active countermeasures.

3. Fundamental CI activities in support of operational commanders are:

   a. Early activation as part of strategic and operational reconnaissance and estimates;

   b. Support to deployment security, including the examination of embarkation, transit and debarkation points;

c. Support to Operations Security (OPSEC);

d. Creation of a multi-disciplinary CI team by the inclusion of counter human intelligence, counter signals intelligence and counter terrorism assets operating in a common theatre of operations;

e. Conduct of CI Source Operations and support to HUMINT;

f. Security investigations; and

g. Screening operations, including the security screening of locally engaged employees (CF deployments only).

111. MANAGE INTELLIGENCE EFFORT

1. Operational and intelligence planning will be integrated from the outset of the planning process for a campaign or operation. The Intelligence staff will carry out the following actions prior to deployment:

a. **Establish Mission and Tasks.**

(1) Clarify the Intelligence missions, tasks and requirements

(2) Work with all staff elements to identify the Commander's Critical Information Requirements (CCIR) and from these, develop the Commanders Priority Intelligence Requirements (PIR).

(3) Develop Information Requirements (IRs) both within and external to the formation.

(4) Develop the Intelligence Architecture.

(5) Identify resources to establish and manage the intelligence architecture.

(6) Identify and task organize intelligence resources including collection assets.

b. **Identify What Support is Required.**

(1) Identify requirement for external intelligence assets.

(2) Identify requirement for additional personnel.

(3) Arrange training of any augmenting personnel.

c. **Collection Management.**

(1) Determine intelligence requirements.

(2) Build the Collection Plan

(3) Establish time schedule for collection.

(4) Identify any shortfalls in collection capacity.

(5) Develop information requirements to cover shortfall and forward to the next level of command.

(6) Coordinate ACINT, HUMINT, IMINT, MASINT, OSINT, RADINT and SIGINT collection.

d. **Intelligence Production Management.**

(1) Confirm and update PIR.

(2) Complete intelligence assessment and update where appropriate.

e. **Dissemination Management.** Plan for the dissemination of information and intelligence through a robust intelligence architecture.

f. **Multinational Integration.** Establish liaison between joint and multinational force intelligence structures.

This Page Intentionally Blank

CHAPTER 2

THE INTELLIGENCE PROCESS

201. LEVELS AND TYPES OF INTELLIGENCE

1. To assist in the management of the intelligence process, intelligence is categorized by levels and types.

202. LEVELS OF INTELLIGENCE

1. There are three levels of intelligence the categorisation of which is based on the use that is to be made of the intelligence.

a. **Strategic Intelligence.** "Intelligence, which is required for the formation of policy and military plans at national and international levels"[7]. This is the highest level of intelligence derived from information gathered over the widest possible area in response to requirements placed by national governments across the complete spectrum of national and international military, diplomatic, political and economic matters (that is, NDHQ)

b. **Operational Intelligence.** "Intelligence required for the planning and conduct of campaigns at the operational level"[8]. More specifically, it is the intelligence required for the planning, execution and support of campaigns and operations within a Theatre of Operations by a Joint Headquarters.

c. **Tactical Intelligence.** "Intelligence, which is required for the planning and conduct of tactical operations"[9]. Intelligence used from the level of formation headquarters downwards which is produced within the formation's area or for the use of tactical units (that is, HMC Ships, Inf BGs, Air Sqns).

203. TYPES OF INTELLIGENCE

1. Within each of the levels, intelligence may be further sub-divided into one of five types of intelligence:

a. **Basic Intelligence.** Basic intelligence is the background intelligence about a subject, which is maintained in databases and continually updated in peace and in the course of operations. The principal use of basic intelligence is to set the scene at the outset of operations and to meet intelligence requirements dealing with unchanging facts such as battlespace terrain and weather, which may be raised, in answer to new requirements in the course of an operation. The definition of Basic Intelligence is: "Intelligence, on any subject, which may be used as reference material for planning and as a basis for processing subsequent information or intelligence"[10].

b. **Current Intelligence.** Intelligence that is produced in response to intelligence requirements linked to a current operation and which refers to events at the time of the operation. It is defined as: "Intelligence which reflects the current situation at either strategic or tactical level.[11]"

c. **Target Intelligence.** This is defined as: "Intelligence which portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance.[12]" Target intelligence provides the targeting data for the Targeting Process. This process ensures that the most effective use is made of offensive fire support systems.

---

[7] AAP-6 (2002)
[8] Ibid
[9] Ibid
[10] Ibid
[11] Ibid
[12] Ibid

d. **Estimative Intelligence.** Estimative intelligence is that which provides forward looking assessment and predictive judgment, and attempts to project probable future looking foreign developments and courses of action and their implications.

e. **Warning Intelligence.** Warning intelligence is that which provides warning of threats to CF or national interests in time to take effective counteraction.

204. DEFINITIONS

1. **Areas.** In order to enable the commander and his Intelligence staff to focus their intelligence effort, Areas of Intelligence Responsibility (AIR), Areas of Intelligence Interest (AII) and Areas of Interest (AI) are established in relation to the Area of Operations (AO). These areas are not only geospatial in nature but may also represent other subjects such as politics, demography or economics. The relationship between these areas is outlined at Figure 2-1.

2. **Area of Intelligence Responsibility (AIR).** This is defined as "The area allocated to a commander for which he is responsible for the provision of intelligence, within the means at his disposal"[13]. In practice, the size of this area will be limited by the capabilities, of which range will be a principal element, of the collection assets at the commander's immediate disposal. Since range is typically the principal limitation it will be within this area that the commander will direct the main effort of the intelligence staff.

3. **Area of Intelligence Interest (AII).** This is defined as "The area concerning which a commander requires intelligence on those factors and developments likely to affect the outcome of his current and future operations"[14]. The commander will require intelligence from the area outside his AIR if it is likely to influence the plan for his current operation or if it could affect future operations that he may undertake. As he is unlikely to be able to acquire this intelligence through his own collection systems, the Intelligence staff will request it from higher or flanking formations. Information and intelligence which is acquired outside the AIR should be disseminated to those other formations or units to whom it may be of interest. The AII should not be seen only in geospatial terms. It may also involve economics, politics and religion to name but a few other factors.

4. **Area of Interest (AI).** This is defined as "The area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of the current or planned operations. This area also includes areas occupied by enemy forces that could jeopardise the accomplishment of the mission"[15].

[13] Ibid
[14] Ibid
[15] Ibid

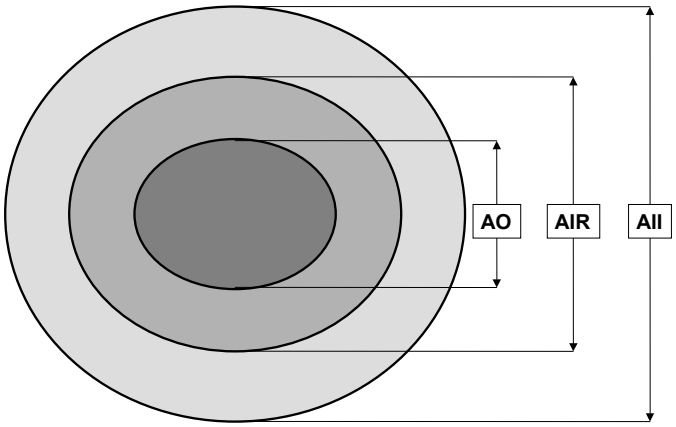

Figure 2-1 The Relationship between AO, AIR and AII

205. THE PRINCIPLES OF INTELLIGENCE

1. There are eight principles that govern the production of intelligence and the organization and activities of those who produce it. They are:

a. **Centralized Control.** Intelligence must be centrally controlled to avoid unwarranted duplication of work, provide mutual support and ensure the efficient, economic use of all resources.

b. **Timeliness.** Intelligence is useless if it arrives at its destination too late. By the same token, the system through which sources and agencies are tasked must be capable of reflecting, without delay, any significant changes in the operational situation.

c. **Systematic Exploitation.** Sources and agencies must be systematically exploited by methodical tasking, based on a thorough knowledge of their capabilities and limitations.

d. **Objectivity.** Any temptation to distort information to fit preconceived ideas must be resisted.

e. **Accessibility.** Relevant information and intelligence must be readily accessible to intelligence staffs and to users. Intelligence is of no value if it is not disseminated nor made accessible to those who require it.

f. **Responsiveness.** The intelligence staff must be responsive to the intelligence requirements of the commander at all times.

g. **Source Protection.** All sources of information must be adequately protected.

h. **Continuous Review.** Intelligence must be continuously reviewed and where necessary revised, taking into account all new information and comparing it with that which is already known.

206. THE INTELLIGENCE CYCLE

1. In order to deal with all the information which is available, identify that which is relevant, seek for that which is not present, and then process the right information into intelligence before distributing it, a structured systematic series of activities has been adopted. The Intelligence Cycle is the framework within which four discrete operations are conducted culminating in the distribution of the finished intelligence product. Each phase of the cycle must be synchronized with the commander's decision-making and operational requirements in order that it may successfully influence the outcome of the operation. The

Intelligence Cycle provides a process for understanding and ordering the many activities involved in the production of intelligence and is useful as an aid to understanding the interrelationships that exist between the various phases. The intelligence process may not continue through the complete cycle and there are no firm boundaries delineating the points at which each stage of the Cycle starts and stops. The stages or steps in the Cycle are:

a. Direction.

b. Collection.

c. Processing.

d. Dissemination.

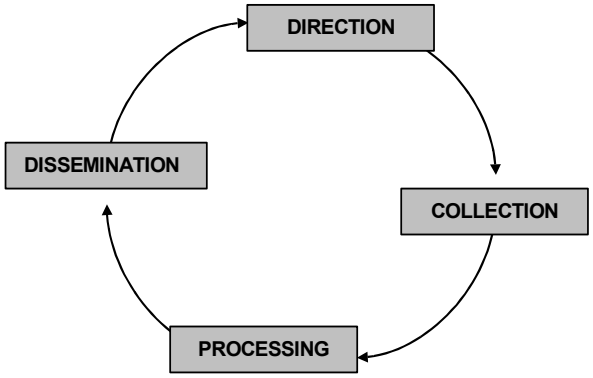

Figure 2-2 The Intelligence Cycle

207. DIRECTION

1. **Definition.** Direction is the first stage in the intelligence cycle and consists of "Determination of intelligence requirements, planning the collection effort, issuance of orders and requests to collection agencies and maintenance of a continuous check on the productivity of such agencies"[16].

2. There are two aspects to Direction:

a. **That given by the Commander to his Intelligence staff.** The commander must direct his intelligence staff. He must give clear instructions concerning the information and intelligence he needs and where necessary, set a time limit on its provision. His direction should always be as specific as possible and wherever possible, he should place his information and intelligence requirements in an order of priority.

b. **That given by the Intelligence Staff to their Sources, Agencies and Personnel.** This forms the basis of the Collection Plan and involves:

(1) The development of information requirements and the tasking of organic and attached sources and agencies.

(2) The development and forwarding of requests for information to sources and agencies that are not organic or attached.

[16] Ibid

3. **The Commander's Critical Information Requirements (CCIR).** At the outset of an operation, possibly even prior to deployment, the commander will begin to formulate questions to which he will require answers in order to conduct the operation successfully. These questions are the CCIR and concern the operational status and capabilities of friendly forces, the operational status, capabilities and intentions of the adversary and details of the battlespace environment.

4. **The Commander's Priority Intelligence Requirements (PIR).** Many of the questions contained in the CCIR will simply demand facts and can be answered by the collection and dissemination of information. There will, however, be some questions concerning the adversary and the environment that are critical to the planning and successful execution of friendly courses of action which cannot be answered by simple facts and which will require information to be processed into intelligence in order to provide answers. PIR are only those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision-making.

5. **Information Requirements.** PIR are broken into individual information requirements the responses to which, when processed and fused together, answer PIR. Information requirements are defined as "Those items of information regarding the enemy and his environment that need to be collected and processed in order to meet the intelligence requirements of the commander"[17].

6. **Indicators.** In order to task collection assets, the intelligence staff has to identify the indicators which address particular information requirements. Indicators, which are defined as " Items of information which reflect the intention or capability of a potential adversary to adopt or reject a course of action"[18], are grouped under three headings:

a. **Alert or Warning Indicators.** These relate to preparations for aggression carried out by an adversary , some of which will give early warning of the fact that hostilities are imminent.

b. **Tactical or Combat Indicators.** These indicators reveal the type of operation that the belligerent is on the point of conducting. Each type of operation across the spectrum of operations will require specific and characteristic preparations. The indicators linked to these preparations can be defined well in advance of operations and linked to specific types of operations.

c. **Identification Indicators.** Identification indicators and signature equipment are those that enable the identity and role of a formation, unit or installation to be determined from the recognition of its organization, equipment or tactics.

7. The selection of indicators that are appropriate to the operational situation will depend to a very great extent on the abilities of the Intelligence staff. The nature of the indicators that they select will drive the choice of sources and agencies that will be tasked to collect the information and intelligence they require.

8. **The Collection Coordination and Intelligence Requirements Management (CCIRM) Concept.** Once the CCIR and PIR have begun to be identified, the process of planning how to collect the information and intelligence to answer them can also begin. The methodology, which has been developed to make the Collection Plan and to manage its conduct in the most effective manner, is CCIRM. CCIRM includes information management in the broadest sense since the CCIRM function should also include the management of production and dissemination of intelligence product to users, verification of customer satisfaction, etc. Intelligence is all about managing information and satisfying the consumer's (Commander's) demands for knowledge. This is an end-to-end process from finding out (or anticipating) what the Commander needs to know to ensuring that he has received the answer that he needs – and every stage in between.

9. CCIRM encompasses those activities that result in the effective and efficient employment of intelligence collection, processing, exploitation and reporting to satisfy tactical, operational, strategic and national Intelligence Requirements. CCIRM consists of two major components: the co-ordination of the

[17] Ibid
[18] Ibid

collection effort and the management of the intelligence requirements arising from particular operations, missions or deployments. An effective intelligence architecture will allow for rapid and efficient tasking and re-tasking of sources and agencies. The making of an effective Collection Plan in accordance with the principles of Intelligence is the key to the answering of the CCIR and PIR.

208. COLLECTION

1. **Introduction.** Collection is the second stage in the intelligence cycle. It is "the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence"[19]. It is the process in which information and intelligence are collected in order to meet the commander's information and intelligence requirements that were identified in the Direction stage of the intelligence cycle.

2. There are three parts to the collection process:

   a. The exploitation of sources by collection agencies and of sources and agencies by the Intelligence staff.

   b. The timely delivery of the information collected by sources and agencies to the next step in the intelligence cycle where it will be processed into intelligence.

   c. The maintenance of a check to ensure that the right information is actually being collected.

3. **The Exploitation Of Sources And Agencies.** The essential difference between a source and an agency is that a source produces raw data and information, and an agency, in addition to having a collection capability, also possesses some degree of processing power and therefore produces intelligence. Sources and agencies[20] are defined as:

   a. **A Source.** a person from whom, or thing from which, information can be obtained[21].

   b. **An Agency.** An organization or individual engaged in collecting and/or processing information[22].

4. Sources and agencies can be grouped under three headings:

   a. **Controlled.** These are those sources and agencies, which can be tasked by an intelligence officer in conjunction with the Commander's staff to provide answers to his questions. These would include, for example, Land and Airborne ISR systems, and crews of ships, ground vehicles and aircraft

   b. **Uncontrolled.** Those sources and agencies which provide information but which are not under the control of a CF Commander and cannot be tasked directly. Newspapers, radio and television broadcasts, technical journals, navigational instructions, and maps and charts produced by hostile or neutral governments are but a few examples of uncontrolled sources and agencies. Also within this category would fall strategic surveillance systems operated by friendly nations. While the output from these might be made available, their programming would be under the control of their owners and other nations would have no say in their use.

   c. **Casual.** a casual source produces information from an unexpected quarter. An example of such a source might be a defector or a refugee. Information from a casual source should always be treated with extra caution as the ability to 'plant' information through a casual source can form part of a deception plan.

5. The Intelligence staff must know the detailed capabilities of all the sources and agencies that are likely to be available to them. This will enable them to select the appropriate source or agency for a

[19] Ibid
[20] For additional detail on Sources and Agencies see Section IV.
[21] AAP-6 (2002)
[22] Ibid

particular collection task and to maintain a check on the reliability and productivity of the sources and agencies that they are using.

6. In selecting a source or agency for a particular task, there are a number of factors which must be taken into consideration:

a. **Security.** In accordance with the Principles of Intelligence, sources and agencies must be adequately protected. Failure to do so will result either in the loss of the source or agency or its compromise and possible use to feed deception information into the intelligence system.

b. **Capability.** The source selected for the collection of a particular item of information must be capable of carrying out the task. For example, humans are tasked to collect HUMINT, cameras and electro-optic devices to collect IMINT. The agency tasked to collect an item of information or produce specific intelligence must be competent. They must have the appropriate sensor system or processing capability, must be capable of producing the information or intelligence in an appropriate format and must have a track record of having carried out similar tasks successfully in the past.

c. **Suitability.** There will be occasions when more than one type of source or agency may be capable of carrying out a collection task and available to do so. In deciding which source or agency to choose, careful consideration must be given to the attributes of each of the systems to ensure that the one most appropriate to the task is chosen.

d. **Risk.** From time to time there will be an element of physical, political or military risk involved in the use of a particular source or agency for a task. In such circumstances the risk involved must be weighed carefully against the value of the information sought. If the risk is considerable, then the decision may have to be referred to a more senior or appropriate authority for a decision.

e. **Battlespace Environment.** Various components of the battlespace environment, such as weather, terrain, or political constraint, may limit the ability of a source or agency to collect information. Such considerations must be taken into account when planning the tasking of sources and agencies. Depending on how critical to success the collection of a particular item of information may be, alternative sources may be tasked on a contingency basis to account for changes in the environment.

f. **Multiplicity and Balance.** Multiplicity is the tasking of more than one source to collect the same information. It gives a greater assurance that the information will be collected, is a valuable aid towards verification of the information and helps to guard against deception. However, it may be an extravagant use of scarce resources and will normally only be used when it is essential that the information is collected or verified. Balance is achieved by achieving an even distribution of the collection workload across the whole range of sources and agencies that are available.

7. **Delivery of Information.** Information and intelligence decays rapidly, its value decreasing with the passage of time. In order to reduce the rate of decay, timings within the intelligence cycle must be as short as possible. It is, therefore, an essential requirement of a source or agency is that it should be able to deliver the information or intelligence which it has collected in as short a time as possible within a time frame specified by the tasking organization. In this context there are two definitions:

a. **Response Time.** Defined as “The lapsed time between the initiation of a request for information and the receipt of that information”. The response time of a collection system will depend to a large extent on the type of source or agency that is employed. The time taken to deploy a source or agency to collect the required information in the required location must be taken into account. Clearly, those sources that are already in the right place will have a shorter response time than those which must be deployed to the area of interest whether it be HUMINT, aerial reconnaissance, or satellite systems.

b. **Reporting Time.** This is defined as “The lapsed time between a sensor detecting an item of information and its reception by an analyst”. The value of the majority of information and certainly of

all that collected for use at the tactical level decreases rapidly with the passage of time. The Latest Time Information is of Value (LTIOV) must be reflected in the Collection Plan. The most desirable state of affairs is that information should reach the analyst in near real-time. This however depends on there being a direct data link between the sensor and the analyst, a state of affairs that seldom exists except in the more sophisticated systems. Reporting time for various sources and agencies can vary widely and must be taken into consideration when choosing a source or agency for tasking. Some of the factors, which affect the reporting time of sources and agencies, are:

(1) The requirement to recover the sensor to the operating base of its carrier system, as in a photo reconnaissance pod.

(2) The requirement for the information to undergo some form of processing to make it intelligible such as the development of the film from a camera.

(3) The availability of communications systems and whether they have sufficient bandwidth capacity for data transmission.

8. **The Nature of the Collection Plan.** The Collection Plan must be seen as a continuous process in that it will task sources and agencies, and react, by re-tasking or by tasking different sources and agencies, to changes in the information and intelligence requirements. These will emerge as the operation progresses and in some cases, will result from the information and intelligence derived from the original tasking.[23]

209. PROCESSING

1. **Introduction.** Processing is that part of the intelligence cycle where the information which has been collected in response to the direction of the commander is converted into intelligence. Processing is a structured series of actions which, although set out sequentially, may also take place concurrently. It is defined, in a definition, which sets out the component parts of processing, as "the production of intelligence through collation, evaluation, analysis, integration and interpretation of information and/or other intelligence."[24].

2. Processing is carried out at a number of points in the information and intelligence chain. It may range from the initial processing carried out within a collection agency which usually involves nothing more than changing raw data into an intelligible form, to the processing carried out at the strategic level of intelligence which has been passed up the chain of command. Each new processing relates the information or intelligence to facts which were not available at the previous level of processing thus enabling new intelligence to be determined.

3. **Collation.** Collation is defined as "a step in the processing phase of the intelligence cycle in which the grouping together of related items of information or intelligence provides a record of events and facilitates further processing"[25]. In practice, it is made up of the procedures for receiving, grouping and recording all reports arriving in an intelligence office, at any level and it involves:

a. The basic task of allocating an identifying number to and registering the receipt of each incoming piece of information and intelligence.

b. The placing of each piece of information or intelligence into an appropriate category or group through logging, marking on a map or chart, filing or card indexing or through the entry into an electronic database of each piece of information or intelligence, as appropriate.

c. The maintenance of a system for conducting these operations, which is designed so that any member of the Intelligence staff can operate it rapidly and efficiently.

[23] The format for a collection plan is shown in Chapter 3 Annex B.
[24] AAP-6 (NATO)
[25] Ibid

4. At the basic levels of command, collation may involve no more than the maintenance of a log and a marked map or chart. However, as the sophistication of the headquarters increases, the collation system may become increasingly more automated involving Information Technology (IT) systems, visual displays, Closed Circuit Television (CCTV) briefing systems, electronic databases and high speed, automatic data transmission. As a basic principle, graphical displays of information and intelligence should be employed wherever possible as an aid to the Intelligence staff in acquiring the maximum amount of information in the shortest possible time.

