"Optimizing Coalition Interoperability"
www.abca-armies.org

COALITION INTELLIGENCE HANDBOOK

ABCA Publication 325
Edition 5

2013

Conditions of Release:

The information contained in this document is releasable only to ABCA nations. It may only be disclosed outside of ABCA Nations with the authorization of the ABCA Armies.

The information belongs exclusively to the ABCA Armies' Program. No material or information contained in this document should be reproduced, stored in an information system(s) or transmitted in any form outside of ABCA nations except as authorized by the ABCA Program.

AMENDMENTS

Amendment No	Date	Details

PREFACE

The Coalition Intelligence Handbook (CIH) is designed to provide commanders and staff on ABCA or wider-based coalition operations with guidelines on the roles, principles and tasks of intelligence, the Intelligence Architecture, intelligence support to operations, targeting, information operations and force protection, and intelligence, surveillance and reconnaissance (ISR). The CIH should be used in conjunction with the ABCA Coalition Operations Handbook (COH), ABCA Publication 332.

Timely and accurate intelligence underpins every aspect of planning and executing operations. Intelligence staff play a key role in providing commander's and their staff with situational awareness on the threat, in particular threat intentions, and the operational environment (OE). Intelligence assessments must be predictive to give commanders the opportunity to accelerate their decision-making and to exploit an adversary's vulnerabilities in order to achieve the desired end state.

CONTENTS

INTRODUCTION

Releasability

1. Although this publication is unclassified it is not to be released outside ABCA nations.

Aim

2. The aim of the Coalition Intelligence Handbook (CIH) is to provide a guide to the planning and conduct of intelligence support in an ABCA coalition. The target audience is ABCA commanders and staff.

Scope

3. The CIH provides ABCA nations with information and guidance on the planning and conduct of intelligence activities in support of the full spectrum of coalition operations. The CIH may also be used for ABCA led operations involving a wider coalition of nations. This product is not designed as a detailed guide for intelligence analysts or to be used as tactics techniques and procedures (TTPs). This edition (Edition 5) includes new chapters on biometrics, human terrain and electronic warfare.

Interoperability

4. Each nation brings its own view and methods of operations. To produce an effective coalition intelligence architecture a high level of interoperability is required. Interoperability may be broken down into two distinct areas, technical and procedural. Technical interoperability is achieved by having systems used to process information and disseminate intelligence within a communications network. Procedural interoperability is achieved through processes and procedures that are the same, similar or, if different, sufficiently understood by each nation to ensure interoperability is still possible. As a minimum, interoperability must cover communications and information systems (CIS), intelligence data and products, terminology and symbols, standards, training, archives and databases.

Terminology

5. This handbook uses terms in accordance with AAP-6 NATO Glossary of Terms and Definitions as well as terminology from ABCA nations. For clarity a CIH glossary that identifies differences in nations' terminology is included. Specific areas of consideration are as follows:

a. **Intelligence, surveillance and reconnaissance (ISR)/intelligence surveillance target acquisition and reconnaissance (ISTAR).** While this is an intelligence handbook, many of the issues it deals with have relevance to the developing wider ISTAR context.

(1) ISR is executed though the operations and intelligence processes (with an emphasis on intelligence analysis and leveraging the larger intelligence enterprise) and information collection. Consent with national doctrine, ISR an

activity that synchronizes and integrates the planning and operation of sensors, assets, processing, exploitation and dissemination systems in direct support of current operations. This is an integrated intelligence operations function.

(2) ISTAR has been defined as the coupling of the ISR process and tactical level targeting processes by a defined military force in an assigned area of operations or area of interest. ISTAR integrates battlefield collection capabilities to target the unknown, synthesize information fragments, corroborate the known, disseminate information and enable the commander's decision making process.

b. Nations use variations on terminology relating to intelligence preparation of the battlefield or battlespace (IPB), intelligence preparation of the environment (IPE) or intelligence preparation of the operational environment (IPOE). For the purposes of the CIH, the term IPB is used throughout.

c. **Land component headquarters (HQ).** It is accepted the CIH will be used to support ABCA work in the creation of the 2 Star HQ as the land component. Given intelligence staff in this organization are supported by other operational domains (maritime, air and space), the generic term of coalition joint 2 (CJ2) will be used throughout.

Supporting ABCA Documents

6. The CIH is supported by the following ABCA handbooks and planning guides:

a. Coalition Operations Handbook (COH) - ABCA Publication 332;

b. Coalition Health Interoperability Handbook (CHIH) – ABCA Publication 256; and

c. Coalition Logistics Handbook (CLH) – ABCA Publication 323.

CHAPTER 1

ABCA INTELLIGENCE ARCHITECTURE

1-1. **The Coalition Intelligence Architecture – an overview.** The ABCA Coalition Intelligence Architecture will consist of the personnel, organizations, policy and procedures, information technology (IT) and communications and other means of dissemination to effect the complete execution of the intelligence cycle and other processes.

1-2. **General.** The Architecture should allow the free flow of information to its constituent elements, the ability to pass requests for information (RFI) and the ability to task as well as control the collection assets. The Architecture should permit this within national chains of command as well as between coalition partners. Establishing a coherent intelligence architecture is vital and must be a primary requirement of the overall campaign planning process. This chapter will provide the guiding principles for the building of a coalition intelligence architecture.

1-3. **Key principles.** A coalition intelligence architecture must be based on the following key principles:

a. enabling the commander to drive the intelligence effort;

b. ensuring intelligence staffs can manage collection and analysis at all levels;

c. supporting co-ordinated collection, requirements management, processing and dissemination at all levels of command;

d. the allocation of task orientated collection assets based on the operational environment (OE);

e. enabling the exchange of information between intelligence cells and databases;

f. ensuring the timely dissemination of intelligence to all users including the responsibility to share across nations; and

g. supporting the passage of appropriate national intelligence.

1-4. **Lead nation.** The lead nation will establish the parameters and procedures for the deployment and employment of declared national intelligence, surveillance and reconnaissance **(**ISR) assets in-theater, as well as the basic CJ2/ISR structure and processes.

1-5. **Intelligence exchange agreements.** Comprehensive intelligence exchange agreements already exist between ABCA nations. These agreements mostly apply at the strategic and operational levels but certain measures will apply at the tactical level. These agreements provide the basis for defining the constraints on the Coalition Intelligence Architecture for each operation. Nations are likely to deploy with their own national intelligence architecture. Such architectures provide direct support to the deployed forces of

the individual nations. The level of integration between nations will be dependent on the coalition contributing nations.

1-6. **Communications and information systems (CIS).** Intelligence processes depend on robust CIS built around common standards. CIS will assist with the transmission of tasking and requests, the transfer of information from sources and agencies, the processing of information into intelligence and the dissemination of the resultant product in a readily accessible and understandable form.

Building the Architecture

1-7. When building an intelligence architecture the commander may want to consider the following:

a. **Architecture relationships.** The effectiveness of the Architecture is based upon the relationships between the functional elements. The nature of intelligence is such that no architecture can permit complete freedom of action for control, tasking, requests and access. Where the Architecture is multi-national, constraints may apply. It is the responsibility of the CJ2 and CJ6 staff to produce an intelligence management plan (IMP) that defines these relationships and systems architectures.

b. **Access and dissemination.** Access is the function of drawing on available information and intelligence. Dissemination is the passage of primarily time critical information and intelligence. Access should be provided to information and intelligence wherever it is held within the Architecture both internally and externally to the ABCA nations, whilst dissemination should happen as a matter of course. Within an ABCA operation there should be minimal barriers to the ability of any nation to access information and intelligence wherever it is held, or to disseminate it to whomever needs it. Within a wider coalition operation, dynamic controls will be put in place to ensure coalition releasable information and intelligence can be freely accessed and disseminated. Further compartmentalization will be put in place to control access to ABCA and national only information and intelligence.

c. **Releasability.** Where possible staff should write for release and be aware of the requirement to share. Tearlines[1] are used to produce multiple classifications of the same intelligence report in order to facilitate sharing to as many coalition partners as possible, including the host nation (HN).

d. **Task.** Within an ABCA Coalition Intelligence Architecture, tasking of other nations' declared collection assets will be possible within the constraints previously agreed. Tasking of collection assets that have not been nationally declared is also possible at the discretion of the owning nation.

e. **Control.** Control implies there is a formal relationship between a headquarters (HQ) and collection assets. Such control will normally be defined in terms of command

[1] See Annex A to Chapter 7 of this handbook for explanation/information on Tearlines

relationships. Control of intelligence assets may include the ability to deploy and re-deploy assets within the area of operations based on an operational need.