5. The categories or groups into which information and intelligence will be placed by the collation system must be related to the formation's Area of Intelligence Responsibility (AIR) and to the type of operations which are to be conducted. They must also be based on:

a. The commander's intelligence requirements.

b. The intelligence requirements of the Intelligence and Operations staffs.

c. The volume of information and intelligence that is expected to pass through the system.

6. **Factors Affecting Collation.** The following factors should be taken into consideration when establishing and operating a collation system:

a. **Standardisation.** Whenever possible, the subject headings and sub headings of the groupings into which information and intelligence is placed in individual collation systems in a formation should conform to a standard set out by the Intelligence staff at the formation headquarters. The use by all Intelligence staff of similar subject headings for the categorizing of information and intelligence and of a standard structure for intelligence databases will simplify and speed processing where time is valuable and will facilitate the exchange of information and intelligence across the formation.

b. **Common Subject Headings and Sub-Headings.** The selection of headings and sub-headings for groupings is to be based on the IR associated with the particular type of operation being undertaken and the battlespace environment within which it is to be conducted. Sensible selection of headings and sub-headings will make the categorisation of information and intelligence relatively straightforward and rapid.

c. **The Importance of Cross Referencing.** All entries in the system should be cross-referenced to the original report and to entries in the filing system and in the log. Where electronic databases are in use, the relational nature of such databases will carry out much of this work automatically.

d **Visual Presentation.** The visual impact of maps, graphs, diagrams and VDU based presentations should be exploited as an aid to the rapid assimilation of large amounts of information and intelligence.

e. **Urgency and Speed of Reaction.** The system must have the capacity to react rapidly to short notice requests for the rapid handling of information and intelligence required to meet the commander's information and intelligence requirements.

f. **Restrictions on the Volume of Records.** The capacity of the system to deal with a particular volume of records in terms of both throughput and storage will be dictated by:

(1) The numbers of Intelligence staff available to operate the system.

(2) The nature and tempo of operations.

(3) The capacity of the recording equipment.

(4) The capacity of the storage and retrieval system.

(5) The space available in the intelligence office or cell.

(6) The size and scope of the intelligence task.

g. **Pragmatism.** There will always be a temptation to attempt to process every piece of information and intelligence coming into the intelligence cell. To do so will almost inevitably lead to systems and procedures becoming overloaded and slowing down. In the worst case, the process will come to a halt and no intelligence will be produced. In order to avoid this, there is a need to strike a compromise between what is desirable and what is possible. This can only be achieved by adopting a pragmatic approach to the collation process, constantly pruning the system, weeding the records and carefully filtering the input so that only information relevant to current intelligence requirements is collated and sent forward to the next stage of processing.

h. **Prioritization.** The collators must always be aware of the priorities placed on various intelligence requirements so that incoming information related to them is prioritised and treated with the appropriate degree of urgency.

7. **Evaluation.** Evaluation is defined as "a step in the processing stage of the intelligence cycle constituting appraisal of an item of information in respect of the reliability of the source and the credibility of the information"[26]. To be more succinct, it is an assessment of how reliable the source is and how likely the information that comes from it is to be true. Incoming information cannot be taken at face value. There are many reasons, not the least being that of deception, why information may not be reliable or entirely accurate. The Evaluation step of Processing allocates an alphanumeric rating to each piece of information or intelligence indicating the degree of confidence which may be placed upon it.

8. The allocation of this rating is based partly on subjective judgement on the part of the evaluator, partly on experience of other information produced by the same source and, in the case of information produced by a sensor, on knowledge of the accuracy of the particular sensor system. The reliability of the source and the credibility of the information, the two factors in the overall assessment of the information must be considered independently of each other. This is to ensure that the rating allocated to the reliability of the source does not influence that given to the credibility of the information, or vice versa. Every piece of information produced by an impeccable source is not necessarily correct; neither does a piece of information that is demonstrably true necessarily indicate that its source is totally reliable.

9. The accepted standardised values for allocating ratings for reliability of the source and credibility of the information are[27]:

Reliability of the Source		**Credibility of the Information**	
A	Completely Reliable	1	Confirmed by other sources
B	Usually Reliable	2	Probably True
C	Fairly reliable	3	Possibly True
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged.

Table 2-1 Reliability Ratings

10. The ratings are produced by combining the values. Thus, a piece of information judged to be "Probably True" from a source known to be "Usually reliable" would be rated B2. On the other hand, a piece

[26] Ibid
[27] NATO, Allied Joint Intelligence, Counter-Intelligence and Security Doctrine (AJP 2.0)

of information of which the “Truth cannot be judged” produced by the same “Usually reliable” source would be rated B6. The advantages of using this method of assessment are that:

a. It provides a universally understood shorthand assessment of information.

b. Over a period of time, it gives an indication of the capabilities of various sources and agencies and aids the selection of those best suited for particular tasks.

11. **Analysis and Integration.** Analysis and Integration are defined separately and respectively as ”a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation”[28] and “a step in the processing phase of the intelligence cycle whereby analysed information or intelligence is selected and combined into a pattern in the course of the production of further intelligence“[29]. In practice, the two processes are treated as one since integration follows on from analysis without a break.

12. In analysis, the collated and evaluated information is scanned for significant facts. These are then related to other facts that are already known and deductions are made from the comparison. Integration is the drawing together of the deductions and the identification from them of a pattern of intelligence; a sequence of events or a picture of an individual. This aspect of processing is almost totally cerebral and is the critical point in the intelligence cycle where there is, as yet, no substitute for the experience and judgement of the analyst.

13. Because of this, there are no rules or guidelines that can be set out to govern or assist the analyst in his task. However, in common with many other routines involving the use of personal judgement, the analyst’s skills will improve with practice.

14. **Interpretation.** Interpretation is defined as “The final step in the processing phase of the intelligence cycle in which the significance of information or intelligence is judged in relation to the current body of knowledge”[30]. It is the final stage in processing where information which has been collated, evaluated, analysed and integrated must finally be interpreted to complete the process of the conversion of information into intelligence.

15. **The Mental Process.** Interpretation is an objective mental process of comparison and deduction based on common sense, life experience, military knowledge covering both adversary and friendly forces and existing information and intelligence. In it, new information is compared with, or added to, that which is already known giving rise to fresh intelligence. This mental process can be broken down into a sequence of three principal questions which must be asked about the piece of information which is being considered:

a. **Identification.** Who is it? What is it? This is not merely matching an identity to a unit, or a name to a piece of equipment; it is the consideration of all the implications of the presence of that unit or piece of equipment at that particular point in time and space.

b. **Activity.** What is it doing? The significance of the activity that is being carried out must always be compared with information about previous activity to discover whether there is any change in the pattern of activity.

c. **Significance.** What do the answers to the first two questions mean? What is their significance? Do they have any relevance to the combat indicators, which have been established?

16. **Wringing the Facts Dry.** In answering the last question, the analyst must be sure that the piece of information has been wrung dry of all its possible deductions. One way of achieving this is, whenever a deduction has been reached, to ask oneself the question “So What?” and when that question has been answered, to ask again “So What?”. Only when no further answer can be found has the fact been wrung dry of its deductions.

[28] AAP-6 (2002)
[29] Ibid
[30] Ibid

17. **Deception.** The Intelligence staff is a prime target for deception. The analyst must, therefore, be suspicious by nature, must not jump to conclusions and must seek confirmation of even the most credible of information from the most reliable of sources. History has shown that deception pays dividends to the deceiver and is a powerful and effective component of Information Operations (IO).

18. **Confirmation.** At the end of the mental process, the deductions and conclusions flowing from it will be fitted into the intelligence picture. However, in almost every case, the resultant intelligence will not be conclusive and there will be a requirement for further information to be acquired either to confirm or to refute it. The need to meet these new requirements dictates the cyclical character of the Intelligence Cycle and the repetitive nature of the Collection Plan.

19. **Summary.** The systematic treatment of information and intelligence carried out in Collation, Evaluation, Analysis, Integration and Interpretation is a combination of bringing order to the receipt and recording of information, and of applying logic and method to the mental process of converting information into intelligence. The mental process itself relies on a wide knowledge of the adversary's tactics, equipment and organization, a depth of tactical experience on the part of the analyst and the possession and the application of large doses of common sense coupled with the ability to make reasoned deductions.

20. It is the reasoning skill of the human and his ability to 'play a hunch' or to conduct predictive analysis based on incomplete information which is critical to the successful operation of the analytical process at the heart of Processing. These skills are acquired rather than taught and are the product of practice and experience over a period of time. They are the key to the predictive nature of intelligence.

210. DISSEMINATION

1. **Introduction.** Dissemination is defined as "The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it"[31]. The key components of the definition are:

a. **Timeliness.** There are two aspects to timeliness. The first is that intelligence which reaches its intended destination too late for the purpose for which it was intended is worthless. The second is that the majority of intelligence, certainly at the operational and tactical levels, is time sensitive, that is to say that it decays or loses its value with the passage of time. Both aspects drive the requirement to get intelligence to its intended user as quickly as possible. When processing has to be truncated in order to meet deadlines, the resultant intelligence must be annotated so that the user may treat it with an appropriate degree of discretion.

b. **Appropriateness.** There is no point in disseminating intelligence which does not answer the requirements of the user, cannot be understood by him or which is being disseminated using a transmission system to which he does not have access. Intelligence must be in a format relevant to the needs of the recipient. It must meet his requirements, it must be in the correct language, and it must be disseminated by a system common to both sender and recipient. If it fails to meet any one of these parameters, it will, in common with belated intelligence, be worthless. CCIRM is as vital in the dissemination stage as it is in the collection phase.

2. **The Principles of Dissemination.** Dissemination is governed by a set of principles. These are as follows:

a. **Clarity.** A clear differentiation must always be made between facts and the interpretation of them. In all written material, any interpretation should be preceded by the word "Comment". In oral briefing, the difference between fact and interpretation should be underlined by the use of a phrase such as "The conclusion to be drawn from this is...." or "We believe this means that....".

b. **Conciseness.** Commanders do not have the time to listen to verbose oral briefings or to wade through lengthy written reports. Reports must be as brief as possible and yet must include

[31] Ibid

everything the recipient needs to know. The effectiveness of visual presentations in imparting information quickly should always be borne in mind.

c. **Standardisation.** Reports can be understood more quickly and easily if they are written in a logical sequence that follows a standard format. NATO's *Bi-SC Reporting Directive Volume 2 (Intelligence Reports)* contains the standard format for each of the key intelligence reports. Standard report formats should be in Unit Standing Operating Procedures (SOP). More detail on standard intelligence reports is provided in Chapter 3.

d. **Evaluation.** An evaluation of each piece of information included in an intelligence report, rather than of the whole report, should be made. The evaluation should be in the alphanumeric form set out in table above.

e. **Urgency.** Whenever possible, information should be converted into intelligence and disseminated because the interpretation of the facts is more valuable than the facts themselves. However, when time is at a premium, processing of urgent information may not be possible. In these circumstances, the information should be disseminated as quickly as possible with the caveat that it has not been processed and may not be reliable. This particularly applies to current information and intelligence at the tactical level.

f. **Distribution.** Intelligence staffs are responsible for ensuring that all information and intelligence is passed to those who need it, including flanking or neighbouring formations.

g. **Regularity.** Urgent information and intelligence collected to meet intelligence requirements will be disseminated whenever it becomes available. The Commander and his Intelligence staff will require, in addition, summaries of all intelligence that affects their operations. These reports will be listed in unit SOPs.

h. **Security.** Do not over-classify intelligence! Over-classification causes delays in handling and transmission. As a general rule, information concerning the adversary need not be encrypted if the adversary would not have sufficient time to act upon it if he intercepted the transmission carrying that information. On the other hand, the greatest care must be taken not to reveal the source of information and there will be occasions where the risk of compromising the source will have to be weighed against the value of the information in making the decision on whether to use it or not. On such occasions, the Intelligence staff will have to make recommendations on the impact of possible compromise in order to assist the commander in making a decision.

3. **Dissemination Formats**. There are four formats in which information and intelligence can be disseminated:

a. Verbally.

b. In Writing.

c. Graphically.

d. As Electronic Data.

4. Intelligence must be provided in a form that is readily understood and directly usable by the recipient in a timely manner without overloading the user and minimizing the load on communications capabilities. Dissemination consists of both "push" and "pull" control principles. The "push" concept allows the higher echelons to push information down to satisfy existing lower echelon requirements or to relay other relevant intelligence to the lower level. The "pull" concept involves direct electronic access to databases, intelligence files, or other repositories by intelligence organizations at all levels. Web-based technologies/standards are now commonly used to organize and present related intelligence products together facilitating "one-stop shopping". This includes operational support pages, which link related intelligence products and operational information together on a single web page. Intelligence sharing and dissemination is further enhanced by

modern communications systems equipped with an electronic publishing capability. Electronic publishing allows organizations to publish their own documents or contribute (collaborative publishing) to the creation of other documents throughout the electronic publishing community.

5. **Principles of Verbal Dissemination.** The verbal briefing is the original method of passing on information and intelligence. It must be governed by the following principles:

a. **Clarity.** The briefer must ensure that he has marshalled his thoughts before he starts his briefing. The briefing should follow a standard format. If necessary, the briefer should use written notes to ensure that his briefing follows this format. The use of visual aids, maps, drawings and diagrams will enhance the briefing and clarify the information, which is being briefed.

b. **Relevance.** The briefer must ensure that the information and intelligence that he is passing on is relevant to the level of operations in which his audience is involved and is current, that is to say it is not out of date or has already been briefed.

c. **Brevity.** To be brief and succinct is the key to the successful dissemination of verbal information and intelligence. The good briefer is the one who imparts the most information in the fewest words.

6. **Types of Verbal Briefing.** Verbal briefings can be either:

a. **Impromptu.** Where the commander requires to be brought up to date as quickly as possible by the Intelligence staff. This would probably take place on a one-to-one basis, would be informal in nature and would not require a structured format. It would contain only those intelligence highlights needed to bring the commander up to date from his last briefing.

b. **Formal.** This is the briefing of a more formally constituted group such as the commander and his staff or a group of formation or unit commanders. Such a briefing requires an element of time for its proper preparation and should be given using a standard format.

7. **The Pros and Cons of Verbal Briefing.** The advantages of verbal briefing are that it is quick, facts are put across succinctly and the briefer can be questioned easily. The disadvantages are that it is dependant on the personality of the briefer for its success and the audience almost always has to leave its place of duty and come to the briefer with the consequent disruption that this involves.

8. **Principles of Written Dissemination.** The principles which apply to Verbal Dissemination; Clarity, Relevance and Brevity, are equally applicable to the process of Written Dissemination.

9. **Communications.** Effective and redundant communications are essential to support all operational aspects of the Intelligence Cycle. To ensure adequate communications are available, Intelligence Staff must advise and coordinate with CIS planners as to anticipated requirements for communication support. Such coordination should include definition of the intelligence architecture focusing on the systems required, connection points, the bandwidth required and the need for security. In designing the intelligence architecture and considering which systems to use the following factors should be taken into consideration.

a. **Speed.** In dissemination of intelligence, speed is of the essence. Therefore, wherever possible, an electronic communication system should be used to pass intelligence in near real time.

b. **Encryption.** Electronic encryption is instantaneous and has no effect on the time taken to disseminate the intelligence. Manual encryption is time consuming and it must be remembered that the process of decryption at the recipient's end of the communication system will take as long, if not longer than the encryption. If there is no alternative to manual encryption and the intelligence is urgent, then the risk of compromise must be weighed against the requirement to get the intelligence to the user in time.

c. **Bandwidth.** The bandwidth of the system will determine the rate at which the intelligence can be sent over the system. The narrower the bandwidth, the slower the transmission rate. This consideration will affect the exchange of large quantities of data between databases rather than the

dissemination of relatively small amounts of intelligence. If, however, the dissemination involves graphics such as maps, photographs or sketches, then bandwidth may again become a consideration as the transmission of all three of these categories of material is demanding of bandwidth. Intelligence products must be tailored to the available bandwidth. Care must be taken that intelligence products are prepared in such a fashion that they can be transmitted quickly given available bandwidth. In some cases this may mean that complex graphics and other features are reduced or eliminated. The key principle must be the timely delivery of the right information – nothing extraneous.

d. **Language.** If the intelligence is to be disseminated in a language different from that of the recipient, a situation that may quite often be the case in combined or coalition operations, consideration may have to be given to dissemination by a Liaison Officer (LO) fluent in the recipient's language. This method of dissemination although slow, will prevent the possibility of the intelligence being misunderstood.

211. INTELLIGENCE SOURCES AND AGENCIES

1. Information, which is processed into intelligence, is collected from a variety of "sources" and "agencies". It is important to have an understanding of the difference between the two terms:

a. **A Source.** This is: "In intelligence usage, a person from whom, or thing from which, information can be obtained."[32].

b. A source possesses information either acquired randomly as in the manner of an overheard conversation in a café or to meet a specific request as in a camera recording images along the programmed flight path of an unmanned aerial vehicle (UAV). The source is the primary origin of the information and either possesses the information itself or by its activity demonstrates that the information exists. a collector is a person or system that obtains the information from the source. The only change to the information that the source may effect is to its format. This may be, for example, a translation from one language to another by a human contact or the conversion of a picture from a visual image to a radio signal by a satellite. a source has no capacity to process information.

c. **An Agency.** This term is defined as: "In intelligence usage, an organization or individual engaged in collecting and/or processing information." (AAP-6). An agency may be capable of collecting and processing information or may simply have the capability to collect information and must pass that information to another agency for processing. At one end of the spectrum of agencies is the reconnaissance section reporting adversary activity at a crossroads and at the other, a large government department receiving information from a wide variety of sources and applying very large amounts of processing power to it in order to produce intelligence. A single-source agency is one that produces intelligence that is largely based on a single source such as imagery.

2. **Collection Disciplines by Source Type.** Intelligence sources are the means or systems used to observe, sense, and record or convey information of conditions, situations and events. The primary source types, also referred to as collection disciplines, are:

a. **ACINT.** Acoustic Intelligence. "Intelligence derived from the collection and processing of acoustic phenomena.[33]" This is intelligence derived from sound. Examples of ACINT sources are hydrophones, geophones, SONAR, IUSS[34] and artillery sound ranging systems. Because of the nature of the origin of sound, ACINT is primarily concerned with movement and the intelligence that can be derived from its detection. ACINT in the CF is predominantly maritime in nature, and involves the detection, tracking and possibly identification of submarine contacts by active and passive sonar of various types, including those that feed into the IUSS.

[32] Ibid
[33] Ibid
[34] Integrated Underwater Surveillance System

b. **HUMINT.** Human Intelligence. "A category of intelligence derived from information collected and provided by human sources.[35]" The range of HUMINT sources is enormous. Every person, friendly, adversary or neutral is a potential source of HUMINT. HUMINT collectors are those personnel trained in the acquisition of information from human sources in response to intelligence requirements. HUMINT collectors include specially trained interrogation and HUMINT collection personnel. Collectors may also be intelligence officers, Counter-Intelligence (CI) agents or Special Operations Forces (SOF) personnel when they are using human collection techniques in the course of their duties. HUMINT is of particular value in the confirmation or augmentation of IMINT and SIGINT.

c. **IMINT.** Imagery Intelligence. "Intelligence derived from imagery acquired by photographic, radar, electro-optical, infra-red, thermal and multi-spectral sensors, which can be ground based, sea borne or carried by overhead platforms.[36]" The adage that 'a picture is worth a thousand words' is especially true in intelligence. The information conveyed by an image is clear, concise and in the main unequivocal and will often serve to support or confirm intelligence derived from other sources. The bulk of IMINT is derived from sources such as satellites, aircraft and UAVs.

d. **MASINT.** Measurement and Signature Intelligence. "Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, spatial, wavelength, time dependence, modulation, plasma and hydro magnetic) derived from specific technical sensors for the purpose of identifying specific features associated with the source, emitter or sender and to facilitate subsequent identification and/or measurement of the sender and to facilitate subsequent identification and/or measurement of the same.[37]" MASINT is derived from the collection and comparison of a wide range of emissions with a database of known scientific and technical data in order to identify the equipment or source of the emissions. Such is the nature of MASINT that its collection is likely to be directed at the strategic level.

e. **OSINT.** Open Source Intelligence. This is intelligence based on information collected from sources open to the public, such as the media; radio, television and newspapers, state propaganda, learned journals and technical papers, the Internet, technical manuals and books, to name but a few. Contrary to popular belief, there is considerable archival evidence to confirm that the intelligence community has always used open sources in the production of intelligence. Freedom of Information legislation around the world has unlocked all but the most valuable of nations' secrets and the ability to reach remote information provided by systems such as the Internet has provided rapidly growing and easily accessible sources of intelligence. OSINT is most likely to be the source of basic intelligence although, with the capabilities of modern news gathering equipment, there will be occasions when 'on the spot' television reporting will be used to produce current intelligence.[38]

f. **RADINT.** Radar Intelligence. This is intelligence derived from the use of radar as a detection device. For example, the identifying of an object, which may or may not be recognisable, at a specific bearing and range from the radar, or the simple detection of movement at a certain point on the ground. This is distinct from the exploitation of radar data under IMINT.

g. **SIGINT.** Signals Intelligence. The generic term used to describe all intelligence derived from the Electro-Magnetic Spectrum (EMS). It is divided into:

(1) **COMINT.** Communications Intelligence. "Intelligence derived from electro-magnetic communications and communications systems by those who are not the intended recipients of the information"[39]. This is intelligence obtained from information gained through the interception of communications and data links. Such information may be collected in verbal form by the reception of broadcast radio messages, by the interception of point-to-point

[35] AAP-6 (2002)
[36] Ibid
[37] US DoD
[38] For additional information on OSINT refer to the NATO Open Source Intelligence Handbook
[39] AAP-6 (2002)

communications such as telephones and radio relay links, or as data through the interception of either broadcast or point-to-point data down links.