National intelligence architecture

1-8. Individual nations may deploy with their own intelligence capabilities that will still function within the wider coalition intelligence effort. Two particular elements of a nation's own intelligence capability may be placed within the Coalition Intelligence Architecture, these are:

a. **National intelligence cells (NICs).** NIC may be provided for coalition operations. NICs provide a national strategic intelligence feed into the operation. The deployment of NICs is a national responsibility; although planning must take into account their support and CIS requirements. They may be attached to the coalition joint HQ and be located inside the ABCA Coalition Intelligence Fusion Center (ABCA CIFC) of the land component HQ.

b. **Declared national collection capabilities.** In certain circumstances nations may provide individual collection capabilities for use by the land component HQ or that can be tasked by other coalition nations. These are termed national declared collection capabilities. If allocated to the land component HQ, such capabilities would be considered to be controlled by that HQ, otherwise they will continue to be controlled by the owning nation. These declared capabilities will always include a command element that has a power of veto (defined by the owning nation) over tasking. This is a national control measure to ensure a collection asset is used in a manner that is appropriate for the operation and the posture of the owning nation within the coalition.

1-9. **Intelligence staff elements of a land component HQ.** The way the intelligence staff elements are organized within a land component HQ will vary according to the national doctrine of the lead nation. The lead nation will normally use its own staff cells as the basis for the coalition CJ2/ISR staff. It will adapt its own cell architecture to a degree to accommodate the requirements of other coalition partners. Coalition partners will not provide discrete cells (other than NICs) within the CJ2/ISR staff elements; rather they will provide individual specialists who will be placed within the CJ2/ISR staff framework of the lead nation. Wherever possible, the CJ2/ISR staff elements should be located as an integral element of, or adjacent to the main command post.

1-10. Support to the commander is the most important consideration in positioning the intelligence cells. The Plans and All Source Analysis cells must be located so they are directly accessible to the commander. Physical location of all elements will be influenced by access to primary and alternate communication links for sensors, data and command and control (C2), access to electrical power and site security, although all of these must be weighed against the need to ensure rapid dissemination of key information to the tactical decision makers. As a general guideline the following functions need to be considered in a generic structure.

a. **The CJ2 Coordination.** The role of CJ2 Coordination is to ensure relevant commander's critical information requirements (CCIR) are processed, the information required is either retrieved or collected, the various ISR collection capabilities are used to best effect, and the product is turned into timely intelligence. It functions as the provider of intimate support to the commander, interpreting his requirements and working to provide information to the level of detail necessary to direct, plan and co-ordinate the ISR capability as a whole.

b. **CJ2 Plans.** Prepares the Intelligence Collection Plan (ICP) and the outline ISR Plan. This provides the detailed direction to ISR, in close conjunction with the CJ3 staff. CJ2 Plans is always looking beyond the requirements for current intelligence and therefore looking at intelligence requirements in line with the battle rhythm of the HQ. There is a close linkage with the CJ3/5 plans staff, especially in developing the IPB.

c. **ISR Collection Management.** ISR collection management executes the ICP. It ensures information requirements (IRs) are being recorded and processed and notes when they have been satisfied and can be removed from the plan.

d. **ISR Co-ordination.** Is responsible for the co-ordination of declared national collection capabilities, including co-ordination with assets at differing levels of command. ISR co-ordination receives direction from the CJ3 staff, but is also closely linked with the CJ2 and other branches to support maneuver, information operations, or effects. As the focus for ISR collection co-ordination, it would also include specialist staff from the various collection capabilities allocated. This could be manned by CJ2 staff, or it may be a CJ3 staff function depending on which ABCA nation is providing personnel.

e. **The All Source Cell (ASC).** The ASC processes collected information into intelligence and disseminates the resultant intelligence product to users. Its primary product, all-source intelligence, is critical to successful combat operations of the combined force. The ASC provides a dynamic, focused view of the battlefield in near real time, assisting commanders to deploy combat support assets and maneuver forces around the battlefield in a timely manner. The ASC simultaneously supports current missions and future contingencies. Typical tasks would include development and maintenance of intelligence databases, production and dissemination of intelligence reports, predictive assessments, targeting support, battle damage assessment (BDA) and interfacing with other analytical elements to exchange information and intelligence, to reconcile processing efforts and to resolve discrepancies. Close and continuous interface between intelligence producers is vital to the intelligence production effort.

1-11. **The ABCA Coalition Intelligence Fusion Center (CIFC).** The ABCA CIFC is a '5 EYES' organization within a land component HQ. It is designed to fuse, integrate and disseminate information and intelligence derived from multiple sources including subordinate formations and national strategic systems from more than one nation. In general terms the ABCA CIFC will draw on information and intelligence, classified at '5 EYES' or below, from the individual ABCA nations' ASCs and NICs conducting further work to refine and then

disseminate intelligence product. Tearlines will be issued from the ABCA CIFC where possible to ensure the timely release of intelligence material to the HN and non-ABCA coalition partners.

Summary

1-12. The establishment of an effective intelligence architecture for a coalition force is vital for effective conduct of an operation. The proposed generic Coalition Intelligence Architecture meets the need of any coalition force and defines the essential links required between each element of that architecture. It fits with the preferred force structure option of a lead nation. Likewise the staff elements outlined, internal to a land component HQ, cross-refer to those of each of the ABCA nations. This approach is generic enough to fit within any potential land component force structure.

CHAPTER 2

INTELLIGENCE THEORY AND CONCEPTS

Introduction

2-1. The organization, activities and production of intelligence are optimized by several guiding principles. Fundamental to these principles is the fullest possible understanding of the stakeholders. This includes knowledge of their goals, objectives, strategy, intentions, capabilities, methods of operation, vulnerabilities and sense of value and loss. The intelligence staff must also understand the stakeholder's character, culture and customs. They must develop and continuously refine their ability to understand the stakeholders in order to advise on likely perceptions, reactions and responses to friendly actions.

Role

2-2. The role of intelligence is to provide the commander with greater understanding about the enemy, weather and environment in order to support decision making. In order to achieve this there must be continual and timely direction from the commander to adjust and prioritize intelligence efforts.

Principles

2-3. While procedures and terminology may differ between coalition nations the following general principles of intelligence should be applied:

a. **Centralized control.** Intelligence must be centrally controlled and coordinated to avoid duplication of effort and gaps in collection, provide mutual support, ensure security of sources, ensure efficient and effective use of limited resources in accordance with the commander's priorities and ensure the effective provision of technical direction to intelligence staffs and agencies.

b. **Responsiveness.** Intelligence must be responsive to the needs of commanders, their staffs and the chain of command. Support to the commander must be anticipatory and precise. Intelligence organizations must also be capable of responding rapidly and flexibly to changes in the operational situation or environment and redirecting collection effort accordingly.

c. **Planning.** Sources and agencies (SANDA) must be systematically exploited by methodical planning, based on a thorough knowledge of their capabilities, limitations and operational constraints.

d. **All-source approach.** The most useful and complete assessments usually emerge by fusing data from multiple sources. To avoid being deceived by analytical errors or adversary deception, all-source techniques that permit the development of corroborating data should be used. An all-source approach develops complementary

data where information from one source confirms and augments information provided by another. This provides a higher level of confidence in the intelligence product.

e. **Intelligence support to the comprehensive approach.** In the contemporary operating environment information must be made available, not only to support the military line of operation, but other agencies governmental and non-governmental to achieve their objectives on the other lines of operation.

f. **Continuous review.** Intelligence products, including factual data, conclusions and forecasts, must be continuously reviewed, and where necessary revised, taking into account all new information and comparing it with what is already known.

g. **Timeliness.** Information or intelligence must be available in a timely fashion so as to gain maximum benefit from its use.

h. **Objectivity.** Any temptation to distort information to fit previous assessments or preconceived ideas must be resisted. The temptation to tell commanders what they want to hear must also be avoided. Intelligence must convey the uncertainties inevitable in assessments and not imply a false degree of confidence.