(2) **ELINT.** Electronic Intelligence. "Intelligence derived from electro-magnetic non-communication transmissions by those who are not the intended recipients of the information"(AAP-6). This is intelligence that is derived from the technical assessment of electro-magnetic non-communications emissions such as those produced by radars and by missile guidance systems. It also covers lasers and infrared devices and any other equipment that produces emissions in the EMS. By comparing information about the parameters of the emission that has been intercepted with equipment signatures held in databases, valuable intelligence about the equipment and its operator can be derived.

3. **Intelligence Functional Disciplines – Subject Areas.**[40] The functional disciplines of intelligence cover subject-focused aspects of intelligence production and often require specialist analytical expertise. They contribute to general intelligence production but may also generate functionally focused product for specific purposes and in response to specific intelligence requirements of customers. These disciplines are not mutually exclusive; aspects of one discipline may also be considered as part of another discipline. The overlap between some of these categories simply reflects the convenience of grouping related subjects that may be the subject of separate study or require specialist intelligence expertise.

4. They include but are not limited to:

a. **Armed Forces Intelligence.** This is intelligence concerning all aspects of foreign space, land, sea and air forces including order of battle (ORBAT), command and control (C2), weapons systems, training, personnel, doctrine, strategy and tactics, logistics, arms trade, defence industry and defence spending.

b. **Biographic Intelligence.** This is intelligence on the views, traits, habits, skills, importance, relationships, health and curriculum vitae of those foreign personnel of actual or potential interest to Defence and the CF.

c. **Economic Intelligence.** This is intelligence concerning foreign economic resources, activities and policies, including the production, distribution and consumption of goods and services, labour, finance, and other aspects of the international economic system such as aid, trade and investment. In the defence intelligence context, it addresses the economic potential to support and develop defence capabilities.

d. **Political Intelligence.** This is intelligence concerning the dynamics of the internal and external political affairs of foreign countries, regional groupings, multilateral treaty arrangements and organizations, and foreign political movements directed against or impacting on established governments and authorities. This includes government structures and domestic and foreign policies.

e. **Targeting Intelligence.** Targeting intelligence is that which portrays and locates the components of a target or target complex and indicates its identification, vulnerabilities and relative importance.

f. **Scientific and Technical Intelligence (STI).** STI is intelligence concerning foreign developments in basic and applied scientific and technical research and development including engineering and production techniques, new technology, and weapons systems and their capabilities.

g. **Technical Intelligence (TECHINT).** "Intelligence concerning foreign technological developments and the performance and operational capabilities of foreign materiel, which have or may eventually have a practical application for military purposes"[41]. This is intelligence derived from the scientific examination and testing of materiel including computer hardware and operating system software. Testing is centred primarily on determining the capabilities and limitations of adversary equipment

[40] Australian Defence Force, ADFP 19 - Intelligence
[41] AAP-6 (2002)

and in support of the development of countermeasures to that equipment. TECHINT is a subset of STI.

h. **Logistics Intelligence.** This is intelligence concerning the ability to move forces, and support and sustain military operations.

i. **Infrastructure Intelligence.** This is intelligence concerning rail, road, pipeline, water and air transportation networks and telecommunications systems and utilities.

j. **Geospatial Intelligence.** Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth.

k. **Sociological Intelligence.** This is intelligence concerning social and cultural factors including population parameters, ethnicity, social stratification and stability, public opinion, education, religion, health, history, language, values, perceptions and behaviour.

l. **Health Intelligence.** This is intelligence concerning health support facilities and capabilities, the impact of disease and environmental hazards on military forces, and other health-related information of interest to the intelligence community and its customers.

m. **Medical Intelligence.** Medical intelligence is a subset of health intelligence and addresses similar issues but is produced specifically for medical and health professionals to aid in developing medical countermeasures and plans for deployments. It contains terminology that must be interpreted by medical and health specialists.

n. **Security Intelligence (SI).** SI is defined as intelligence on the identity, capabilities and intentions of organizations or individuals who pose, or may pose, a threat in peace, emergency or conflict, to the security of the resources, activities, operations, personnel and information of DND and the CF. It includes intelligence on the identity, capabilities and intentions of foreign intelligence systems, criminal/organized crime and organizations or individuals that may be engaged in espionage, sabotage, subversion, violence or terrorism against DND and the CF. It is especially related to CI activity.

CHAPTER 3

INTELLIGENCE PRACTICE

301. INTRODUCTION

1. The chapter addresses the scope and nature of intelligence activities and the way in which they are put into practice. The three key aspects or components of intelligence activity are:

   a. **Intelligence Staff Functions.** Intelligence staff functions encompass the intelligence staff process that provides input to decision-making processes, intelligence planning, liaison, requirements and collection management, and the management of intelligence assets and operations.

   b. **Production Functions.** Production function involves the output of intelligence products.

   c. **Conduct of Intelligence Operations.** This encompasses those operations conducted by intelligence personnel for information or counter-intelligence (CI) purposes.

302. JOINT INTELLIGENCE STAFF STRUCTURES

1. **Essentials.** An efficient joint intelligence staff structure is based on:

   a. Interoperability and mutual support between all elements of the joint intelligence architecture.

   b. Close liaison between the joint intelligence staff, other branches of the joint headquarter, and intelligence agencies and units.

   c. Adequate and secure communications and information systems.

2. **Staff Elements.** The organization of the intelligence staff will be determined by the organization of the headquarters (HQ) it supports and the resources available, but will usually include the following elements:

   a. A senior intelligence officer, who is one of the principal staff officers in the headquarters.

   b. An element that produces intelligence staff work, including estimates and plans.

   c. A requirements and collection management cell.

   d. A processing and production element (which may be referred to as an all-source cell).

   e. A CI element.

   f. Support groups, as required, from specialist collection agencies.

3. **Staff Coordination.** Intelligence staffs are an integral part of the operations process and, together with operations and plans staff, have a significant input in the planning and conduct of operations. Close coordination and cooperation between all branches of a joint headquarters is imperative. For instance, many of the sources and agencies on which intelligence staff rely for information and intelligence can only be tasked by other elements within a headquarters. The requirement for intelligence staff to work in an area of restricted access must be balanced against the need for contact with other elements of the headquarters staff. Coordination is achieved through:

   a. An integrated information system available to all who need access.

   b. Co-locating intelligence, plans and operations staff.

   c. Personnel contact within the joint HQ.

d. Conferences, briefings and planning groups.

e. Carefully compiled distribution lists.

303. LIAISON

1. **Requirement for Liaison**. Intelligence staff may be required to liaise with other HQ, coalition partners, police, local authorities, civilian intelligence organizations, and other government or non-government groups. Effective liaison requires: the allocation of liaison effort to those organizations that can best facilitate the achievement of the commander's mission; sound professional knowledge of intelligence responsibilities, capabilities, operations and procedures; thorough situational understanding and knowledge of intelligence requirements; and effective communications.

304. JOINT INTELLIGENCE ARCHITECTURE AND PLANNING

1. A Joint Intelligence Architecture is the connectivity, which is put in place to connect collectors, producers and users of intelligence in an information network.[42] A Joint Intelligence Architecture facilitates the management of intelligence, enables ISR including the conduct of the CCIRM process, and optimizes intelligence functions at all levels of a force, component or formation. It enables the timely flow of critical information and intelligence vertically and horizontally both within and external to the force or formation.

305. PRINCIPLES

1. The establishment and management of an intelligence architecture is based on the following principles:

a. **Primacy.**

(1) The operational commander must drive the intelligence effort.

(2) The Intelligence staff is responsible for the establishment of the intelligence architecture in consultation with the Operations staff and manages all intelligence activity within the architecture.

(3) There will be a single Intelligence point of contact at each level of command within the architecture for CCIRM, Processing and Dissemination.

b. **Flexibility.**

(1) Intelligence architectures should be established and practised in peace and should be so designed as to be capable of seamless transition to operations.

(2) Intelligence architectures must be dynamic and flexible, capable of rapid re-configuration to meet the changing demand for information and intelligence throughout the conduct of operations.

(3) Intelligence architectures must be designed to support the planning and conduct of operations at all levels of command.

c. **Interoperability**

(1) Intelligence systems and communications throughout the architecture must interoperate in a seamless manner using collaborative tools..

[42] CFCS (TITAN/SPARTAN) is the means by which intelligence information is processed and disseminated and made available to CF users; it is also the means by which CF intelligence is provided to our allies and to the Government of Canada and by which we receive Allied intelligence.

(2) Intelligence products must be in a form, content and language usable by all components of the intelligence architecture.

d. **Security.**

(1) Intelligence must be disseminated at the lowest possible level of security classification. Procedures for the sanitization of intelligence are required and the responsibility for the provision of the sanitization mechanism lies with the provider of the information or intelligence that is required to be sanitised.

(2) Coalition and Allied partners must be considered in the dissemination process subject to bi-lateral agreements and/or review by appropriately appointed personnel.

(3) The intelligence architecture must be capable of handling information and intelligence at all levels of classification. If this is not possible, then commanders may be denied access to the best intelligence.

e. **Accessibility.**

(1) The ability of components of a joint force to gain access to intelligence databases is the key to successful intelligence operations. Intelligence architectures must provide the ability for users to access databases as appropriate.

(2) The responsibility for the maintenance of intelligence databases included in the architecture including read, write and access authority must be clearly defined.

f. **Common Standards/Interoperability.** Common standards must exist within the architecture in order to allow information and intelligence to be exchanged through the architecture to enable interoperability. These standards will include:

(1) A common data standard to enable IT systems to exchange information and intelligence throughout the architecture.

(2) Common encryption systems.

(3) Common procedures for the conduct of the intelligence process to ensure coherent intelligence products.

(4) The use of common formats and terminology to prevent misunderstanding and to avoid ambiguity.

306. COMMUNICATIONS CAPABILITY

1. The communications links, which make up the bearer systems of intelligence architecture are the key to the successful operation of the Architecture and also enable the effective operation of the ISR system. They must have:

a. Sufficient bandwidth to carry large volumes of data.

b. Redundancy to protect the architecture against systems failure or adversary action.

c. The ability to be reconfigured rapidly in order to maintain the flexibility of the architecture.

d. The ability to work together, either directly, or through interfaces in order to provide a real time communications capability.

e. Appropriate security to protect the information and intelligence that they will carry.

2. It is imperative that the Intelligence Staff clearly define the intelligence architecture (see below) and coordinate communications with CIS planners to ensure that the CIS community is fully aware of intelligence requirements for communications links and systems.

307. PLANNING THE ARCHITECTURE

1. The Intelligence staff are responsible for the development of the intelligence architecture to support the mission. This will be established using the principles set out above. In establishing the architecture the Intelligence staff will ensure that:

a. They know the task organization of the intelligence organization including the allocation of collection assets to the operation together with the allocation of any strategic assets such as National Intelligence Cells (NICs).

b. The nature and capabilities of the collection assets allocated for the operation and their C2 arrangements are properly understood.

c. All the potential users of intelligence products have been properly identified.

d. No source of information collection, or of intelligence production and dissemination is subject to a single point of failure.

e. The architecture can cope with both ‘pushing’ and ‘pulling’ intelligence and contains controls to enable these functions to be carried out.

f. The architecture will be able to cope with all the scenarios likely to be encountered in the course of the operation or campaign.

g. The architecture will be:

(1) **Survivable.** The technical aspects of the architecture must be as survivable as the command structure it supports. Assets that are vulnerable to damage or destruction must have alternative means of providing data.

(2) **Interoperable.** The Intelligence and J3 systems must be interoperable in order to allow the production and display of a Joint COP.

(3) **Secure.** A policy for protection of the information and intelligence in the architecture must be developed. At the same time the architecture must be designed so that the widest possible access is permitted without compromising the security of the information and intelligence.

(4) **Compatible.** Every component’s intelligence systems must be capable of receiving and exchanging data, information and intelligence products. This capability must extend to applications, databases and communications protocols.

308. INTELLIGENCE STAFF PROCESS

1. The intelligence staff process is a generic term encompassing the various activities and specific processes involved in providing intelligence staff support to the commander. It represents the practical implementation of the intelligence cycle and is an ongoing process. Even when operations are not under way or contemplated, the intelligence staff process provides for a continuous flow of intelligence to the commander in response to standing IR. When focused specifically in support of joint operations, the intelligence staff process is known as Intelligence Preparation of the Battlespace (IPB). This staff process involves several intelligence process tools, methodologies and outputs. Some of these supporting activities may be applied as intelligence processes in their own right, such as Indications and Warning (I&W), but they all contribute to the overall intelligence staff process. Detail on the intelligence staff process, as represented by IPB, and the supporting tools, processes and outputs are described in Chapter 4.

309. INFORMATION MANAGEMENT

1. Once the commander's PIR have begun to be identified, the process of planning how to collect the information and produce the intelligence to answer them can also begin. The making of an effective Collection Plan[43] in accordance with the principles of Intelligence is the key to the answering of the commander's PIR. The methodology developed to make the Collection Plan and to manage its conduct in the most effective manner is Collection Coordination and Intelligence Requirements Management (CCIRM).

2. CCIRM encompasses those activities that result in the effective and efficient employment of the planning, collection, processing and dissemination phases of the intelligence cycle to satisfy tactical, operational, strategic and national Intelligence Requirements. It is a management function that enables the timely flow of intelligence by co-ordinating the information collection effort and facilitating the provision of intelligence. CCIRM consists of two major components:

a. Coordinating the collection effort.

b. Managing the intelligence requirements, arising from particular operations, missions or deployments.

310. COLLECTION MANAGEMENT

1. CCIRM is the process of collection management. This is defined as "The process of converting intelligence requirements into collection requirements, establishing, tasking or co-ordinating with appropriate collection sources or agencies, monitoring results and retasking, as required"[44]. The outline concept is shown in Figure 3-1 below.

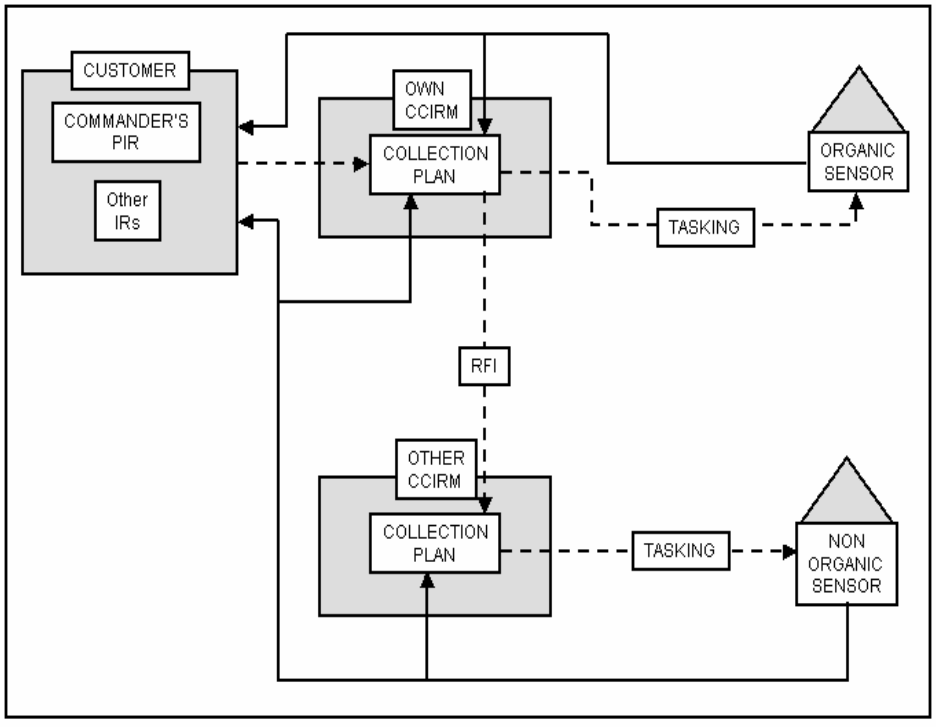

Figure 3-1 The CCIRM Process

[43] The format for a collection plan is shown at Annex B.
[44] AAP-6 (2002)

311. INTELLIGENCE REQUIREMENTS MANAGEMENT

1. Intelligence requirements management begins with the formation of the commander's PIRs, which, once identified, are initially formed into a series of questions in the form of Information Requirements (IR). The methods pursued to answer these questions form the basis of a Collection Plan and the role of CCIRM is to:

   a. Manage the Collection Plan ensuring that unnecessary duplication of tasking does not occur (although there will be occasions when duplication is planned deliberately to provide confirmatory information).

   b. Ensure that the most appropriate resources are used to obtain the necessary information. This may be the retrieval of data from one or more of the intelligence databases to which CCIRM has access and/or a fresh request for tasking of collection assets.

   c. Monitor the requirements of operations in progress and guide the allocation of necessary resources to meet those requirements.

2. IRs will normally be divided into two categories: those derived from intelligence requirements that are ongoing and require regular updates, and those, which result from more time sensitive requirements such as PIRs.

3. IRs will be forwarded by customers to their appropriate CCIRM staff with an information copy distributed to the wider CCIRM network. IRs must state:

   a. What information is needed?

   b. By whom?

   c. By what time/date?

   d. In what format?

   e. By what means (website, message, brief etc)?

4. Upon receipt at a CCIRM desk all IRs will be logged on a Collection Worksheet or in an online RFI log used for this purpose.

5. Once an IR is recorded CCIRM staffs will validate, clarify and refine it. They will also conduct a priority assessment with the staff to determine its importance relative to other operations and plans, and thus its urgency of handling; this will be based on the commander's PIRs. If an IR has to be rejected for any reason, the customer will be informed. Once this initial validation process has been carried out, the CCIRM staff will:

   a. In the first instance, arrange for a search of existing databases and publications to which they have access. This will ensure that the answer is not already extant in existing records. The CCIRM staff will then determine if they can meet the requirement by tasking their own assets, or, if not, the request will be passed through the chain of command in the format of a Request for Information (RFI) until CCIRM staffs at a higher level can satisfy it.

   b. If their own assets can meet the IR as a new collection effort, the CCIRM staffs will identify and task the source or agency that will best provide the answer.

312. COLLECTION CO-ORDINATION

1. This is the development and control of a collection plan, which sets out how the information and intelligence needed to meet the IRs is to be collected. The IRs are converted into taskings, which are the specific questions that are put to organic sources and agencies or, where no suitable organic collection

system is available, into Requests for Information (RFIs). The RFI is the format[45] in which an IR is passed to CCIRM authorities at higher, lower or adjacent levels. The Collection Plan is constantly revised and updated and Intelligence staffs must also closely monitor the productivity of sources and agencies as they fulfil the collection plan. Collection Coordination has two parts:

a. The exploitation of sources by collection agencies.

b. The delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.

2. Once a collection task has been completed the answers are sent directly to the customer. This may be either a higher, lower or adjacent formation or the organic processing unit. The only CCIRM involvement will be to consult both the producer and customer near to the LTIOV to confirm that the remit has been or will be met. If there is doubt as to whether the timescale can be achieved, the CCIRM staff will consult the customer to ascertain if a later delivery is acceptable or the task should be cancelled, releasing assets for other tasks. If a product does not arrive at the customer by the LTIOV, the appropriate CCIRM staff should be alerted.

313. CCIRM STAFF PROCEDURES

1. The CCIRM concept is underpinned by the principles of intelligence, in particular centralised control, timeliness, systematic exploitation, accessibility, responsiveness and continuous review. It encompasses both Collection Co-ordination and Intelligence Requirements Management and has as its principal objective the timely provision of the best possible intelligence.

2. CCIRM staffs at the customer headquarters carry out the following actions:

a. Create and manage the Collection Plan.

b. Convert the IRs into a series of taskings or RFIs (Taskings of organic collection assets or RFIs to other formations).

c. Provide answers to requirements where possible from within its own resources.

d. Send RFIs through the CCIRM chain, in order to acquire information that is unavailable through that headquarters' own resources.

3. CCIRM staffs at the higher levels conduct the following actions:

a. Validate and prioritise the requests.

b. Record the incoming RFIs on the Collection Worksheet and annotate their Collection Plan accordingly.

c. Answer those they can from within their own resources.

d. Place collection tasking requests to agencies and sources that fall within their level of authority. These should report directly to the customer, and not through CCIRM staffs.

314. SUMMARY

1. Central to the CCIRM methodology is the identification of a focus within existing intelligence staffs at their level of command. Each CCIRM focus acts as the interface between other CCIRM foci within the intelligence chain of command. A CCIRM manager is responsible for the day-to-day co-ordination of work and represents CCIRM on behalf of the commander. The flexibility of CCIRM must not detract from the

[45] Format for a RFI is contained in NATO STANAG 2149 – Request for Information.

underlying principle that the responsibility for intelligence reporting and the information flow must parallel the chain of command.

2. CCIRM is a tool for the harmonisation of a range of interrelated management activities whose objective is the meeting of the commander's PIR in the most efficient and effective manner. A central element of CCIRM is ensuring that the product answers the customer's requirements? CCIRM must always be customer focused and responsible for quality control of intelligence products.

315. PRODUCT TYPES

1. This section outlines some of the main product types including:

   a. Threat and risk products.

   b. Basic intelligence products.

   c. Military capabilities assessments and studies.

   d. Operations specific products.

   e. Reports and summaries.

316. THREAT AND RISK PRODUCTS

1. **Threat Products.** A threat is a person or thing likely to cause harm. A risk is the chance and nature of the harm likely to be suffered as a result of a threat. In other words, threats to the CF are created by someone or something else and generate risk that is borne (and managed) by the CF[46]. The two broad types of written threat products are the threat assessment and the estimate.

   a. **Estimates.** Estimates are produced when there is an identified adversary command that will act against the supported friendly commander. At the strategic level, the intelligence estimate may be incorporated in the military strategic estimate rather that be issued as a separate intelligence document. Chapter four describes how intelligence estimates are produced.

   b. **Assessments.** Threat assessments are produced for specific events or activities where there are multiple threat sources and it is difficult to define adversary courses of action. Examples include security threat assessments.

2. **Indications and Warning (I&W).** Estimative intelligence on potential adversary courses of action or potential scenarios, are linked to collection planning and the commander's decision cycle by warning intelligence products, such as warning reports, I&W matrixes and I&W briefings. I&W products are used to advise the development of commander's decision points; that is, the commander's preordained response options to potential circumstances that may arise or be uncovered in the I&W process. They therefore facilitate threat monitoring and assessment, and lead to timely and accurate advice for commanders and decision makers.

317. BASIC INTELLIGENCE PRODUCTS

1. **Databases.** A series of linked databases are designed to meet the base requirements of the range of potential defence operations. The databases will be "pull" retrieval systems designed to assist the estimative, warning and current intelligence applications at the strategic, operational and tactical levels of command as contingencies or situations occur. Examples of such databases include order of battle, infrastructure, technical intelligence (TECHINT), and biographical. Additional information on intelligence databases is included in Annex B.

[46] See "Risk Management for CF Operations" (B-GJ-005-502/FP-000) for additional information on Risk Management.

2. **Country Briefs.** J2/DG Int produces a range of low classification briefs on countries of operational interest to the CF. Each country brief covers the political, military, geographic and economic aspects of the country of concern.

318. MILITARY CAPABILITY ASSESSMENTS AND STUDIES

1. Military capability assessments look at the overall capability of a specific country and military capability studies focus on a specific element of that capability, for example, airborne or maritime capability. These products fulfil the basic intelligence function and the estimative intelligence function in that they provide judgments on future developments as well as basic reference material.

319. OPERATIONS SPECIFIC PRODUCTS

1. Information guides can be produced within the intelligence system to support those entering specific environments or operations. Examples of such a product include:

a. **Operations Support Packages.** This term is used for the compilation of those databases and packages developed to satisfy the forecast information and intelligence requirements for the planning and conduct of the deployment of a force on operations or future contingencies. Generally, the detail contained tends to focus on geospatial information but may include detail on a belligerent's tactics, techniques, organization, and equipment.

b. **Country Handbooks.** CF personnel deploying on operations overseas are normally issued with a country handbook produced for the deployment. The aim of the handbook is to provide background on the geographic, situational, military, economic and cultural (including language) aspects relevant to the proposed or existing AO.

c. **Weapons Recognition Guide.** A weapons recognition guide may be incorporated into the country handbook or issued as a separate product. The aim of the guide is to provide a reference to the various weapons active in a proposed or existing AO. The guide will generally provide both written characteristics such as calibre, rate of fire and ranges, as well as graphic representation of each weapon.

320. REPORTS AND SUMMARIES

1. **Intelligence Reports.** Information and Intelligence is disseminated in written form through the medium of Intelligence Reports. The Canadian Forces use the standardised NATO intelligence reports summarised in the NATO *Bi-SC Reporting Directive Volume 2 (Intelligence Reports)*. The reports fall into two categories:

a. **Common User Reports.** There are three intelligence reports that fall into this category. These are as follows:

(1) **Intelligence Report (INTREP).** The short title INTREP is always to be used in these messages, which can be originated at any level.

(a) **Description.** The INTREP is a report sent spontaneously, without regard to a specific time schedule, whenever the information or intelligence it contains is considered to require the urgent attention of the commander to whom it is addressed. The INTREP should contain any deductions that can be made from the information and intelligence in the time available. The minimum distribution of INTREPS should be laid down in SOPs at each level of command but this should not inhibit the originator of the INTREP from widening the distribution if he believes this to be necessary.

(b) **Format.** The format of an INTREP must conform to agreed NATO standards. It may either be sent as free text with a structured header and footer following the format set

out in Bi-SC Reporting Directive, Volume 2 (Intelligence Reports). In order to simplify the process, further messages which contain specific structured data referring to Naval, Land or Air matters have been developed and form the basis of the MARINTREP, LANDINTREP or AIRINTREP. The structures of these messages are also contained in Bi-SC Reporting Directive, Volume 2 (Intelligence Reports).

(2) **Intelligence Summary (INTSUM).**

(a) **Description.** The INTSUM is a concise, periodic summary of intelligence on the current adversary situation within a commander's AIR designed to update the current intelligence picture and to highlight important developments during the reporting period. It should therefore include any information that may be relevant to the intelligence requirements of any commander to whose headquarters it is disseminated and should contain an assessment of future intent based on evaluation and interpretation of that information. At the higher echelons, emphasis should be placed on appraisal and not on detail. The INTSUM is disseminated either at the discretion of the originating commander or, at the direction of a higher formation. The distribution of an INTSUM must include all those whose responsibilities and interests may be affected by the contents of the summary.

(b) **Format.** The format of the INTSUM must conform to agreed NATO standards as set out in Bi-SC Reporting Directive, Volume 2 (Intelligence Reports).

(3) **Supplementary Intelligence Report (SUPINTREP).**

(a) **Description.** This report may be produced from time to time, on special request or in preparation for a special operation. It is designed to provide detailed reviews and analyses of all the intelligence data on one or more specific subjects that have been collected over a period of time. The distribution of the SUPINTREP will be governed by its content.

(b) **Format.** There is no NATO agreed format for this report with the exception of the requirement for the word SUPINTREP to appear at the beginning of each report. Bi-SC Reporting Directive, Volume 2 (Intelligence Reports) contains a format for a free text report with a header and footer in a specific format.

b. **Specialist Reports.** There are a number of other intelligence reports and summaries which are grouped either under the heading of a particular service or of a particular specialization.

2. **Intelligence Briefings.** Intelligence is also disseminated by verbal briefings, telephone and videoconference. More detail on intelligence briefings is contained in Chapter 2.

321. INTELLIGENCE OPERATIONS

1. In addition to the intelligence staff's primary function of providing intelligence support to their commander, they are required to plan and supervise intelligence operations within their command. This goes beyond simple collection management. It includes aspects of operations and logistics planning, oversight, personnel management and supervision. The level of residual command responsibilities is negotiated at an early stage in planning intelligence-related operations and approved by the commander.

2. Intelligence Operations include those operations conducted by or which involve intelligence personnel for information or counter-intelligence (CI) purposes. Examples include:

a. **HUMINT Activities.** The type of HUMINT activities conducted in-theatre depends upon the mission and could include all or some of the following:

(1) **Conventional Directed Activity (CDA).** This includes the normal activities that soldiers carry out in the performance of their duties, such as patrolling.

(2) **Tactical Questioning.** The first questioning and screening to which a Prisoner of War (PW)/detainee is subjected. Tactical Questioning usually takes place at the HQ of the unit that captures the PW/detainee. There is a need to question recently captured PW/detainees to obtain intelligence of immediate tactical value. As interrogators will generally constitute a very small pool of expertise within a theatre of operations, the limited tactical questioning of PW/detainees by other than Intelligence Branch specialists might be necessary depending on the situation. Only designated, trained personnel within a unit will conduct Tactical Questioning. Under the Laws of Armed Conflict (LOAC) and International Humanitarian Law (IHL) questioning PW/detainees to collect information also requires that providing such information be voluntary.[47]

(3) **Military Intelligence Reconnaissance.** Intelligence personnel will periodically conduct overt reconnaissance and surveillance of a target area, person, structure or organization.

(4) **Contact Handling.** It is the process of running human sources by trained HUMINT personnel. It involves structured inter-personal contact between trained HUMINT operators and individuals with access to information of potential intelligence interest.

(5) **Tactical CI.** Tactical CI is the process of providing force protection services to tactical commanders by the conduct of CI Source operations, support to HUMINT operations, counter-surveillance, tactical CI investigations, vulnerability assessments, screening operations, and CI liaison.

(6) **Enhanced Reconnaissance.** This involves remote and close reconnaissance and surveillance of specific targets by air, land, sea, foot and vehicle by personnel who have received specialized surveillance training.

(7) **Interrogation.** The systematic questioning of a PW by a trained interrogator for intelligence gathering purposes. It will only be conducted during an armed conflict in which Canada is a participant. Only qualified interrogators from the CF Intelligence Branch are authorized to conduct interrogation. Interrogation will be based on the use of kinesic interviewing and questioning techniques only. No physical or mental torture or threat thereof, nor any other form or threat of physical coercion will be employed in interrogating a PW at any time.[48]

(8) **Covert Passive Surveillance (CPS).** This is conducted by highly trained personnel and involves detailed surveillance of a target for extended periods of time. It describes the covert systematic observation of a person, place or object in order to gain information from a concealed location or by foot or vehicle.

(9) **Agent Handling.** This describes the process of running someone covertly, and who is formally accredited, recruited and controlled by HUMINT personnel.

b. **Counter-Intelligence Operations.** These are operations conducted by specialist CI personnel to collect security intelligence and counter the threats from espionage, subversion, sabotage or terrorism. While often focused on the human element, CI operations are by definition multidisciplinary and can utilise any form of collection under the security intelligence umbrella.

[47] Refer to B-GG-005-027/AF-021 "The Law of Armed Conflict at the Operational and Tactical Level" and B-GJ-005-110/FP-020 "Prisoner of War Handling, Detainees, Interrogation and Tactical Questioning" for additional information.

[48] B-GG-005-027/AF-021 "The Law of Armed Conflict at the Operational and Tactical Level" Chapter 10 Paragraphs 22 and 23 clearly state that "It is forbidden to apply any form of coercion to PWs…". Such coercion may amount to a war crime and both the individuals committing such crimes and the commanders who direct or condone such acts may be prosecuted under both Canadian and international law.

c. **Exploitation of Personnel, Documents and Equipment.** The exploitation of personnel, documents and equipment naturally falls across the domains of HUMINT and scientific disciplines such as MASINT. Intelligence agencies, units and staffs involved in the exploitation of personnel, documents and equipment may be required at various levels with the CF. Planning for exploitation should be flexible to allow the organization of the exploitation system to be tailored to meet particular operational requirements. Detailed procedures for the exploitation of personnel, documents and equipment are described in the following publications:

(1) Prisoner of War Handling, Detainees, Interrogation and Tactical Questioning (B-GJ-005-110/FP-020); and

(2) Handling of Captured Personnel, Equipment and Documents (NATO AJP 2.5)

ANNEX A - INTELLIGENCE DATABASES

3A01. INTELLIGENCE DATABASES

1. Intelligence is stored in two formats:

   a. **Structured.** Structured intelligence data is stored in a database in which each record has a defined structure consisting of a series of fields. Details of the field description, the field length, that is to say the number of characters for which there is space in the field, and the type of characters; alphabetical, numeric or a mixture of the two are set out in the Data Dictionary for the database. Intelligence is retrieved from the database through the use of a web browser designed specifically for use within the structure of a specified database.

   b. **Unstructured.** Unstructured data is stored in a data repository, and in the case of intelligence data, usually in the form of text. Intelligence is retrieved from the repository through the use of a search engine similar to that used in a web browser.

2. There are advantages and disadvantages connected with the two data formats. These can be summarised as follows:

   a. **Structured Data.**

      (1) Can be manipulated that is, modelled.

      (2) Can be counted.

      (3) Can be displayed graphically.

      (4) Is resource intensive to maintain.

      (5) Loses intelligence nuances when structured data is converted from the original textual data.

      (6) Structured data can easily be exchanged with other structured databases using the same data standards.

      (7) Searches for specific information and intelligence are easily conducted.

   b. **Unstructured Data.**

      (1) Cannot be manipulated, modelled or displayed graphically.

      (2) Cannot be counted.

      (3) Difficult to exchange.

      (4) Limited maintenance overheads.

      (5) Retains all nuances of original message.

      (6) Searches for specific information or intelligence may be complicated to set up.

3. In choosing the format in which to store data, the Intelligence staff will take into account the use for which the stored data is intended and choose the storage medium with the most appropriate characteristics. Modern computer and web technologies, specifications, standards and languages such as meta tags and XML (Extensible Markup Language) greatly facilitate the sharing and exchange of both structured and unstructured intelligence data.

4. **Relational Databases**. Intelligence databases are almost exclusively relational databases in which intelligence is stored in the form of relationships between entities. Relationships may represent, for example, the number of a certain type of aircraft at an airfield – a relationship between an equipment and a place or the presence of a particular officer at a named regiment – a relationship between a person and a unit.

3A02. DATABASE STANDARDS

1. In order to exchange data between two structured databases there has to be a common exchange format. In effect this means that the structure of the sending and receiving databases have to be the same. Fields within the structure have to have the same title and the data standards for the fields, the field length and character type also have to be the same. Finally, the value tables for both databases, the codes that are entered into the fields and which represent specific details also have to be common to both databases.

2. When these conditions have been fulfilled and where a communications link between both structured databases exists, data can be passed or 'exchanged' from one database to the other. In NATO, the standard for intelligence data exchange is set out in AIntP-3 Edition 2. Although this is the exchange format, it has become the *de facto* standard for structured intelligence databases.

3A03. DATABASE MANAGEMENT

1. The Intelligence staff are responsible for:

   a. Establishing an architecture that allows access to all databases containing information and intelligence relevant to the operation or campaign.

   b. Allocating read/write permissions for databases to appropriate Intelligence personnel.

   c. Establishing a policy for the maintenance of the database through reviewing information and intelligence stored in the database.

   d. Allocating security classifications to data to be stored in a database.

   e. Arranging for downloads from the database to other databases as appropriate.

   f. Arranging for downloads from other databases to the database as appropriate

   g. Using the Defence Subject Classification and Disposition System (DSCDS) to organize databases and other information holdings so that the holdings are stored, retrieved, used and disposed of in a systematic and efficient manner.[49]

[49] Within DND/CF, the DSCDS has been sanctioned by the National Archives of Canada (NA) as a disposition authority - thereby enabling its users to dispose of information legally, under the terms and conditions of the National Archives of Canada Act.

ANNEX B - FORMAT FOR A COLLECTION PLAN[50]

(CLASSIFICATION)

DTG:_____

MISSION:_____

PIR NO.	PIR	IR NO.	IR	NAI TAI DP/ DL	I[1] NO.	INDICATOR	PRIORITY	NET[2]	LTIOV[3]	STATUS	SOURCES		AND		AGENCIES	COORDINATION	REPORTS
A	Will bde-sized or larger adversary force attack across the COLORADO	A-1	Adversary engineer recce along COLORADO River.		A-1-1	Engineer recce at LAMAR bridge (UB3467).		110930Z	120400Z		X						
					A-1-2	Engineer recce in vicinity of MONTOPOLIS.		110930Z	120400Z				X				
B	Adversary's main effort NORTH?	B-1	Passage of at least two bdes through NAI 1.	NAI 1	B-1-1	Div recce bn on Highway 183.			120300Z					X	X		

[1] Indicator.
[2] Not Earlier Than.
[3] Latest Time Information Is of Value.

(CLASSIFICATION)

[50] NATO, Intelligence Procedures (AJP 2.1)

This Page Intentionally Blank

CHAPTER 4

INTELLIGENCE SUPPORT TO PLANNING

401. INTRODUCTION

1. The Intelligence Preparation of the Battlespace process provides a focus for the wider and ongoing intelligence effort identified in the intelligence cycle in chapter 2 and is fundamental to intelligence staff practice outlined in chapter 3. While this chapter concentrates on the intelligence staff process supporting the CF Operational Planning Process (CF OPP), the IPB process is equally applicable to the intelligence support provided to strategic level planning processes.

402. INTELLIGENCE STAFF RESPONSIBILITIES

1. In meeting the requirement for the provision of accurate, timely and relevant intelligence to meet the commander's intelligence requirements, the J2 will carry out the following tasks:

a. Develop an intelligence architecture for the passage of information both within the force and to higher, subordinate and adjacent commands.

b. Develop a policy for the operation of the intelligence process within the force consistent with CF and, as applicable, coalition or NATO intelligence practices and procedures.

c. Working together with the Operations and Commander's staff, identify the commander's PIRs.

d. Through the medium of the CCIRM process, develop and implement a Collection Plan.

e. Develop a plan for sharing national intelligence throughout NATO or coalition force having regard to the constraints imposed by national security procedures.

f. Carry out IPB in support of the commander's decision-making process.

g. Contribute to the Command and Control Warfare (C2W) effort through intelligence support to Operational Security (OPSEC), Deception, Psychological Operations (PSYOPS), Electronic Warfare (EW) and Physical Destruction.

2. The fundamental responsibility of the Intelligence staff is to provide decision-makers at all levels of command with the fullest possible understanding of their adversary and of the operational environment. This understanding will include a comprehensive understanding of the adversary's desired end state, interim objectives, strategy, tactics, strengths and vulnerabilities, doctrine and order of battle and his capabilities and intentions. The staff must strive to understand every facet of the adversary's character, culture, social and ethnic background, traditions and history. If possible they must also have some degree of command of his language.

3. The intelligence staff must have the ability to provide for the commander an understanding of how the adversary will view a situation, the courses of action that will be open to him and how he will react to our actions. This is a fundamental part of the relationship that should be developed between the Intelligence staff, the commander and other staff branches within the headquarters.

403. THE CF OPERATIONAL PLANNING PROCESS (CF OPP)

1. The CF Operational Planning Process (CF OPP) is a coordinated process to determine the best method of accomplishing assigned operational tasks or of planning for possible future tasks. Planning may be inhibited by inadequate information, insufficient time and limited resources. The planning process is designed to optimize logical, analytical steps of decision making in conditions of uncertainty and ambiguity. The process is applicable to any type of operation in both the Deliberate and Time-Sensitive Planning

environments. The CF OPP is described in more detail in “CF Operational Planning Process” (B-GJ-005-500/FP-000).

2. **Objectives**. The objectives of the planning process are to:

a. Standardize the planning process within the CF,

b. Ensure strategic/political control is effected during the development of the plan,

c. Enable the staff to translate strategic political objectives provided by the Government of Canada into strategic/ operational-level military objectives,

d. Enable commanders to guide development of the planning process, and

e. Maximize the staff’s creative thinking and associated thought processes.

3. **Output**. The output of the planning process is a CONPLAN, Op Plan or Op O, designed to produce a desired end-state and to achieve an assigned mission.

4. **Design.** The planning process is applicable to all CF operations. It consists of five steps, leading from the initiation of planning through to plan review and, if necessary, a repetition of the process. The five steps are:

a. Initiation;

b. Orientation;

c. Course of Action (COA) Development;

d. Plan Development; and

e. Plan Review.

5. The product of the intelligence contribution to the CF OPP is expressed in three ways. First, intelligence assists the commander and the staff in the decision making process. Second, the intelligence annex to the Op O provides direction to guide intelligence effort to meet the commander’s priorities. The format for an intelligence annex is provided at Annex B. Lastly, the documented intelligence estimate or assessment allows all cooperating commands (higher, lower and adjacent) to share and compare their assessments of the situation. Details of specific intelligence tasks to support CF OPP are described in Chapter 5 of NATO’s AJP 2.1 – Intelligence Procedures.

404. INTELLIGENCE PREPARATION OF THE BATTLESPACE (IPB)

1. The purpose of IPB is to support the commander’s decision-making process by providing him with the basis for achieving situational awareness. It also helps the staff answer his requirements and assists in focusing reconnaissance and surveillance assets on critical activities.

2. IPB is designed to present information and intelligence graphically, and is more readily supported by information technology than a written estimate. The basic elements used in IPB are the same as those of the Intelligence Estimate, and it is essentially only the means by which those elements are developed and displayed that are different. The main advantages of IPB over the Intelligence Estimate include:

a. Ease and speed in updating and presenting a large quantity of information and intelligence.

b. Ease of assimilating information and making amendments to the intelligence picture due to changes in variable factors, as they occur, by making simple changes to overlays or computer graphics.

c. Ease of co-ordinating large quantities of unprioritized information contained in intelligence databases.

d. Ease of identifying essential areas of intelligence interest and vital decision points.

3. Although the procedures described here were originally aimed at ground forces in a conventional battlespace, the principles involved can also be adapted for use by the other environments. They can be applied to any operational environment including jungles, mountainous terrain, deserts, urban areas, the littoral, etc.; and to operational specialities such as fire support, air defence, anti-submarine warfare and electronic warfare. The IPB process is also well suited to Non-Article 5 Crisis Response Operations (NA5 CRO), including Peace Support Operations. Furthermore, the techniques used in the IPB process can be applied equally well to the analysis of operations by friendly forces including mobility factors, battlespace environment and vulnerabilities to actions by threat forces.

405. USE OF IPB

1. The principles of IPB can be applied in all theatres, by land, maritime and air forces, and in all types of operations[51]. The extent to which it can be used will vary according to local circumstances. Precise procedures can be adapted to meet the factors relevant to a given situation, to the service and the arm of the service concerned, local staff resources and to the level of technological support available.

406. THE IPB CONCEPT

1. IPB is a systematic, cyclical and dynamic process, which is closely connected to the individual stages of the commander's decision-making process. The results of the IPB process are represented graphically on a series of overlays. The overlays include basic data on terrain, weather and the threat's tactical doctrine, all of which can be prepared well in advance. Just before and during combat, current data will be added which, when integrated, graphically show:

a. Possible threat options.

b. Places where intelligence collection assets must be used in order to monitor or detect threat actions.

c. Places where own forces can influence the course of events by using manoeuvre and strike assets.

d. Decision points at which the commander must act to influence threat operations.

407. IPB AND THE INTELLIGENCE CYCLE

1. IPB meshes closely with and is dependent on intelligence produced through the Intelligence Cycle. During the IPB process new intelligence requirements will be identified. These requirements will then be translated into questions, and appropriate sources and agencies will be tasked with the collection of information in response to them. This information will then be processed, thereby producing intelligence. This new intelligence is used in the various steps of the IPB process in the planning phase and in combat.