i. **Accessibility.** Information and intelligence must be readily accessible, both for users, since the best intelligence is useless if it is not available, and for intelligence staff, since the essence of intelligence processing - the conversion of new information into intelligence - is comparison. Information and intelligence must be stored in a form that allows rapid and flexible response to queries.

j. **Responsibility to share.** Intelligence must be produced with a focus on the responsibility to share within a coalition environment in order to allow maximum exploitation.

k. **Source protection.** In collecting information, sources must not be employed on tasks where their loss would be disproportionate to the value of the information they provide or are seeking to collect. Similarly, in disseminating intelligence, sources and methods must be protected to avoid compromise and subsequent loss of collection ability.

l. **Balance**. The structure and activities of intelligence staffs must be balanced. The key elements are:

(1) An appropriate balance must be struck between the requirement to protect sources, while at the same time ensuring the widest possible dissemination of intelligence. In essence, this involves a command decision on the balance between the protection of the source and the satisfaction of users' intelligence requirements (IR).

(2) A balance must be struck between collection and production activities and between the effort devoted to the various types of intelligence, such as

basic intelligence (including database maintenance), current intelligence and estimative assessments.

(3) A balance must be struck and clear distinction made between fact and judgment (assessment) in intelligence reporting.

(4) Intelligence production agencies must strike a balance between the competing demands of customers who will range from national level decision-makers through strategic level commanders to operational and tactical level commanders.

m. **User awareness and confidence.** Intelligence organizations and staff need to liaise closely with users in order to ensure user requirements are clearly understood and met in a timely and preferred manner. Key elements are:

(1) Ensuring a high degree of confidence that requirements are being met. Not only in terms of the finished product provided to the user, but also in terms of collection requirements being satisfied and intelligence databases being maintained to support the intelligence capability.

(2) Ensuring there is a general awareness of the intelligence process and the broad capabilities and limitations of intelligence SANDA.

n. **Continuous improvement.** Intelligence organizations and staffs must continuously review procedures, processes and practices to ensure changes in the operational environment technology and customer requirements are accommodated.

2-4. **Characteristics of effective intelligence.** Effective intelligence is intelligence that meets the commander's needs. In order to achieve this, intelligence products must have the following characteristics:

a. **Relevance.** Intelligence must support the commander's mission, concept of operations, and IR.

b. **Usability.** Intelligence products must be in a format that can be easily used and they must highlight the significance of the information or intelligence they contain.

c. **Timeliness.** Intelligence products must be available in sufficient time to enable decisions to be made and executed.

d. **Accuracy.** Intelligence must be factually correct and indicate the degree of confidence in intelligence assessments and judgments.

e. **Objectivity.** Intelligence must be unbiased, undistorted and free from political influence or constraints. Intelligence methodology and products must not be directed or manipulated to conform to a desired result, preconceptions of a situation or adversary, predetermined objective or institutional position.

f. **Availability.** Intelligence must be readily available to those who need it.

g. **Completeness.** Intelligence should be as complete as possible, using all available information to answer customers' requirements and provide a full understanding of the situation.

h. **Clarity.** Intelligence should be clearly presented to avoid the chance of misinterpretation by the user.

The Intelligence Cycle

2-5. The Intelligence Cycle is a planned, methodical and logical process through which information is collected, converted to intelligence and disseminated to users. This is a continuous process and is applied at all levels. The Intelligence Cycle is depicted at Figure 2-1 and involves four phases of activity: direction, collection, processing and dissemination.