408. IPB PROCESS

1. The IPB process consists of four distinct steps[52]:

a. **Step 1 - Define the battlespace environment**. This step identifies the geographical limits of the unit's/formation's area of operations (AO), battlespace, and area of interest (AI). In addition, it identifies the general physical characteristics of the battlespace that will influence both friendly and

[51] Note that this manual does not address domestic operations. Specific guidance regarding the employment of intelligence resources of the CF in domestic operations has been promulgated in the NDHQ Instruction DCDS Directive 2/98.
[52] The IPB process and the associated products are described in detail in Land Force Intelligence Field Manual (B-GL-357-001/FP-001).

adversary operations. Included in these characteristics are population demographics together with existing political or socio-economic factors.

b. **Step 2 - Describe the battlespace effects**. When describing the battlespace effects, the intelligence staff should visually and orally describe to the Commander and the staff how both weather and terrain will affect the their mission.

c. **Step 3 - Evaluate the adversary**. This step occurs when the intelligence staff determines the capabilities of adversary forces. It focuses on the specific adversary forces expected to be operating in the unit's/formation's AO and AI. The intelligence staff will evaluate the adversary doctrinal principles, tactics, techniques and standing operating procedures. To adequately evaluate the adversary the intelligence staff must analyze the battle from the perspective of the adversary commander, that is, the battle through the adversary's eye. During Step Three, for each prospective COA, the intelligence staff will produce these products:

(1) A situation template based on doctrinal templates;

(2) Description of tactics and options; and

(3) Initial High Value Targets List (HVTL).

d. **Step 4 - Determine adversary courses of action**. This is where all of the IPB process comes together. The products produced in this Step are, (1) Event Templates, (2) Event Matrix, (3) draft ISR Plan and (4) Updated HVTL. Steps One through Three must be completed prior to initiating Step Four. When determining the adversary's COAs, the intelligence staff attempts to graphically portray likely adversary actions. They will identify a minimum of three adversary COAs based on the Situation Templates - most likely, next likely and most dangerous. They will attempt to identify as many adversary courses of action, as time will allow. During step four of the IPB process the intelligence staff will also assist in developing the High Payoff Target List (HPTL).

409. APPLICATION

1. Besides enabling a commander to determine his intelligence requirements through clarity of presentation and logic, IPB also provides the basis for wargaming, which is used to develop the detailed plan, by comparing the COAs determined by the commander or his operations staff with the most likely threat COAs identified through the IPB process. The Decision Support Overlay refined through wargaming can assist the commander and his staff in managing the plan.

2. The products of the IPB process can support and be enhanced by the development of overlays showing for example, the assessed indirect fire support capability of the threat, possible dispositions of the threat's air defence, estimates of the threat's surveillance capabilities, assessments of the threat's EW capability and offensive NBC capability.

410. IPB AND THE TARGETING PROCESS

1. The targeting process closely parallels IPB. Initial targeting data is developed and refined through the various stages of the IPB process. Additional information requirements arise from the targeting process and are integrated into the Collection Plan.

2. The results of IPB and wargaming support the identification, selection and location in time and space of High-Payoff Targets, which may be integrated into the Decision Support Overlay as Target Areas of Interest (TAIs). IPB also identifies the Decision Points (DPs) or Decision Lines (DLs) at which the commander must decide to use organic and allocated strike assets against a particular TAI. The need for accurate and timely Battle Damage Assessment generates additional intelligence requirements.

411. INFORMATION OPERATIONS (IO)

1. **Definitions.**

   a. **Information Operations (IO)**. Information Operations are defined as actions taken in support of political and military objectives, which influence decision makers by affecting other's information while exploiting (fully utilizing) and protecting one's own information[53]. There are two categories of IO including Defensive IO and Offensive IO, depending upon the nature of the actions involved.

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

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

2. A more detailed explanation of the terms is set out later in this section but in general:

   a. Offensive IO will generally have two principal objectives:

      (1) To attack the adversary commander's perception of the situation, undermining his will and weakening his resolve, painting the inevitability of defeat while offering plausible alternative options for action; essentially persuading the adversary commander to think what you want him to think and making him choose what you want him to do.

      (2) The disruption of the adversary commander's ability to exercise command; paralysing him and preventing him from taking the initiative.

   b. Defensive IO has as its principal objectives the protection of the cohesion of the force and the maintenance of the integrity of the friendly force's command and information systems.

3. **The Information Environment.** IO are conducted in the information environment, which is a continuum of individuals, organizations and of systems that collect, process or disseminate information as well as the information itself. The Information environment is one of the components of the Battlespace. It includes the World Wide Web, C2 systems of friendly and adversary forces, all personnel, friendly or adversary, who make decisions and handle information, the climate, terrain and weather that affect the information environment and weapons effects. All military operations are conducted within the information environment, much of which is beyond immediate military control and in order to conduct successful operations, the commander must consider the conduct of IO within that part of the information environment which is within his control in his decision making process.

4. **Defensive IO.** Defensive IO are aimed at protecting friendly information and CIS systems against attacks by another party. They include the capability to:

   a. Assess the vulnerability of friendly information, information based processes, C2 systems and CIS to manipulation or disruption by an adversary or potential adversary and to natural or accidental actions.

   b. Protect friendly information, information based processes, C2 systems and CIS against an adversary's IO attack through protective mechanisms, software or procedures.

[53] CF Information Operations (B-GG-005-004/AF-010)

c. Assess the ability of an adversary to conduct offensive IO to attack, intrude or manipulate friendly information and information-based processes.

d. Identify the existence and perpetrator of an IO attack.

e. Restore friendly information and information-based processes that have been damaged or corrupted as a result of hostile, natural or accidental actions.

5. **Offensive IO.** Offensive IO attacks other parties' information and information systems and includes:

a. The ability to assess the vulnerabilities of others' information, information based processes, C2 systems and CIS to influence by friendly IO resources.

b. The ability to co-ordinate and apply all available IO resources to exploit others' IO vulnerabilities.

c. Mechanisms to ensure that offensive IO actions are applied only to the extent necessary to achieve friendly political and military aims.

412. INTELLIGENCE SUPPORT TO IO

1. Intelligence support is critical to the planning, execution, and assessment of IO. The joint staff intelligence (J2) representative(s) assigned to support IO should be the liaison for intelligence support for all IO planning. Intelligence must be readily accessible, timely, accurate and sufficiently detailed to support an array of DND IO requirements, to include research, development, acquisition and operational support. The conduct of sophisticated IO requires unique and detailed intelligence never before asked of intelligence collection agencies and activities. Intelligence Preparation of the Battlespace (IPB) is vital to successful IO. Intelligence products must support IO planning, provide analysis of a potential adversary's IO vulnerabilities, allow determination of a potential adversary's IO capabilities and intentions, provide Indications & Warning (I&W) of any potential threat and contribute directly to the Precautionary Measures System.

2. Guidance for specific intelligence support required for offensive and defensive IO is provided in CF Information Operations (B-GG-005-004/AF-010) Chapters II, "Offensive Information Operations," and III, "Defensive Information Operations," respectively.

413. INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE

1. **Intelligence Surveillance & Reconnaissance (ISR).**[54] Integrated ISR is the capability that combines command direction, surveillance and reconnaissance sensors, and processed Information & Intelligence (I2) to provide a timely fused multi-source I2 picture to the Common Operational Picture. As such, ISR directly focuses on supporting current military operations. ISR is more than the sum of Intelligence + Surveillance + Reconnaissance. The synergy created by integrating the tasking and control of these traditional military tasks with focused dissemination of the fused product resulting from these activities creates an entirely new level of capability.

2. Key terms associated with ISR include:

a. **Reconnaissance.** A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

b. **Situational Awareness.** The complete understanding of what is happening, and what will happen in a defined Area of Interest. Commanders at all levels require Situational Awareness as one of the key elements of effective Command and Control. Situational Awareness is created in the mind of the Commanders by merging the appropriate Common Operational Picture with additional data and knowledge affecting the employment of the forces under their command.

[54] Integrated Intelligence, Surveillance & Reconnaissance (ISR) Capability Planning Guidance

c. **Surveillance.** The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. Surveillance implies a continuous observation over a continuous or extended period of time.

d. **TPED.** Tasking/Processing/Exploitation/Dissemination. This acronym summarizes the four principal steps in the ISR process from the tasking of ISR assets (sensors and intelligence sources), through the processing of the data received to generate information, and the exploitation of that information to answer a commander's information requirements, to the dissemination of the processed information to those who need it in the form that they need and within the time that they specify.

e. **Common Operational Picture(COP).** The Common Operational Picture is the integrated graphically based representation of the location and activities of all forces on land, sea, air, and in space in a defined Area of Interest. The COP will depict the location of friendly, hostile and neutral units, assets, and reference points. It will also depict topographical, meteorological, oceanographic, and Nuclear Biological and Chemical (NBC) information.

3. **Principles.** The principles of ISR are based on the Principles of Intelligence and are:

a. **Centralized Co-ordination.** ISR has strategic importance and is employed by a multitude of users; therefore, it must be coordinated centrally without sacrificing the principle of decentralized execution implicit in mission command. This ensures the most effective and efficient use of resources. The net-centric focus of the future emphasizes that intelligence can be obtained by a variety of platforms and means, which may not be directly controlled by a central agency. In order to maximize this potential, every effort must be taken to access and incorporate data from all sources into a centralized fusion process.

b. **Timeliness.** Information and intelligence must be provided to the commander in a timely fashion to allow him to work within the adversary's decision-action cycle.

c. **Accuracy.** The ISR product must be accurate and relevant to the operation it is supporting.

d. **Passage of Information.** Within an ISR system it must be possible to pass relevant information between appropriate commanders and staffs without overloading them with irrelevant data.

e. **Economy of Effort.** The ISR system provides improved situational awareness, allowing the Commander to achieve economy of effort in his manoeuvre and firepower assets.

4. **Desirable Capabilities of an ISR System.** The ISR system should, as far as possible possess the following capabilities:

a. **Responsiveness.** The system must be able to react quickly to the commander's information and intelligence requirements and to rapidly exploit targeting information.

b. **Continuous Coverage.** Surveillance and reconnaissance must be able to provide 24-hour coverage in all weather conditions.

c. **Robustness.** ISR assets must provide a robust mix of overlapping systems in terms of technology, range and performance in order to cope with adversary action as well as changing meteorological and light conditions and to defeat adversary deception plans.

d. **Flexibility.** ISR assets should be modular so that the right mix of assets can be tailored for a force, according to the needs of the mission.

414. ISR CONCEPT OF OPERATIONS

1. The basis of the ISR Concept of Operations is that there are three main functional areas in the ISR system: the Fusion Centre[55], the Sensors, and the Sensor Management Cell. These last two may be collocated or separate.

2. **The Fusion Centre.** The key to the ISR concept of operations is the ISR Fusion Centre. Its role is to:

a. Conduct the CCIRM and Tasking function.

b. Fuse and collate information.

c. Analyse information.

d. Pass intelligence to the Intelligence Staff.

3. The composition of the Fusion Centre will vary according to the deployed resources. It is based on the intelligence organization and could include representation from some or all of the following:

a. Air.

b. Aviation.

c. EW.

d. Reconnaissance.

e. Special Operations Forces (SOF).

f. Artillery.

g. Targeting and BDA.

h. HUMINT Organization.

i. SIGINT Organization.

j. CI Specialists.

k. Single source intelligence such as MASINT.

l. Intelligence Analysts.

m. Open source intelligence.

n. Representatives of other agencies for example, CSE, CSIS, CCRA, DFAIT, RCMP, DFO, Coast Guard, etc.

4. **The Sensor Management Cell.** The role of the Sensor Management Cell is to exercise command and control of the Sensors assigned to it, in accordance with the demands of the Collection Plan and to anticipate the assessed future collection requirements of the intelligence staff.

5. The integration of first three stages of the Intelligence Cycle, Direction, Collection and Processing, into the ISR Fusion Centre allows the closest relationship between the various sensors, the tasking system and the fusion and analysis function.

[55] Ibid

6. The information and intelligence flows in the ISR system are shown in the diagram at Figure 4-1 below.

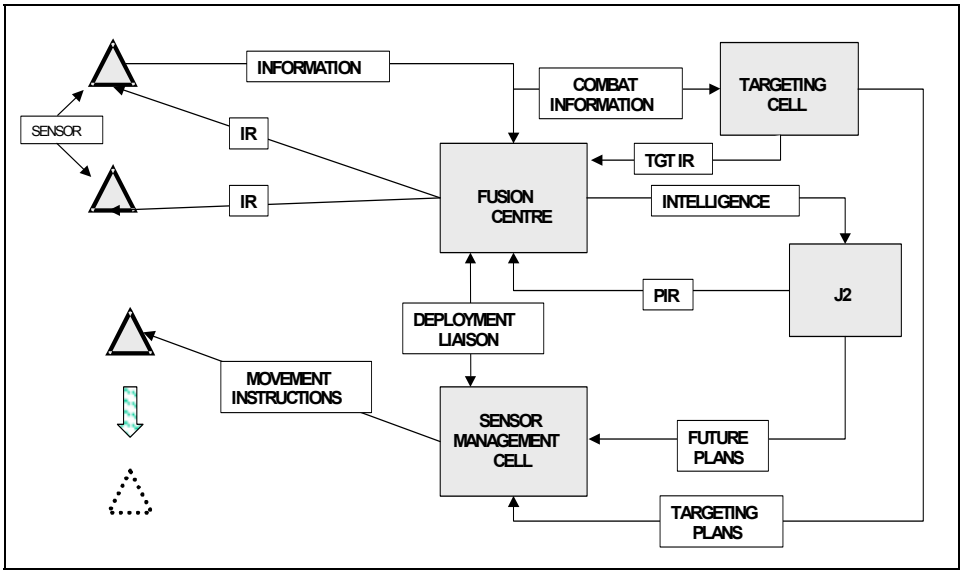

Figure 4-1 Information and Intelligence Flows in an ISR system

7. **Command and Control of the ISR System**. Adopting the principle of Centralized Coordination, there should be an overall commander of the ISR System. He will have overall responsibility for conduct of ISR operations in accordance with the commander's mission.

8. **The Targeting Cell**. In order to derive the maximum synergy from the ISR system, the Targeting Cell should be fully integrated into the system. It is accepted that arrangements may not support this integration but in order to achieve maximum benefit from ISR, the closest liaison should be maintained between the Targeting Cell and the remainder of the ISR system.

415. CONCLUSION

1. The ISR system provides the means of meeting the increased demands placed on the intelligence process by Manoeuvre Warfare. However, in coalition operations, ISR places a greater emphasis on interoperability for, if the individual components of the system are unable to interoperate, the synergy derived from the system will not occur.

2. The effective operation of the ISR system requires that all the component systems are operating to a single common standard and that ISR operations are based on a common doctrine. When ISR operations are to be conducted on a coalition basis, these requirements are essential for success.

416. THE INTELLIGENCE ESTIMATE

1. The primary purpose of the Intelligence Estimate is to provide the commander with a reliable basis for making decisions about his own operations. The object of the Intelligence Estimate is to analyse the adversary’s situation and to assess their capabilities, likely intentions and probable courses of action at a particular time.

417. METHODOLOGY FOR THE ESTIMATE

1. The creation of the Intelligence Estimate is a process that comprises an analysis of the situation and an assessment. The estimate must include:

a. An assessment of the adversary's capabilities and likely intentions based on the available intelligence.

b. Identification of the adversary's probable courses of action and the order of probability of their adoption.

418. FACTORS TO BE CONSIDERED

1. When compiling an Intelligence Estimate, the following factors are taken into account:

a. The commander's mission.

b. Weather and terrain.

c. The general situation of the adversary and their conduct of operations so far.

d. The activities and capabilities of the adversary to include possible reinforcements and any forces in adjacent areas that are able to influence operations in the commander's Area of Interest.

e. The options and possible courses of action open to the adversary including those in adjacent areas.

f. The adversary's likely intentions including their aims and objectives in immediate and follow-on operations.

419. PRINCIPLES

1. To prevent speculation, as a basic principle, assessments have to be based on the best possible intelligence. Assumptions may be used when there are gaps in the intelligence staff's knowledge. To avoid any misunderstanding, assumptions should always be clearly identified as such. Logical consistency of thought and a clear separation of facts from assumptions are essential for the production of a reliable assessment.

2. The intelligence estimate results in a forecast based on degrees of probability. It is a series of logical deductions drawn from the information available and influenced by the knowledge and experience of the author. There must always be close liaison between intelligence and operations staffs, particularly when considering the commander's Priority Intelligence Requirements (PIRs) and preparing the information requirements arising from them, which shape the Estimate.

3. Many facts and conclusions from the Intelligence Estimate will also be used in an operational appreciation for example, adversary strengths, capabilities, vulnerabilities, intentions, possible courses of action and the most likely course.

420. ADDITIONAL GUIDANCE

1. When analysing a particular force's situation and the results it has achieved, consideration should be given to deducing the intentions of the force from its past activities.

2. When analysing current activities and assessing a force's capabilities, the focus should be on availability in terms of strengths, time and space, combat readiness, combat effectiveness and terrain.

3. When analysing options open to a particular force, its probable courses of action and intentions, it is advisable to look at the situation from that force's point of view bearing in mind what he may know about our own situation. This requires an extensive knowledge of its commander's mentality, and of its organization, patterns of activity, tactics and habits. All factors affecting its capabilities and operations should be taken into consideration to include a force comparison from an opposing point-of-view. It should be assumed that the commander has a reasonably good knowledge of our capabilities, intentions and vulnerabilities although this could be degraded by deception.

4. When analysing a force's possible future intentions, one should bear in mind the force's general situation and what intentions have been identified so far. Since the intelligence estimate is based on assumed aims, a series of separate estimates, each based on differing aims, may have to be made. In the course of time, complete revision may be necessary in the light of fresh information.

5. When assessing a force's probable intentions, and probable course of action, the order of probability of their adoption should always be stated.

421. TYPES OF INTELLIGENCE ESTIMATES

1. **Intelligence Estimate**. There are three choices in terms of the type of Intelligence Estimate to be produced:

a. **The Deliberate Intelligence Estimate**. Due to the nature of CF operations, it may be beneficial to conduct a deliberate Intelligence Estimate (written[56]) in which theatre activation is to be initiated or the proposed area of operations is complex with regard to terrain, ethnicity or the environment (for example, urban ops).

b. **IPB Intelligence Estimate**. It may be advantageous for the intelligence staff to capture the essence of the IPB process and disseminate it beyond their own HQ. The intelligence estimate is essentially a by-product of IPB and is normally disseminated as a graphical product. At the tactical level, a graphical Intelligence Estimate focusing on the effects of terrain on adversary options, as well as a higher level picture is normally sufficient; and

c. **Combat Intelligence Estimate**. The Combat Intelligence Estimate is an abbreviated version of the Intelligence Estimate to be used when there is little time available.[57]

[56] The format for a written Intelligence Estimate is at Annex A.
[57] More detail on the Combat Intelligence Estimate is contained in the Land Forces Intelligence Field Manual (B-GL-357-001/FP-001)

This Page Intentionally Blank

ANNEX A - FORMAT FOR AN INTELLIGENCE ESTIMATE

Unit/HQ:

Place/Location:

DTG & Zone:

Maps/Charts and other documents:

1. **Review of the Situation.**
   a. Adversary Forces.
   b. Friendly Forces.
   c. Commander's Mission.
   d. Adversary's wider aims and courses.
   e. Commander's Priority Intelligence Requirements.
2. **Adversary Aim.**
3. **Factors[58].**
   a. Terrain (approaches, axes, routes, obstacles, effect on own/adversary forces).
   b. Adversary (dispositions, equipment, activity, vulnerabilities).
   c. Relative Strengths (allocations, reinforcements, committed/reserve forces, combat effectiveness).
   d. Time and Space.
   e. Assessment of Tasks.
   f. Weather.
   g. Logistics.
   h. Local Population/Refugees.
   i. Air Situation.
   j. Deception.
   k. Security and Surprise.
   l. Personalities.
   m. Morale.
   n. Weapons of Mass Destruction.
   o. Adversary Capabilities.
4. **Summary of Deductions.**

[58] Including, where appropriate, deductions and vulnerabilities in each case.

5. **Adversary Courses of Action.**

   a. **Course A.**

      (1) Advantages.

      (2) Disadvantages.

   b. **Course B.**

      (1) Advantages.

      (2) Disadvantages.

   c. **Course C.**

      (1) Advantages.

      (2) Disadvantages.

6. **Adversary's Most Probable Course of Action.**

7. **Adversary's Probable Plan.**

   a. Mission.

   b. Execution.

8. **Summary of Adversary Vulnerabilities.**

9. **Information Requirements.**

   a. Gaps in knowledge.

   b. Priorities for collecting/requesting intelligence.

……..……Signature
……..…….Rank and appointment

ANNEX B - INTELLIGENCE ANNEX FORMAT[59]

OPLAN XXXXX
OPERATION XXXXXX

ANNEX D - INTELLIGENCE

1. **SITUATION.**

a. **General.** With this paragraph the planner should explain the aim of the Annex and provide the basic guidance on the conduct of Intelligence in support of the Operation.

b. **Military Threat.** This paragraph provides a summary of the key points of the risk/threat assessments that are normally described in detail, for each phase of the operation, in Appendix 1 (Risk Assessment).

c. **Enemy/Adversary/Parties Course(s) of Action (COA).** Likely courses of action of the enemy/adversary or involved parties and factions are to be described in this paragraph, in order of probability, underlining, in particular, the most dangerous.

d. **Area of Intelligence Responsibility (AIR).** The Area of Intelligence Responsibility will be designated by the superior command to meet the requirements of the mission. It will normally focused on the operational area defined to the Commander and will be limited by the capabilities of the means at his disposal to conduct the Intelligence effort.

e. **Area of Intelligence Interest (AII).** The Commander's AII must be defined at each level of command to comprise those areas beyond the assigned AIR where factors and developments are likely to impact upon the Commanders current or future operations. It may include nations, states or factions outside the immediate operation area. Intelligence on the AII normally exceeds the capabilities of the means at disposal of the commander and is to be requested to superior and lateral commands.

2. **PRIORITY INTELLIGENCE REQUIREMENTS (PIRs)**

Critical requirements, for which the Commander has an anticipated and stated priority in his task of planning and decision-making, are to be listed in this paragraph as PIRs. They are derived from the Commander's Critical Information Requirements (CCIRs) listed by the J2 and will be approved by the Commander.

3. **INTELLIGENCE TASKS.** Within this subtitle the planner has to define:

a. Tasks assigned to subordinate HQs/Commands.

b. Contributions requested from supporting HQs/Commands.