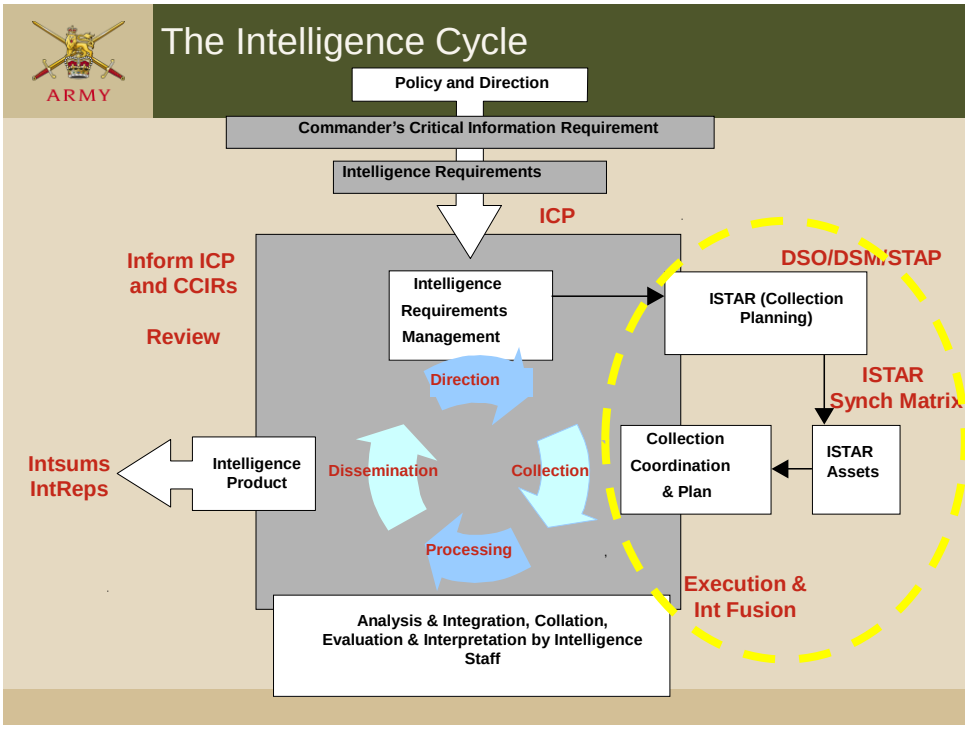

Figure 2-1: The Intelligence Cycle

2-6. The purpose of using a theoretical model of the intelligence cycle is to aid understanding of the logic of the process and introduce the varied activities that contribute to intelligence production. In practice, the Intelligence Cycle is applied throughout the intelligence staff process. When applied at the tactical level in support of operations planning, the intelligence staff process is known as intelligence preparation and monitoring of the battlespace (IPMB).

2-7. **Simultaneous nature of the process**. The model is cyclic in nature, since intelligence requires constant review and updating if it is to remain current and relevant to the commander's needs. This cycle of direction, collection, processing and dissemination is presented sequentially, simply to illustrate the logical flow of the process. The process is a continuous one however, and all phases occur concurrently. Viewed simply, the Intelligence Cycle is constantly in motion.

2-8. The four phases of the Intelligence Cycle: Direction, Collection, Processing and Dissemination will be covered in Chapters 4-7 inclusive.

Relationships between intelligence and other staff

2-9. The key relationships for the intelligence staff are with the commander and the plans and operations staff.

a. **Relationship with the commander.** The intelligence function exists to support the commander, who drives the process by providing guidance. The intelligence officer is one of the principal staff officers on a HQ and must gain and maintain the commander's confidence by providing effective intelligence.

b. **Relationship with plans and operations staff.** The relationship between the intelligence and plans and operations staff is symbiotic. Intelligence staffs need to understand both current and planned operations in order to anticipate IR and to focus their efforts. Similarly, operations staffs rely on intelligence staff to provide the knowledge of the threat and the environment required for the planning and conduct of operations. Co-location of operations, plans and intelligence staff is vital.

2-10. Intelligence staffs have relationships with the other staff elements as follows:

a. **Relationship with combat service support (CSS) staff**. Intelligence support for CSS includes the provision of basic intelligence on the area of operations (AO) and the conduct of counter-intelligence (CI) activities in the rear area in support of force protection and rear area security. CSS staff advice may be required when the threat's logistics capability is being assessed (in the production of logistics intelligence).

b. **Relationship with offensive support staff.** All forms of offensive action including maneuver, fire planning, close air support, electronic attack and psychological operations (PSYOPS) must be synchronized within the HQ. During IPB, the intelligence staff assesses the adversary's course of action (COA), vulnerabilities, center of gravity (COG), and provides advice on the decisive time and place for the possible engagement of the threat's high value targets (HVT). These assessments are confirmed during wargaming.