4. **INTELLIGENCE STRUCTURE.** This paragraph details the intelligence organization to be employed with related systems and connectivity, with particular reference to the following:

a. **Intelligence Systems Architecture.** Detailed instructions are provided in Appendix 2.

b. **Collection, Co-ordination and Intelligence Requirements Management (CCIRM).** Detailed instructions are provided in Appendix 2.

c. National Intelligence Cells (NICs).

[59] Refer to BI-SC FPG INTEL for complete format.

d. **Target Intelligence (TARINT).** Detailed instructions are provided in Appendix 4.

e. **Human Intelligence (HUMINT).** Detailed instructions are provided in Appendix 5.

f. **Imagery Intelligence (IMINT).** Detailed instructions are provided in Appendix 6.

g. **Signals Intelligence (SIGINT).** Detailed instructions are provided in Appendix 7.

5. **COUNTER-INTELLIGENCE AND SECURITY (CI & Sy).** This paragraph must address the significant CI & Sy requirements. The full details are contained in Appendices 8 and 9.

6. **COMMUNICATIONS REQUIREMENTS.**

a. **Use of Hardware and Software.** This paragraph provides guidance on the employment of Hardware and Software, based on the equipment that can be provided by the participating nations and organizations.

b. **Secure Communications.** This paragraph lists the secure communications that are required, as a minimum, and the level down to which they are to be established, it must contain a clear reference for coordination instructions provided in the CIS Annex (Q).

7. **REPORTS AND DISTRIBUTION.** Reporting and distribution advice will be laid out in Annex CC of the respective COP/OPLAN/OPORDER. However, the reports are to be completed in accordance with the Bi-SC Reporting Directive and/or supplementary directives. For NATO operations the following reports are mandatory:

a. The Intelligence Summary (INTSUM)

b. The Intelligence Report (INTREP)

c. The Counter-Intelligence Summary (CI-INTSUM)

d. The Counter-Intelligence Report (CI-INTREP)

e. Target Status Assessment Report (TSAREP)

8. **OTHER INSTRUCTIONS.**

a. **Documents.** The appropriate national and NATO references for Intelligence Operations should be available.

b. **Intelligence Staff.** If required, this section defines any constraints for the manning of the intelligence staff.

c. **Geographic Support.** This paragraph should provide basic indications of the geographic support information required to complete, from the Intelligence perspective, Annex T, Environmental Support.

d. **Maritime Intelligence.** If required by the operation, this paragraph should contain appropriate instructions that can be amplified by an Appendix 10.

e. **Release/Exchange of Information/Intelligence with non-NATO Contributors.** This paragraph should provide instructions on the release exchange of information/intelligence. These instructions must be based on the pre-operations policy decisions taken by the NATO Military Committee, after agreement with nations on a case by case basis, and comply with Reference I.

f. Measures for the intelligence exploitation of PWs, captured documents, and captured

equipment including associated technical documents[60].

APPENDICES:

1. Risk Assessment
2. Intelligence Systems Architecture and CCIRM
3. Global Geospatial Information and Services
4. Target Intelligence
5. Human Intelligence
6. Imagery Intelligence
7. Signals Intelligence
8. Security
9. Counter-Intelligence
10. Maritime Intelligence

[60] Detailed procedures for the intelligence exploitation of PWs, documents and equipment are described in the following publications: Prisoner of War Handling, Detainees, Interrogation and Tactical Questioning (B-GJ-005-110/FP-020); and Handling of Captured Personnel, Equipment and Documents (NATO AJP 2.5)

This Page Intentionally Blank

CHAPTER 5

OPERATIONAL INTELLIGENCE

501. INTRODUCTION

1. The purpose of this chapter is to provide the procedural guidelines for intelligence support at the Operational level.

2. The mission of intelligence is to provide timely, accurate, relevant, predictive, and usable intelligence to the commander. At the Operational level, Intelligence focuses on the capabilities and intentions of current and potential adversaries and the effects of the environment on adversary and friendly operations. The Intelligence staff monitors events in the area of interest and supports the conduct of joint campaigns.

502. JOINT OPERATIONS

1. Joint operations are defined as operations in which the elements of more than one service or environment participate. Joint operations may involve air, space, maritime, amphibious, land and special operations forces. A joint operations plan synchronises the employment of these forces. A joint operation is oriented on the adversary's strategic and operational centre of gravity (CoG).

2. The Operational level is concerned with the employment of the whole force through the conception, planning and execution of campaigns and major operations. These must contribute directly towards achieving previously defined military-strategic objectives, which are drawn from the overarching political aims of the operation. The operational focus of joint military activities will be at the regional level. Joint Force Commanders provide the link between strategic level direction and lower level execution.

503. PURPOSE OF INTELLIGENCE AT THE OPERATIONAL LEVEL

1. **Supporting the Commander.** The Intelligence staff supports the commander in determining objectives, and the planning, execution, and assessment of operations. The intelligence staff will also provide intelligence support to subordinate commands and continually support force protection. This function is coincident with, but separate from, the Intelligence staff's responsibilities to support other staff divisions as well as responsibilities to meet subordinate components' Requests for Information (RFIs).

2. **Integrated Mission Support (IMS).**[61] There are four principal elements in a modern operationally deployed weapon system: the equipment itself; its operators; the logistic support to maintain it; and the mission support information that enables its operational capability. The mission support function covers a variety of activities, all of which need to be coordinated into an integrated whole, throughout the life of the equipment: this forms the concept of Integrated Mission Support (IMS). The quality and quantity of IMS required, and the importance of the latter to mission success, increases directly with the complexity of the weapon system supported. Moreover, in joint and multinational operations, where effective interoperability between individual platforms and weapon systems is paramount, IMS must be both consistent and coherent across the entire force. Operational level Intelligence forms a crucial element within IMS. Specialist information on specific adversary equipment characteristics and emitter parameters is vital to providing timely IMS. Mission dependent data is required in the form of: threat overlays to support mission planning systems, warning and defensive aids systems, electronic warfare information for use with electronic support measures and data parameters to support automatic target recognition systems.

3. **Identifying and Determining Objectives.** All aspects of military operations are dependent on the determination of clearly defined objectives. In the process of assisting in the identification of objectives, the Intelligence staff should understand the commander's responsibilities, his mission and intent, means available (including multinational forces), adversary forces and the characteristics of the operational environment. Operational level intelligence must provide the commander with an understanding of the

[61] JDCC (UK), Joint Operations (JWP 3-00)

adversary in terms of his estimated intent, objectives, strengths, weaknesses, values, and critical vulnerabilities. The Intelligence staff then recommends attacking those adversary capabilities and exploiting those adversary vulnerabilities critical to likely courses of action – both friendly and adversary. Once the commander determines objectives, the Intelligence staff will continuously review them with respect to the adversary and the changing situation to see whether they remain relevant to the commander's intent. Intelligence will also provide considerable input to the threat assessment that is the basis of Force Protection.

4. **Planning and Conducting Operations.** Intelligence should be provided at all command levels for planning, directing and conducting operations. It will be critical to commanders and staffs in identifying and selecting specific objectives and targets and in determining the means, operations, and tactics to be used in achieving the Operational Commander's mission. The Intelligence staff then supports the execution of the plan with the intelligence needed to sustain the operations, attain objectives, and protect friendly forces. To maintain the initiative, the Commander will seek to conduct his decision/action cycle more rapidly than his adversary and thus, react faster to the evolving situation. The Intelligence staff has a key part to play in this process by meeting the Commander's Priority Intelligence Requirements (PIRs) as quickly as possible.

504. OVERVIEW OF INTELLIGENCE REQUIREMENTS

1. Battlespace situational awareness is the requirement that focuses on three overlapping and complementary components: the adversary, the operational environment, and the friendly forces. The Intelligence staff is responsible for providing information/intelligence on the first two components. The Operations staff provides the third. The adversary component requires knowledge of the current dispositions and activities of the adversary forces throughout the battlespace. It requires knowing the current and future capabilities of adversary forces to operate in and across each battlespace dimension based on detailed analysis of the effects of weather on operations and terrain analysis. The operational environmental component requires the knowledge of geography, climate and demographic factors and their impact on operations.

2. **The Adversary.**

a. **Character.** There is a requirement for intelligence on the adversary, relating to political leadership, ideology, policies, structures, national morale, psyche, tradition, personalities, history and status of the armed forces. In total, this intelligence forms the strategic context in which adversary operations are considered. Such intelligence supports an assessment of the adversary's will and commitment, popular support, willingness to accept casualties, and susceptibility to psychological operations (PSYOPS) and deception.

b. **Capabilities.** There is also a need for intelligence on the organization and resources of the civil authorities, the command structure, order of battle (ORBAT), standard of training, doctrine, weaponry and equipment including technical characteristics, ISR assets, and logistics of the armed forces. Such intelligence supports an assessment of the adversary in relation to friendly forces. This intelligence is used in particular to assess force ratios, the nature of the threat and adversary strengths and weaknesses, including critical vulnerabilities.

c. **Location.** Positional intelligence is required in order to identify adversary posture to assist in assessing intentions and threat, provide warning and enable efficient targeting to be carried out. During Peace Support Operations (PSO) the distribution of population groups may also be important.

d. **Intentions.** Understanding adversary intentions and likely reactions to friendly force activities is fundamental to operational success. It gives commanders an advantage in preparing and protecting own forces, and allows them to pre-empt adversary operations. It also enables them to select decisive points at which to concentrate the capabilities and efforts of own forces against adversary vulnerabilities, in order to attack the adversary centre of gravity. Predictive intelligence reports and assessments are critical to this requirement.

3. **The Operational Environment.**

a. **Geography/infrastructure.** Land, air and maritime geographic, economic and infrastructure intelligence is required in order to assist force packaging, preparation and deployment of the force, efficient planning and conduct of operations, as well as targeting.

b. **Climate.** Intelligence relating to prevailing weather conditions and the likely effect on intelligence sensors and platforms, strike assets, movement and manoeuvre, personnel, logistics, and communications, is required to decide the timing of deployment and operations, to assist the training and preparation of the force, and to aid deception and surprise.

c. **Demography.** Intelligence about the culture, language, religion, laws, and traditions, of the population in the operational area is required to assist the preparation of the force and for the planning and the conduct of operations. Technological advances in computer processing, precise global positioning, and telecommunications enhances the operational level commander's capability to determine accurate locations of friendly and adversary forces, as well as to collect, process, and disseminate relevant data to thousands of locations. These capabilities, combined with the ability to deny or degrade the adversary's ability to collect, process, and disseminate an uninterrupted flow of information, will provide the commander with information superiority. Likewise, the fusion of all-source intelligence along with the integration of sensors, platforms, command organizations, and logistic support centres will allow a greater number of operational tasks to be accomplished faster, and will enhance battlespace awareness — a key component of information superiority.

d. **Space.** Operations in, and from space, are becoming more important. Due to the nature of space operations, they will primarily be strategic in nature. Despite this, space-based sensors will have an impact on the operational and tactical levels of operations. This use of space-based sensors must be accounted for in intelligence planning. Also the counter space battle must also be planned.

505. INTELLIGENCE SUPPORT TO PLANNING

1. Planning for an operation is an essential function of the Joint Task Force Commander (JTFC). The JTFC must direct planning and decide upon the Course of Action that will form the basis of his campaign plan. The campaign plan is the practical expression of operational art. A campaign plan has amongst other things an End-State, defined Centres of Gravity (CoG), Decisive Points, determination of Main Effort, Culminating Points[62] and exit strategies[63].

2. The Intelligence Cycle is a simplified conceptual model of how intelligence operations are conducted. Details of the Intelligence Cycle can be referenced in Chapter 2 of this publication.

3. At the Operational Level, the intelligence cycle provides the basis for common intelligence terminology, tactics, techniques and procedures. Knowledge of the intelligence cycle is fundamental to understanding the intelligence operations addressed in the latter part of this chapter.

4. The Commander's mission provides the focal point for all phases of the cycle. The activities within each phase are conducted continuously and in conjunction with activities in other phases.

506. CF OPERATIONAL PLANNING PROCESS (CF OPP)

1. The CF Operational Planning Process (CF OPP) allows a JTFC to prepare timely and efficient operational plans in response to an actual or developing crisis. The CF OPP is applicable to any Strategic, Operational or Tactical HQ. The overall process consists of five stages that are described in Chapter 3. [64]

[62] CF Operations (B-GG-005-004/AF-000), Art 313 Para 4.
[63] Civil-Military Cooperation In Peace, Emergencies, Crisis And War (B-GG-005-004/AF-023), Art 517.
[64] A summary of intelligence tasks during OPP at the Operational level is contained in Chapter 6 of AJP 2.1 – Intelligence Procedures.

507. JOINT INTELLIGENCE PREPARATION OF THE BATTLESPACE (JIPB)

1. The primary purpose of JIPB is to support JTFCs' and component commanders' campaign planning and decision-making. JIPB is a continuous process that enables JTFCs and their staffs to visualise the full spectrum of adversary capabilities and potential Courses of Action (COA) across all the dimensions of the battlespace. JIPB facilitates campaign planning and the development of friendly COAs. JIPB also provides the basis for intelligence direction and synchronization. JIPB is conducted prior to and during a joint force's operations, as well as during planning for follow-on missions. There is more detail on the process in Chapter Three.

508. INTELLIGENCE SUPPORT TO OPERATIONS

1. Enabling a commander to accurately visualize the battlespace requires carefully coordinated and synchronized intelligence operations. Intelligence operations are the wide-ranging activities conducted by intelligence staffs and organizations for the purpose of providing the commander with relevant, accurate, and timely intelligence. Effective intelligence operations enable commanders at all levels to apply their available forces wisely, efficiently, and effectively. Intelligence operations are characterized by centralized planning and decentralized execution. Intelligence operations seek to maximize the support offered to the operational level commander, while simultaneously providing specialized and detailed intelligence to other commanders and staffs throughout the joint force.

2. Of particular importance is the seamless provision of joint intelligence support to operational forces across the range of military operations as they deploy from one theatre to another. To effectively plan and execute unit missions, deploying intelligence personnel must know the supported theatre's intelligence concept of operations, intelligence architecture, estimate of the situation, map standards, and other theatre specific requirements. Intelligence producers should rapidly provide this information to deploying forces in a standardized electronic format.

509. INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR)

1. ISR at the Operational Level co-ordinates the Intelligence process and the various collectors in the Joint Force. It also incorporates the CIS to support it. The ISR system focuses on the JTFC's Area of Intelligence Responsibility (AIR) and identifies the JTFC's Area of Interest.

2. The Joint ISR system of systems must be capable of detecting, locating and identifying adversary combat forces. The identification and location of adversary CoGs, critical nodes, main axes, second echelons and weapons of mass destruction will be of prime importance. At the other end of the spectrum of conflict the ISR system must identify and locate key personalities and individual operatives, critical centres of activity, operating cells and/or groups. The protection of friendly formations from adversary reconnaissance and surveillance intelligence assets will also be a high priority.

3. The Intelligence Cycle applies well to ISR. Direction is key to the efficient use of staffs and collectors. Collection of data is fundamental to the development of situational awareness. Processing is executed in an all-source analysis organization and then intelligence and information is disseminated to those who need it. ISR and its resultant activities within the Intelligence process is critical to the successful implementation of the CF OPP and the attainment of the commanders objectives.

510. JOINT TARGETING

1. These articles are being held in abeyance so that they can be released in concert with revisions to CF Operations (B-GG-005-004/AF-000) and annexes D and E of Use of Force in CF Operations (B-GG-005-004/AF-005).

511. INTELLIGENCE AND INFORMATION OPERATIONS (IO) AT THE OPERATIONAL LEVEL

1. IO represent an integrating strategy at this level. IO links C2W, Public Affairs (PA) and Civil Affairs (CA)[65], and all of these apply at the Operational Level. Within a Joint Headquarters, an IO Coordination Cell (IOCC)[66] should be established to plan and assist in the execution of IO. Intelligence and counter-intelligence is represented in this organization. The IOCC maintains a database that can be analyzed to determine an adversary's IO capabilities, vulnerabilities and methods.

2. **Intelligence Support**. Intelligence support is critical to the planning, execution, and assessment of IO.

a. The joint staff intelligence (J-2) representative(s) assigned to support IO should be the liaison for intelligence support for all IO planning.

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

c. Intelligence products must support IO planning, provide analysis of a potential adversary's IO vulnerabilities, allow determination of a potential adversary's IO capabilities and intentions, and provide Indications & Warning (I&W) of any potential threat.

d. Guidance for specific intelligence support required for offensive and defensive IO is provided in CF Information Operations (B-GG-005-004/AF-010) Chapters II, "Offensive Information Operations," and III, "Defensive Information Operations," respectively.

512. INTELLIGENCE SUPPORT TO POST CONFLICT OPERATIONS

1. The ultimate end-state in any operation is a return to a politically led operation. At some point in an operation there must be a hand over of responsibility from military personnel to civilian personnel. This hand over must be included in strategic and joint force planning. Intelligence supports this transition in many ways, but primarily it must provide Indications and Warning of threats to a secure environment.

513. JOINT INTELLIGENCE ARCHITECTURE

1. A JTFC must be capable of coordinating the actions of people, organizations, and resources at great distances. Successful operations require that the JTFC be supported by an integrated C4I infrastructure that is capable of generating and moving intelligence, operational information, and orders where needed in the shortest possible time.

2. To prevail, the JTFC's decision-making and execution cycles must be consistently faster than the adversary's and able to provide better information. Being faster and better requires having effective control over the collection, processing, and dissemination of intelligence.

3. Therefore the C4I support must be interoperable, flexible, responsive, mobile, disciplined, survivable, and sustainable. Intelligence organizations use a variety of sensors and other information sources to collect and analyze data and produce, providing the communications interface and media required to move intelligence.

514. CHARACTERISTICS

1. The joint intelligence architecture must be a dynamic, flexible structure capable of providing global access to an information grid that consists of all intelligence sources at all echelons.

[65] CF Information Operations (B-GG-005-004/AF-010), Art 101 Para 1a(9)(h).
[66] Ibid, Art 401.

2. The architecture is integral to each phase of the intelligence cycle — from planning and direction through dissemination and integration, with evaluation and feedback being done throughout each phase. The architecture supports intelligence functions over a distributed global network employing communications systems, computers, space-based C4I support systems, and their associated resources and technologies.

3. The operational architecture supports the range of military operations as envisioned during the Operational Planning Process. To that end it supports the intelligence requirements of the JTFC. It incorporates the policies, procedures, reporting structures, trained personnel, automated information processing systems, and connectivity to collect, process and disseminate intelligence that is fused into the JTFC's C4I systems.

515. PLANNING CONSIDERATIONS

1. Joint intelligence architecture planning requires early identification of information requirements including procedural and technical parameters. Establishing information flow, timeliness, content, format, and priorities will help shape the requisite joint intelligence architecture's technical specifications that most efficiently supports a JTFC.

2. Joint intelligence architecture planning must ensure survivability, security, and interoperability of both information architectures and the information contained therein for all combinations of government-commercial configurations. Organizational, doctrinal and personnel issues should also be considered to maximize the benefits of technical architectures for the goals of the JTFC.

516. REQUIREMENTS

1. The joint force Intelligence staff is responsible for establishing the joint force intelligence operational architecture required to accomplish the assigned mission. This architecture must be capable of being tailored to support the JTFC's information requirements. Intelligence must be provided in a form that is readily understood and directly usable by the recipient without providing the user irrelevant data.

2. Dissemination of intelligence consists of both "push" and "pull" control principles. The Intelligence staff is responsible for setting these controls. The "push" concept allows the higher echelons to push intelligence down to satisfy existing lower echelon requirements or to relay other relevant information to the lower level. The "pull" concept involves direct electronic access to databases, intelligence files, or other repositories by intelligence organizations at all levels. "Push" updates must be based on the JTFC's PIRs to ensure that the JTFC receives critical information and intelligence. Other information must be available on an as-needed "pull" basis so that the joint force Intelligence staff avoids information overload.

3. The operational architecture must ensure that no source of information collection, production, or dissemination is subject to a single point of failure. At the same time, the architecture must identify and eliminate the unnecessary duplication of intelligence capabilities so that scarce resources can be focused to meet prioritized requirements.

4. The operational architecture must be capable of accommodating the widest possible range of missions and operational scenarios. It must respond to the JTFC's requirements for information at any time and any place and be capable of supporting multinational operations with no loss in timeliness. In addition it must achieve a seamless integration of the JTFC's decision-making and execution cycles with all phases of the intelligence cycle. In developing the operational architecture, the intelligence community must streamline the processes in each phase of the cycle to ensure responsiveness to the JTFC's requirements. Development and implementation of the intelligence operational architecture must be closely coordinated with CIS.

517. THE INTELLIGENCE TASK ORGANIZATION

1. The design of the intelligence organization, particularly the collection force package, to meet the requirements of a particular operation and operational environment, must be addressed early in the planning

stage. This is a DCDS responsibility in concert with the J2/DG Int and supporting commands. The resulting intelligence architecture must centre on the JTFHQ and describe links and tasking authorities to all collection and processing activity, to superior and subordinate commands, and to flanking formations. The CDS, in allocating forces and defining the support available for an operation, defines the level of intelligence support available to the JTFC. The DCDS and the J2/DG Int assist the CDS in this responsibility.

2. The JTFC determines what intelligence capabilities and assets are needed to support the operation and then liaises with J2/DG Int and COS J3 to establish how the force can be supported. Requests for intelligence support from other national agencies and from allied agencies are routed through NDCC 2, although, once these links are established, the JTFC may liaise directly with these agencies.

518. JOINT INTELLIGENCE CENTRE

1. The Joint Intelligence Centre (JIC) is the primary intelligence organization providing support to the JTF Headquarters. The JIC concept fuses the main support capabilities of all the components (multi-service) and combat units into a central location for intelligence support. Although the JIC cannot be expected to completely satisfy every RFI, it can coordinate support from other intelligence organizations, lower, higher, and laterally.

2. The JIC has a flexible design and can expand to meet the needs of the JTFC as required. During non-crisis periods, JIC personnel levels are normally maintained at the minimum level required to perform essential functions such as I&W, current intelligence, collection management, and General Military Intelligence production in the JIC's area of production responsibilities.

3. The JIC:

a. Is responsible for processing all available information (including open source material) and intelligence - whether it is basic, current, applied or targeting intelligence.

b. Requires a capable, task-organized structure in terms of manning, systems applications and communications. The JIC must be capable of processing large amounts of information in order to meet local IRs as well as the demands of superior headquarters and subordinate formations.

c. Supports a deployed JTFHQ comprising a number of elements:

(1) A headquarters to provide command, control, personnel and logistic support.

(2) CF NIC

(3) The Intelligence Production Section, with specialist teams dealing with:

(a) Current intelligence.

(b) Current ORBAT and Table of Organization and Equipment.

(c) Support to C2W.

(d) Target development.

(e) Tailored geographic and hydrographic data.

(4) Specialist intelligence staff such as EW, artillery, engineer, SF, maritime operations and OSINT experts.

(5) Single-source feeds such as the Recognised ELINT Picture and ground terminals linked to near real-time collectors such as UAVs and SF patrols.

(6) Liaison Officers (LOs) from superior, subordinate, flanking, and coalition headquarters.

519. NATIONAL INTELLIGENCE CELLS

1. Although the JTF Commander may arrange the organization of the JTFHQ as he deems appropriate to perform the required mission, his staff should always include intelligence representatives from participating nations and services as required, for example, in the form of nationally contributed augmentation personnel. Additionally, a number of NICs would normally be associated with the JTFHQ provided by contributing nations on a voluntary basis, to act as gateways between the national intelligence agencies and JIC. These elements should, in principle, be self-sustainable.

520. COLLECTION PLANNING

1. **Levels of Command.** Each level of command controls its own set of collection assets, but advances in technology and the nature of operations mean that the IRs at each level of command may be met by collection assets at more than one level. For example, strategically controlled Imagery Intelligence (IMINT) and Signals Intelligence (SIGINT) sensors can produce a wealth of tactical information, while HUMINT collection assets controlled at the tactical level can report on activities, which have strategic and political importance. In providing operational intelligence support, flexibility in the tasking and allocation of collection assets will be required.

2. **Collection assets.** A distinction between strategic, operational and tactical collection is therefore not always clear. As a rule:

a. **Signals Intelligence.** Static or permanently located SIGINT collection assets within the CF are assigned to the Canadian Forces Information Operations Group (CFIOG). Tasking is primarily at the strategic level in support of Defence Intelligence priorities. The focus is largely on foreign military targets of a strategic nature; however, in the increasingly complex communications world, these assets often have access to operational and tactical level Intelligence. Another avenue for the tasking of static CF SIGINT assets is through the national SIGINT authority (CSE) in support of the National Cryptologic Program (NCP). Tasking supporting the NCP is generally against foreign political and leadership entities. The CF also has the capability to deploy SIGINT assets that can support the operational or tactical Intelligence requirements of any of the components.

b. **Electronic Warfare.** EW assets are under command of the deployed commander and are primarily tasked for Force Protection, counter C2 and operational and tactical intelligence. A number of these assets have a SIGINT capability and, if made available, may be tasked against operational or strategic targets.

c. **Imagery Intelligence.** IMINT collection assets that have utility at the operational level include the output of overhead reconnaissance platforms, while tactical assets include tactical air reconnaissance and UAVs.

d. **Human Intelligence.** At the operational and tactical levels, SF, specialist debriefers and agent handlers, military observers, liaison officers, CI teams, special reconnaissance, and armoured reconnaissance, will be available.

e. **Geospatial Intelligence.**Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Assets at the strategic level include worldwide library acquisition. At the operational level collection is conducted by deployed terrain analysis teams.

3. **The Balance of Collection Capability.** The capability, and hence the value, of each collection discipline (that is, IMINT, SIGINT, HUMINT, etc) varies according to the type of operation, the nature of the adversary and the operational environment, and the phasing of the operational plan will all have an influence on the types of collection undertaken. At the upper end of the operational spectrum, the technical sensors providing IMINT and SIGINT cope best with the collection requirements of rapid tempo and modern manoeuvre warfare, but the capability is reduced if the nature of the adversary does not offer suitable targets or weather and terrain constrain collection opportunities. In other operational environments such problems

are even more acute. In these circumstances HUMINT collection takes on increased importance, but collection assets must have freedom of movement in the area of operations. To be of real value collection assets must be deployed early, noting that appropriate language skills are essential. Finally, the phasing of the operation will have an effect. Strategic collection, for instance, takes on additional significance during the planning phase when operational and tactical collection assets cannot yet be deployed.

4. **The Limits of Collection.** All collection assets have limitations. It is the responsibility of the J2 staff to ensure that the commander and all staff branches are given a realistic appraisal of collection capability, including the limitations of each collection asset, its vulnerability to physical and electronic attack and to deception, its coverage of the AO and the response time to meet requirements. Commanders should also understand the threat, strengths and weaknesses of adversary collection assets. Finally, commanders must acknowledge that they may well have to fight for intelligence.

5. **The All Source Approach.** Because of the range, balance and limits of collection capability, the underlying principle is that of the all-source approach. This concept encompasses the exploitation of all available collection assets from all levels of command, packaged according to the nature of the adversary, the operation and the operational environment, and focused by the CCIRM process. It also involves the cross-cueing of sensors to ensure the most comprehensive coverage.

This Page Intentionally Blank

CHAPTER 6

GUIDELINES FOR JOINT INTELLIGENCE PRACTICE

1. This chapter[67] incorporates intelligence theory, concepts and operating experience into guidelines that will contribute to the planning and execution of effective and successful joint operations. They highlight the importance of inter-operability among CIS capabilities, procedures and information. Joint operations demand composite views of ongoing activity in all operating environments.

2. The fundamental responsibility of operational intelligence[68] is to provide decision makers, at all levels of command, with the fullest possible understanding of adversaries and the operational environment. This understanding includes a comprehensive knowledge of adversary goals, objectives, strategy, intentions, capabilities, methods of operation, vulnerabilities and sense of value and loss. The J2 staff must understand the adversary's character, culture, social norms, customs and traditions, language, and history. Understanding how an adversary will view the situation, his courses of action, and how he will react to our actions, should be an inextricable part of a continuing interaction between the J2 staff, the commander and other staff divisions. This comprehensive understanding is essential to: recognising challenges to national security interests; establishing policy; formulating relevant and attainable military objectives and strategy; determining, planning, and conducting joint operations that will help attain Canadian policy objectives; and identifying the adversary's strategic and operational centres of gravity.

3. The J2 staff must develop and continuously refine their ability to think like the adversary. They must offer this particular expertise for the maximum benefit of the whole of the JTF components. Joint commanders should require the J2 staff to assess all proposed actions from the following perspective: 'How will the adversary probably perceive this action, and what are his probable responses?' Carrying out these intelligence responsibilities calls for sound judgement as well as expertise. The following are some guidelines for joint intelligence practice.

601. ANALYSE OPERATIONAL INTELLIGENCE IN CONTEXT

1. Intelligence analysis is best done in a context of understanding the relative friendly-adversary situation. The commander must provide the J2 staff and supporting intelligence organizations with a clear understanding of the mission, intent, objectives, plans and the unfolding conduct of operations. The exchange of information and intelligence among commanders, all staff divisions and supporting intelligence organizations, must be continuous. The JTFC must weigh the pros and cons of providing information and intelligence to supporting intelligence organizations outside the Joint Operations Area (JOA).

602. DEFINE SUPPORT

1. The JTFC, supported by his J2 staff, determines the IRs and direction of the intelligence effort in support of his objectives. The intelligence effort is critical to the mission. Its nature, orientation and scope depend on the commander's decision on the relative importance of operational intelligence in accomplishing the mission. The J2 staff must refine the concept of intelligence operations to reflect changes in the commander's mission, estimate of the situation, and objectives. The JTFC, with his J2 staff, must ensure that intelligence objectives are correct, adequately stated, understood, synchronized, prioritised, and translated into actions that will provide the operational intelligence needed to accomplish the mission. Intelligence operations must be synchronized with other operational activity to ensure integrated and responsive support throughout all phases of the operation. Acquiring the appropriate operational intelligence is the responsibility of the commander.

2. Commanders, J2, J3 and J5 staffs developing strategy and operations and assigning mission responsibilities, have the earliest view of IRs and the intelligence effort that must commence at the inception of joint operations. It is at this early stage that the NDHQ and JTFHQ J2 staff must work-up the IRs both for their headquarters and their subordinate commands. They must identify the desirable JTF organic

[67] UK, Joint Operational Intelligence (JWP 2-00)
[68] While not widely used in the CF, some Allies and NATO use the abbreviation OPINTEL for Operational Intelligence.

operational intelligence capability (the intelligence architecture) and highlight any shortfalls. NDHQ must task national agencies, via the DCDS (J2/DG Int), to cover shortfalls and ensure operational intelligence is provided or available to those who need it. Assignment of appropriate movement priority within the Desired Order of Arrival Staff Table (DOAST) is essential to ensuring that required operational intelligence support will be available when needed to support joint operations.

603. INVOLVE THE J2 STAFF

1. The J2 staff must participate in decision and planning processes from the initial point when operations are contemplated. Effective operational intelligence support requires a two-way flow of essential information: the J2 staff should be integrated with the planning and operations staff to provide the commander with the best possible view of the situation and adversary, to identify, develop, and disseminate the operational intelligence needed to support operations. The NDHQ J2 staff must appraise the JTFC as to whether adequate operational intelligence support can be made available for the campaigns, operations and courses of action being considered.

604. CONSTITUTE JOINT INTELLIGENCE STAFFS

1. The JTFHQ J2 staff must have intelligence experts from each of the services and incorporate an understanding of each component's intelligence capabilities, limitations and requirements. The JTFC, through his Chief J2, must establish a task-organized J2 staff to manage centrally the joint intelligence effort together with a supporting JIC.

605. SYNCHRONIZE EFFORT

1. Commanders should require, and the J2 staff must ensure, that all operational intelligence activities are applied in time, space and purpose to support the operation plan. This synchronization process occurs across the range of military operations to provide timely, tailored and relevant operational intelligence to achieve assigned operational objectives. This integration of intelligence and operations ensures the totality of effort against the adversary's centres of gravity. The product of effective synchronization is maximum use of the operational intelligence component where and when it will make the greatest contribution to success.

606. UNDERSTAND REQUIREMENT

1. The J2 staff must resolve discrepancies between the JTFC's IRs and intelligence capabilities. If the staff do not understand fully how a stated IR relates to the commander's objectives, intent, or plans, the commander should be asked for clarification. In combat and other critical situations, the JTFC's intelligence needs should outweigh otherwise valid intelligence management efficiencies. Although it may later be found that an operation received duplicate or more intelligence than was needed, for an operation to receive less than is needed, when available, is an intelligence failure. If it is not possible to meet a commander's stated requirements, the commander must be notified immediately so that alternative intelligence requirements can be developed or the risks to operations of not having pertinent intelligence can be assessed.

607. ESTABLISH CAPABILITY

1. Intelligence capabilities and skills must be established in order to be available for contingencies and operations. This applies to all intelligence disciplines, but is especially true for Human Intelligence (HUMINT) and Signals Intelligence (SIGINT), which are not surged easily or with certainty, since relatively long lead times are required to establish resources. If HUMINT and

SIGINT access to denied areas is to be available when needed, then the resources must be developed and operated in advance of anticipated operations. Language capabilities are an example of skills that should be developed in good time to be available for contingencies.

2. Operational intelligence infrastructure must be constituted as soon as possible. Operational intelligence for decision making, operational planning, and conducting operations may not be adequate if intelligence activities are delayed until organic intelligence resources are available to fully constituted commands and forces. Theatre and national intelligence resources can bridge the gap. The JTF C3I requirements must be developed early during the pre-deployment phase to support the JTFC's concept of operations.

3. Where missions and objectives are contemplated for JTFs yet to be constituted or still assembling, NDHQ J2 staff must co-ordinate the identification and fulfilment of the estimated IRs as well as the intelligence needed for initial planning. Deliberate planning can facilitate a smooth transfer of responsibilities. In developing the concept of intelligence operations for a joint operation, the NDHQ J2 staff must address, in detail, the support desired during all stages of a crisis from strategic and operational intelligence organizations. The resulting Intelligence Annex must identify specific criteria to be met before designated J2 staffs and supporting organizations assume responsibility for operational intelligence activity initially provided by other organizations.

608. STRATEGIC SUPPORT

1. Strategic intelligence agencies support joint operations. They will make operations feasible that could not be accomplished without their access, capability, capacity, or expertise. They will need to be responsive to military requirements by providing rapid access to pertinent databased intelligence and current intelligence products as well as to collection (reconnaissance and surveillance) capabilities. The NDHQ J2 staff co-ordinate the delivery of strategic intelligence agencies, and will need to be prepared to commit sufficient and appropriate resources to ensure timely, complete, and accurate production and dissemination of required operational intelligence. They will prepare to place co-ordinating, communication and liaison resources well forward, commensurate with requirements for security, to assist in the identification and development of IRs and the delivery of operational intelligence products.

609. ENSURE UNITY OF EFFORT

1. For each operation there should be unity of intelligence effort to ensure complete, accurate and current operational intelligence to develop the best possible understanding of the adversary and the situation, and to reduce unnecessary redundancy and duplication. The JTFC has the responsibility and authority to determine, direct, and co-ordinate all mission-related operational intelligence activity through his J2 staff. When liaison personnel are provided by national intelligence agencies and operational formations, the host intelligence staff must ensure their integration within the operational intelligence organization.

2. Access to intelligence capabilities to support mission responsibilities must not be bound by inplace organizations or command configurations. This approach allows the commander and J2 staff to orchestrate intelligence activities to meet JTF IRs. The JTFC must have assured access to all necessary national intelligence capabilities. If higher priority or competing tasks preclude optimum support to the JTFC, he must be informed so he may make timely and alternative provision for operational intelligence, or assess the effects of gaps in intelligence to the operation.

3. Subordinate commanders employ organic operational intelligence capabilities to support their assigned missions. At the same time, those capabilities must be available to assist the joint effort under the JTFC's concept for synchronizing all assigned forces' IRs. The J2 staff must establish a flexible and task-organized operational intelligence architecture of procedures, organizations, and equipment focused on the JTFC's needs. This operational intelligence concept of operations complements and reinforces the organic capabilities at each echelon and, when necessary, provides direct support to subordinate commanders whose organic capabilities are inadequate or cannot be brought to bear.

4. The keys to unity of intelligence effort for joint operations are ensured access to any required operational intelligence capability and the co-ordination of all intelligence operations and associated activity. Cooperation between intelligence organizations is important, but it is not a substitute for a unified and co-ordinated effort. The JTFC must ensure that component commanders assist each other in collecting and

evaluating intelligence needed to the maximum extent compatible with the requirements of their respective commands and the JTF. This includes sharing intelligence sources, collection assets and operations, collection management, databases, intelligence production, and communications. This principle of sharing also applies to other forces and to intelligence organizations that support the JTF. Sharing is the responsibility of commands and organizations that have the ability to support joint operations. Sharing and mutual support are essential to integrating all resources and capabilities into a unified system that will best fulfil the prioritised IRs for joint operations. The JTFC must establish the command relationships for all assigned forces, including intelligence assets. Normally, components having organic intelligence staffs and forces will remain the assets of that component commander. If the JTFC wants organic intelligence assets of a component to support other units, the JTFC will usually assign that intelligence support mission to the component commander.

610. MAKE ALL ORGANIC INTELLIGENCE CAPABILITIES AVAILABLE TO THE ENTIRE JOINT TASK FORCE

1. All in-theatre operational intelligence capabilities must be made available to support any requirements of the JTF. The JTFHQ will require access to all of the products derived from the capabilities available to NDHQ and the component commands. The JTFHQ J2 staff manage the employment of all organic and in-theatre intelligence assets for the JTFC.

611. VIEW THE ADVERSARY AS JOINT OR UNIFIED

1. A JTF is potentially faced with adversary capabilities and operations of a joint nature. It is essential; therefore, that intelligence on the adversary is jointly constructed and considered in its entirety, not separately. Only by complete integration can the J2 staff determine or estimate the whole of the adversary situation.

612. KEEP OPERATIONAL INTELLIGENCE CURRENT

1. All aspects of operational intelligence must be kept current, including support to ongoing, planned and contingency operations. New information must be integrated with what is already known. The nature, purposes, content, location and availability of operational intelligence, including databases, must be systematically reviewed to ensure that it is necessary, appropriate and current. Commanders' IRs and resulting collection plans, together with RFIs, must be continually reviewed and evaluated against mission responsibilities.

613. MAINTAIN FLEXIBILITY

1. Operational intelligence structures, methodologies, databases and products need to be flexible to meet changing operational situations, needs, priorities and opportunities. They should support all possible strategies and tactics. The JTFC needs timely intelligence products to identify, influence and exploit opportunities. Intelligence organizations must be able to adapt rapidly to unforeseen events.

614. ENSURE ACCESSIBILITY OF INTELLIGENCE

1. Operational intelligence must be readily accessible to those who need it while still adhering to security requirements determined by the imperatives of OPSEC, source protection and national/international protocols. The JTFC must have access to all intelligence available in his AIR and be in receipt of sufficient tailored intelligence on his Area of Intelligence Interest (AII).

2. Whenever possible, the types of operational intelligence needed must be anticipated and arrangements made for personnel involved, including the operations, planning and other key staff personnel, to have the appropriate clearances and access. This should be done as a matter of routine before operations begin. Although some intelligence will require extraordinary protection (for example, to protect sensitive sources and methods or the fact that certain knowledge is held), all efforts must be made to ensure

access to required intelligence. Operational intelligence should be sanitised wherever possible and especially when personnel who need it cannot be cleared for knowledge of its sources and methods, cannot meet the security requirements for that category of intelligence material, or the timeliness for application is jeopardised. Security by sanitization is attained by effectively separating intelligence from its sources and methods. While intelligence should always be produced at the lowest possible classification to ensure the widest dissemination, operational intelligence product must not be 'diluted' by the sanitization process to a point whereby it ceases to be of real utility to the JTFC, his staff and component forces. A headquarters that is not capable of receiving and handling highly classified intelligence is unlikely to be in a position to deliver effective operational intelligence support to its decision makers.

3. The policy for sanitizing intelligence must be understood by the JTFC who, with the assistance of his J2 staff, has the best appreciation of the criticality, utility and time sensitivity, of the intelligence. The sanitization policy should be established prior to, or at the outset of, joint operations. This is of particular importance in multinational operations.

4. Where the sources and methods of critical information collection cannot be protected (that is, the intelligence cannot be sanitized), the commander must be informed. When the protection of the information sources and methods is paramount, the commander can then make a re-evaluation of objectives in light of the probable outcome of operations without the intelligence, or take action to disguise the source by additional, discernible collection activity.

615. USE AN ALL-SOURCE APPROACH

1. Information and intelligence from all sources must be processed into products that present the most complete, accurate, and objective view possible. Joint operations in particular require complete and composite views of the current situation and of the status of an adversary's land, sea, air and space forces.

2. Having access to and using all sources of information and intelligence is essential to understanding the current situation. Single-source intelligence analysis may lead to unbalanced or incomplete assessments. Use of the all-source concept and methodology will reduce the risks of deception. It will also become the basis for the nomination and development of counter-measures against hostile intelligence and operations.

616. DISTINGUISH BETWEEN FACT AND ASSESSMENT

1. The J2 staff and other intelligence producers must distinguish between what is known with confidence, based on the facts of the situation and the adversary, and what are untested assumptions. Intelligence can be facts that have been observed, or it can be a conclusion based on facts of such certainty that it is considered to be knowledge. Intelligence can also be conclusions and estimates deduced from incomplete sets of facts or induced from potentially related facts. Where intelligence is used for operations, these distinctions should be made and maintained. The commander's determination of appropriate objectives and operations may rest on knowing whether operational intelligence is 'fact' or 'assumption' and knowing the particular logic used to develop an intelligence estimate, as well as knowing the confidence level his J2 staff place on the provided intelligence. The confidence level scale should be used as often as necessary to present intelligence analysis and conclusions to decision makers in a uniform, consistent manner.

617. USE LIAISON

1. Intelligence liaison personnel must be employed on a basis designed to acquaint the receiving headquarters or unit with the operational intelligence requirements, responsibilities, capabilities, operations and units of the liaison officer's parent organization, and to help exchange or share all significant intelligence and information.

618. PRIORITISE COMPONENT INFORMATION REQUIREMENTS

1. The J2 staff must carefully manage the flow of operational intelligence to subordinate components. Critical, time-sensitive component Requests for Information (RFIs) should be expeditiously answered at the lowest command level possible.

619. RECOGNISE COUNTER-INTELLIGENCE AS A SOURCE OF INFORMATION

1. Counter-intelligence is an intelligence discipline with a distinct operational focus aimed at influencing an adversary's visualization of friendly capabilities and intentions. CI's primary purpose is the collection of intelligence required to implement countermeasures designed to degrade an adversary's intelligence and targeting capabilities. CI assets collect information and develop operational intelligence regarding threats to plans, operations, C2, logistics and sustainment assets from hostile intelligence services, as well as from asymmetric threats such as terrorist and organized criminal elements. Traditionally viewed as a separate and distinct intelligence discipline, modern views of CI emphasize the elimination of CI "stovepipes" capable of impeding a commander's ability to develop a comprehensive picture of the threat environment.

620. EMPLOY ALL DEPLOYED FORCES AS SOURCES

1. Information from reconnaissance and surveillance units and elements in contact with the enemy should be integrated with intelligence from other sources. Forward and engaged combat forces must be tasked to collect and report information. They have unique opportunities to collect significant information. A lack of contact with the adversary may be just as significant as positive intelligence.

621. USE THE CHAIN OF COMMAND TO SATISFY REQUESTS FOR INFORMATION

1. The JTFC and his J2 staff must use the chain of command to obtain operational intelligence. Using the joint intelligence architecture should facilitate a rapid, time-sensitive flow of operational intelligence throughout the chain of command. RFIs should be answered at the lowest possible echelon of the JTF or supporting joint intelligence infrastructure, and then shared vertically and horizontally.

2. Commanders, through their J2 staff, must negotiate authorized skip-echelon direct operational intelligence support' when necessary to provide timely critical intelligence for operating forces being constituted, in transit, or engaged. Analyst-to-analyst exchange is a form of 'skip-echelon' support. Intelligence analysts at all levels can contribute important perspectives to other intelligence organizations engaged in collecting, processing and disseminating operational intelligence. Command authorization of 'skipechelon' intelligence support does not alleviate the requirement to provide the same intelligence to intermediate commands through the chain of command and to supporting commands and organizations. 'Skip-echelon' intelligence support should be used as an exception to the normal method of dissemination.

622. STRUCTURE FOR CONTINUOUS OPERATIONS

1. Intelligence organizations must be structured for continuous day-night and all-weather operations. A JTFC needs this support to rapidly determine and exploit adversary vulnerabilities, to apply coherent and unrelenting force, and to protect operations and forces. The J2 staff and supporting intelligence production organization must establish 24 hour, all-source current intelligence teams together with staff officers to direct and manage intelligence operations. This concept of intelligence operations should provide for continuity of support even if communications are severely stressed or temporarily lost. The J2 (Ops) staff must: develop concepts of intelligence operations for remote terminal access that incorporate pre-positioned standard graphic databases; designate alternate staff for deployed intelligence staff elements and alternate organizations for intelligence production, which should include procedures and means for the designated alternate location to monitor activity; ensure the backup understands the supported commander's objectives, and is prepared to provide support when continuity is lost. Supporting intelligence organizations, such as NDCC 2 and elements of J2/DG Int, responsible for CCIRM and for intelligence processing and dissemination, must also be postured to provide 24-hour support. Comprehensive surveillance may be

effected by synchronizing the integrated use of different and complementary strategic, operational and tactical collection assets. Overlapping coverage by different collection resources and sensor types can operate against hostile denial and deception measures. Intelligence resources, activities, and communications must be structured and operated to be sufficiently survivable to ensure required operational intelligence support is available to commanders and forces. An important component of survivability is redundancy in critical C3I capabilities.

623. USE INTELLIGENCE LESSONS IDENTIFIED

1. Intelligence procedures must ensure a systematic approach to operational intelligence lessons identified.

This Page Intentionally Blank

GLOSSARY

AIR ***Area of Intelligence Responsibility***

The area allocated to a commander for which he is responsible for the provision of intelligence within the means at his disposal (AAP-6)

AI ***Area of Interest***

The area of concern to the commander, including the area of influence, areas adjacent thereto and extending into enemy territory to the objectives of the current or planned operations. This area also includes areas occupied by enemy forces who could jeopardise the accomplishment of the mission. (AAP-6)

AOR ***Area of Responsibility***

A defined area of land in which responsibility is specifically assigned to the commander of the area for the development and maintenance of installations, control of movement, and the conduct of tactical operations involving troops under his control along with parallel authority to exercise these functions. (AAP-6)

Asymmetric Warfare

Those actions which employ levels of forces and technologies to achieve a degree of effectiveness out of all proportion to forces employed, by seeking to exploit the vulnerabilities of NATO's civil and military infrastructures. (MC 161)

Battlespace

The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space environments, the included enemy and friendly forces, facilities, weather, terrain, the electromagnetic spectrum and the information environment within the operational areas and areas of interest.

CoG ***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)

Coalition

A grouping of nations or forces, usually on a temporary basis, for the accomplishment of a stated goal.

Collection

The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (AAP-6)

Combined

In concert with the forces of another nation.

CONOPs ***Concept of Operations***

A clear and concise statement of the line of action chosen by a commander in order to accomplish his mission. (AAP-6)

DL ***Decision Line***

A line on the ground where a commander must make a decision if he is to effect a result at a particular Target Area of Interest.

Direction

Determination of intelligence requirements, planning the collection effort, issuance of orders and requests to

collection agencies and maintenance of a continuous check on the productivity of such agencies. (AAP-6)

Dissemination

The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. (AAP-6)

INT ***Intelligence***

The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity, which results in the product and to the organizations engaged in such activity. (AAP-6)

IPB ***Intelligence Preparation of the Battlespace***

A systematic and continuous process of analysis of adversary/targeted force doctrine, order of battle, weather and terrain matched against the friendly commander's mission in order to determine and evaluate the threat's/targeted force's capabilities, intentions and vulnerabilities.

Joint

Involving two or more of the Services of the Armed Forces of a nation.

JIPTL ***Joint Integrated Prioritised Target List***

Once the JTL is expanded with the addition of targets drawn from the component operations plans, it becomes the Joint Integrated target List (JITL). Once the JITL has been approved, it is prioritized and becomes the JIPTL. The JIPTL is the basis for the weaponeering process that links weapons to targets.

JTL ***Joint Target List***

The JTL is the primary target list for supporting a particular operation. It represents the compendium of available targets for the achievement of strategic and operational effects that could be attacked in pursuit of the operational objectives.

LTIOV ***Latest Time Information Is of Value***

Multinational

In concert with both Alliance and non-Alliance forces.

NAI ***Named Area of Interest***

An area or point from which intelligence could confirm or deny the threat's intentions or limitations.

NSTL No-Strike Target List

A list of geographic areas, complexes, or installations not planned for capture or destruction. Attacking these may violate the laws of armed conflict, may interfere with or upset projected friendly military operations or interfere with friendly relations with indigenous personnel or governments. Additions to or deletions from the NSTL must be carefully controlled and coordinated by the targeting staff in order to minimize the possibility of fratricide and to maximize combat effectiveness.

Operational Level of Command

The level of war at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objectives within theatres or areas of operations. (AAP-6)

PIR

Commander's Priority Intelligence Requirements

Processing

The production of intelligence through collation, evaluation, analysis, integration and interpretation of information and/or other intelligence. (AAP-6)

RT ***Real-Time***

Restricted Targets

Restricted targets are a sub-set of the targets on the Joint Integrated Target List (JITL), which require special consideration, usually where simple destruction is not sought. This may be because of the particular sensitivity of the site, the need to deconflict any proposed action with other activities or because the site is assessed as having a significant intelligence value, the wish to use a unique weapon or the desire to exploit the target or because of post conflict reconstruction considerations. A proposal to attack a Restricted Target must be authorized through the JFHQ.

Strategic Level of Command

The level of war at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them (AAP-6)

Tactical Level of Command

The level of war at which battles and engagements are planned and executed to accomplish military objectives assigned to tactical formations and units. (AAP-6)

TAI ***Target Area of Interest***

An area where the commander can influence the battle by destroying, delaying or disrupting threat or targeted forces.

Unrestricted Targets

These are target sets, types or areas for which approval to engage has been delegated to the commander without further higher military or political approval. They remain subject to legal validation.

This Page Intentionally Blank

LIST OF ABBREVIATIONS

The following abbreviations are used in this publication.

ACINT	Acoustic Intelligence
AI	Area of Interest
AII	Area of Intelligence Interest
AIR	Area of Intelligence Responsibility
AIRINTSUM	Air Force Intelligence Summary
AJP	Allied Joint Publication
AO	Area of Operations
BDA	Battle Damage Assessment
Bi-SC	Bi-Strategic Command (that is, ACE and ACLANT)
C2	Command and Control
C2I	Command and Control and Information
C2W	Command and Control Warfare
C4I	Command, Control, Communications, Computers and Information
C4I2	Command, Control, Communications, Computers, Information and Intelligence
CCIR	Commander's Critical Information Requirements
CCIRM	Collection Co-ordination and Intelligence Requirements Management
CCTV	Closed Circuit Television
CF OPP	Canadian Forces Operational Planning Process
CI	Counter-Intelligence
CIMIC	Civil Military Co-operation
CIS	Communication and Information Systems
COA	Course of Action
CoG	Centres of Gravity
COMINT	Communications Intelligence
CONOPs	Concept of Operations
COP	Common Operational Picture
DL	Decision Line
DMP	Decision Making Process
DP	Decision Point
DSO	Decision Support Overlay
ELINT	Electronic Intelligence
EMS	Electromagnetic Spectrum
EW	Electronic Warfare
HPT	High Pay-off Target
HPTL	High Pay-off Target List
HUMINT	Human Intelligence

HUMINT	Human Intelligence
HVT	High Value Target
HVTL	High Value Target List
I&W	Indications and Warning
IMINT	Imagery Intelligence
IO	Information Operations
INFO OPS	Information Operations
INFOSEC	Information Security
INT	Intelligence
INTREP	Intelligence Report
INTSUM	Intelligence Summary
IPB	Intelligence Preparation of the Battlespace
IR	Intelligence Requirements
ISR	Intelligence Surveillance Reconnaissance
IT	Information Technology
JTFC	Joint Task Force Commander
LANDINTSUM	Land Force Intelligence Summary
MARINTSUM	Naval Intelligence Summary
MASINT	Measurement and Signature Intelligence
NAI	Named Area of Interest
NATO	North Atlantic treaty Organisation
NBC	Nuclear Biological and Chemical
NGO	Non-Governmental Organisation
NIC	National Intelligence Cell
NRT	Near Real-Time
OPLAN	Operation Plan
OPSEC	Operations Security
ORBAT	Order of Battle
OSINT	Open Source Intelligence
PIR	Priority Intelligence Requirements
PSO	Peace Support Operations
PSYOPS	Psychological Operations
PW	Prisoner of War
RADINT	Radar Intelligence
RFI	Request For Information
SA	Situational Awareness
SIGINT	Signals Intelligence
SOF	Special Operations Forces
SOP	Standing Operating Procedures

STANAG	Standardisation Agreement
SUPINTREP	Supplementary Intelligence Report
TA	Target Acquisition
TAI	Target Area of Interest
TECHINT	Technical Intelligence
UAV	Unmanned Aerial Vehicle

This Page Intentionally Blank

LIST OF REFERENCES

DND/CF

Asymmetric Threats and Weapons of Mass Destruction Study

Canadian Forces Command Decision Support Capability (CoDSC) Planning Guidance (DRAFT) (3 May 02)

Canadian Forces Common Operational Picture Concept of Operations (Revised Draft 11 Jul 02)

Canadian Forces Doctrine Development (A-AE-025-000/AJ-001)

Canadian Forces Information Operations (B-GG-005-004/AF-010)

Canadian Forces Joint Information & Intelligence Fusion Capability CONOPs

Canadian Forces Operational Planning Process (B-GJ-005-500/FP-000)

Canadian Forces Operations (B-GG-005-004/AF-000)

CFCS Framework CONOPs (15 Apr 02)

Civil-Military Cooperation In Peace, Emergencies, Crisis And War (B-GG-005-004/AF-023)

DCDS Direction for International Operations

Department of National Defence Plan (DNDP) 15, DND Emergency Book (also referred to as the "War Book")

Force Employment (B-GG-005-004/AF-004)

HUMINT Operations (1st Draft) (B-GL-357-002/FP-001)

Integrated Intelligence, Surveillance & Reconnaissance (ISR) Capability Planning Guidance

Intelligence Field Manual (B-GL-357-001/FP-001)

J Staff SOPs

NDHQ Instruction DCDS 2/98 Guidance for the Conduct of Domestic Operations (3310-0 (DCDS) dated 10 Jul 98)

Prisoners of War Handling, Detainees, Interrogation and Tactical Questioning (PWDITQ)

Risk management for CF Operations (B-GJ-005-502/FP-000)

The Law of Armed Conflict at the Operational and Tactical Level (B-GG-005-027/AF-021)

NATO

ACE Directive 65-7 (HUMINT)

Allied Joint Intelligence, Counter-Intelligence and Security Doctrine (AJP 2.0)[69]

Bi-SC FPG[70] Intelligence in Operational Planning (FPG Intel)

Bi-SC Reporting Directive Volume II – Intelligence Reports

Counter-Intelligence and Security Procedures (AJP 2.2)

Handling of Captured Personnel, Equipment and Documents (AJP 2.5)

Intelligence Procedures (AJP 2.1)

[69] AJP = Allied Joint Publication
[70] FPG = Functional Planning Guide

NATO Glossary of Terms and Definitions (AAP-6 (2002))

NATO Open Source Intelligence Handbook

NATO Precautionary System Manual

Recognized Maritime Picture (RMP) Manager Guide (EXTAC 619(B))

Request for Information (STANAG 2149)

AUSTRALIA

Intelligence (AFDP 19)[71]

UK

Joint Operational Intelligence (JWP 2-00)[72]

US

Doctrine for Intelligence Support to Joint Operations (Joint Pub 2-0)

Intelligence (MCDP 2)[73]

Joint Doctrine for Targeting (Joint Pub 3-60)

Joint Intelligence Support to Military Operations (Joint Pub 2-01)

Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations (Joint Pub 2-03)

Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace (Joint Publication 2-01.3)

National Intelligence Support to Joint Operations (Joint Pub 2-02)

Naval Intelligence (Naval Doctrine Publication 2)

[71] AFDP = Australian Defence Force Publication
[72] JWP = Joint Warfare Publication
[73] MCDP = Marine Corps Doctrine Publication

INDEX

“

“agencies” 2-15
“CF Operational Planning Process” 4-2
“command led” 1-1
“Comment” 2-12
“Defensive Information Operations,” 4-6, 5-5
“knowledge edge” 1-1
“Offensive Information Operations,” 4-6, 5-5
“one-stop shopping” 2-13
“process” 1-2
“pull” 3-8
“push” and “pull” 2-13, 5-6
“So What?” 2-11
“sources” 2-15
“stovepipes” 6-6
“The conclusion to be drawn from this is....” ... 2-12
“Truth cannot be judged” 2-11
“Usually reliable” 2-10, 2-11
“We believe this means that....” 2-12

2

24-hour support 6-6

A

ability to be reconfigured 3-3
adversary intentions 5-2
adversary’s likely intentions 4-10
Agent Handling 3-11
AIR 5-4
Alert or Warning Indicators 2-5
All Source Approach 5-9
amounts of information 1-2
analysing a force’s possible future intentions . 4-11
analysing current activities 4-10
Appropriateness 2-12
architecture of procedures 6-3
Area of Intelligence Interest (AII) 2-2
Area of Interest (AI) 2-2
Area of Operations (AO) 2-2
Areas of Intelligence Responsibility (AIR) 2-2
assessments 3-8
Assignment of appropriate movement 6-2

B

background intelligence 2-1
Balance of Collection Capability 5-8
Basic intelligence products 3-8
battlespace 1-2
Battlespace 4-1
battlespace awareness 5-3
battlespace’s effects 1-4
BDA 1-5
B-GG-005-004/AF-000 5-4
B-GG-005-004/AF-005 5-4
B-GJ-005-500/FP-000 4-2

C

C2W 4-1
C4I 5-5
categorisation 2-1
CCIR 2-5
CCIRM 3-5, 6-6
CCIRM concept 3-7
CCIRM staff 3-6
CDA 3-11
CDE 1-5
Centralized Control 2-3
Centralized Co-ordination 4-7
CF OPP 4-1, 5-3
CI 1-5
COA 1-4, 5-4
CoGs 5-4
Collation 2-8
collection assets 1-6
collection plan 3-6
Co-locating intelligence 3-1
Combat Intelligence Estimate 4-11
Command and Control of the ISR System 4-9
commander 1-1
commander’s determination 6-5
commander’s mission 4-10
commander’s PIR 3-5
Commander’s visualization 1-1
common data standard 3-3
Common encryption systems 3-3
common formats and terminology 3-3
Common Operational Picture 4-7
Common Standards/Interoperability 3-3
complete integration 6-4
component to support other units 6-4
comprehensive understanding 6-1
concepts and operating experience 6-1
conduct of operations 4-10
conduct of sophisticated IO 5-5
conduct of tactical operations 2-1
Conferences, briefings and planning groups 3-2
confirmatory information 3-6
connectivity 3-2
Contact Handling 3-11
Continuous Coverage 4-7
Continuous Review 2-3
COP 1-4
Counter-Intelligence Operations 3-11
country briefs 3-9
country handbook 3-9
CPS 3-11
Critical Information Requirements 1-6

D

databased intelligence 6-3
databases and publications..... 3-6
DCDS 5-7, 6-2
decreasing the risks 1-3
deduction of some sort..... 1-2
Deliberate Intelligence Estimate..... 4-11
Demography..... 5-3
Desirable Capabilities of an ISR System 4-7
Desired Order of Arrival Staff Table (DOAST).. 6-2
determining objectives 5-1
Direction is key to the efficient use of staffs..... 5-4
Dissemination Formats 2-13
dissemination of information 1-7
distribution lists..... 3-2
Documents and Equipment..... 3-12

E

Economy of Effort..... 4-7
effectively separating intelligence from its sources
..... 6-5
Electronic Warfare..... 5-8
employment of the whole force 5-1
Estimates..... 3-8
Estimative intelligence..... 2-2
Evaluating the adversary..... 1-4
existing databases and publications 3-6
Exploitation of Personnel 3-12

F

Flexibility..... 3-2
Force Protection..... 5-2
formation of policy and military plans..... 2-1
Fusion Centre..... 4-8

G

geographic areas 1-4
geographic characteristics 4-6
Geospatial Intelligence..... 5-8
great value..... 1-2
Guidance for specific intelligence support 5-5

H

Handling of Captured Personnel..... 3-12
harmonisation..... 3-8
hostile forces 1-3
HQ 3-1
HUMINT activities 3-10
hydrographic characteristics 4-6

I

I&W..... 3-8
I&W systems 1-4
Identification Indicators 2-5
Identify requirement 1-6
Identifying and Determining Objectives..... 5-1
IMS 5-1
Information Requirements..... 3-6

'

'intelligence' *1-1*

I

intelligence activities..... 3-1
intelligence architecture 1-6
intelligence cycle 5-3
Intelligence Estimate 4-9
intelligence failure..... 6-2
Intelligence operations must be synchronized .. 6-1
Intelligence Preparation of the Battlespace 4-1
Intelligence procedures 6-7
Intelligence Production..... 5-7
Intelligence Reports.....*2-13*, *3-9*
intelligence staff..... 3-1
Intelligence staff functions..... 3-1
intelligence staff practice..... 4-1
intelligence staff process..... 3-4
Intelligence staff's responsibilities..... 5-1
Intelligence support 5-5
intelligence theory 6-1
intentions 5-2
Interoperability..... 3-2
Interpretation 2-11
INTREP 3-9
INTSUM..... 3-10
IPB..... 3-4
IPB Intelligence Estimate 4-11
ISR..... 4-6
ISR Concept of Operations 4-8

J

J2 staff..... 6-2
J2/DG 5-7
joint intelligence..... 3-1
Joint intelligence architecture..... 5-6
Joint Operations Area (JOA). 6-1
JTFC..... 6-1
JTFCs' 5-4
JTFHQ..... 5-8

K

Karl von Clausewitz..... 1-1

L

Limits of Collection 5-9
logistic support 5-7
LTIOV 3-7

M

management of the intelligence process..... 2-1
Managing the intelligence requirements 3-5

MASINT 4-8
mental process 2-11
meteorological characteristics 4-6
Military capabilities assessments and studies ... 3-8
Military Intelligence Reconnaissance 3-11
missions and objectives are contemplated 6-3
multinational force intelligence 1-7

N

national/international protocols 6-4
NATO *Bi-SC Reporting Directive Volume 2* *3-9*
NATO's *Bi-SC Reporting Directive Volume 2* . *2-13*
NDCC 2 5-7
NDHQ J2 staff 6-2
negotiate authorized skip-echelon 6-6
NICs 3-4

O

Objectivity 2-3
operability 6-1
operational architecture 5-6
operational intelligence 6-3
operations conducted by intelligence personnel 3-1
OPSEC 1-6
ORBAT 5-7
Overlapping coverage 6-7

P

packaging, preparation and deployment of the force 5-3
Passage of Information 4-7
phases of the cycle 5-3
PIR 1-6, 2-5
Planning and Conducting Operations 5-2
policy for the operation of the intelligence process 4-1
prediction of his adversary's likely tactics 1-3
pre-emptive 1-2
preventive 1-2
Primacy 3-2
Principles of Verbal Dissemination 2-14
Prisoner of War Handling 3-12
procedural guidelines for intelligence 5-1
process 1-2
production, or dissemination 5-6
protection of the information 6-5
Provide answers to requirements 3-7
Public Affairs (PA) 5-5
pull concept 5-6
push and pull control principles 2-13

R

reconnaissance 1-5
Reports and summaries 3-8
requirement 1-6
Requirement for Liaison 3-2
Responsiveness 2-3
risks 1-3
Robustness 4-7

S

seamless provision of joint intelligence 5-4
Sensor Management Cell 4-8
Sharing is the responsibility of commands 6-4
shortfalls in collection capacity 1-6
Signals Intelligence 5-8
Signals Intelligence (SIGINT), ... 6-2
single item of data 1-2
single point of failure 5-6
situation of the adversary 4-10
Situational Awareness 4-6
sound judgement 6-1
source protection 6-4
Special Operations Forces 4-8
specialist collection agencies 3-1
Staff Coordination 3-1
staff officers 3-1
state in any operation 5-5
subordinate commands 5-1
SUPINTREP 3-10
systematic approach 6-7
Systematic Exploitation 2-3

T

Table of Organization and Equipment 5-7
Tactical CI 3-11
Tactical or Combat Indicators 2-5
Tactical Questioning 3-11
Target System Analysis 1-5
Targeting Cell 4-9
Targeting intelligence 1-4
tasking of organic and attached sources 2-4
The Adversary 5-2
the production of intelligence 2-8
Threat and risk products 3-8
timely provision 3-7
TPED 4-7
training 1-6

U

ultimate end-state in any operation 5-5
Understanding adversary intentions 5-2
understanding of the adversary 5-2
understanding of the capabilities 1-2
understanding of the physical 1-1
Use of Force in CF Operations 5-4

V

Validate and prioritise the requests 3-7
value of the majority of information 2-7
visualisation of the adversary 1-5
vulnerabilities 1-1

W

Warning intelligence 2-2
Weapons Recognition Guide 3-9
Weather and terrain 4-10
Wringing the Facts Dry 2-11