c. **Relationship with artillery intelligence staff.** Artillery intelligence results from the collection and processing of all available information on adversary indirect fire systems. Artillery staffs with a surveillance and target acquisition (STA) role, including intelligence, are usually part of the offensive support cell at task force (TF) level and above. The STA staffs are the principal advisers to the intelligence staff on the

adversary's artillery assets and provide the interface between the offensive support cell and the ASC. As part of this interface, the STA officer is usually located in the ASC to allow the rapid engagement of identified targets.

d. **Relationship with engineer intelligence staff.** Engineer intelligence provides information and assessments of terrain, the effects of weather on terrain and adversary engineer capabilities including mobility, counter-mobility and survivability. Hence, engineer staffs support the terrain analysis aspects of the operational environment (OE), and efforts should not be duplicated between engineering and intelligence staffs. At planning or orders groups, the engineer's brief should detail specific aspects of terrain critical to operations. At TF level and above, an engineer intelligence liaison officer (LO) will normally be appointed and acts as the principal engineer adviser to the intelligence staff.

e. **Relationship with military police staff.** Military police are tasked to conduct forensically sound examinations of locations, vehicles and personnel in order to capture information as part of criminal investigations; this may be passed to intelligence staff for further analysis. When intelligence exploitation activity is likely to be used to support the criminal justice process, military police have an important role in ensuring sound chain of custody, evidential handling and forensic processes.

CHAPTER 3

INTELLIGENCE SUPPORT TO OPERATIONAL PLANNING

3-1. **Context.** The operational planning process (OPP), intelligence preparation of the battlefield (IPB) and collection management are the three primary staff processes involved in the provision of intelligence support to operations. Whilst intelligence support is provided to other staff processes, these processes represent the major interactions between Intelligence and operations staff on any headquarters (HQ).

3-2. The OPP is a doctrinal approach to decision making that allows a situation to be examined and a logical decision reached. It promotes flexible, proactive planning regardless of the type of operation. The OPP consists of four consecutive steps:

a. step one – mission analysis;

b. step two – course of action (COA) development;

c. step three – COA analysis; and

d. step four – decision and execution.

3-3. The OPP is supported by a dynamic IPB which is closely connected to the individual stages of this decision making process. IPB is a continuous and systematic process of analyzing the threat with the existing weather conditions within a specific geographic environment. The results of the IPB process are represented graphically in a series of overlays and consist of four distinct steps:

a. step one – define the battlefield environment;

b. step two – describe the battlefield's effects;

c. step three – evaluate the threat; and

d. step four – determine threat courses of action.

3-4. The IPB process provides an invaluable aid to planning and, through the decision support matrix, provides a clear link to the operations process.

3-5. Although a discreet intelligence process, collection management runs in parallel to OPP and IPB and is an essential component of intelligence, surveillance and reconnaissance (ISR).

Operational planning process

Step 1 – mission analysis

3-6. **Commander's guidance.** During mission analysis, the commander should confirm or modify any assumptions that have been made, whilst noting the effects of the environment on the development of threat and possible friendly courses of action. At this stage of the OPP, the commander should also confirm or modify priority intelligence requirements (PIR) and (if required) modify the threat COA, prioritizing the threat courses of action the intelligence staff is to develop further.

3-7. **Operations staff action.** Operations staff will conduct an appreciation of time, space and troops to task; identify the mission and determine the senior commander's intent; identify specified, implied and essential tasks; and determine the degree of freedom of action available to them. Additionally, they should consolidate IPB and mission analysis, which should identify decisive events.

3-8. **Intelligence staff action.** IPB should be commenced as soon as possible, preferably well before the commencement of the OPP so formation staff can initiate planning with best possible level of situational awareness. Similarly, the intelligence surveillance and reconnaissance (ISR) plan needs to be developed early in order to identify and answer the commander's critical information requirements (CCIR), PIR and requests for information (RFI) during staff planning.

3-9. During mission analysis, key intelligence gaps and PIR are identified and included within the ISR plan. In many cases, the collection manager has already requested or tasked relevant agencies (generally higher level sources) to answer the CCIR. During this step intelligence staff provide input to the following:

a. a review of the situation, including the known or assessed threat mission, dispositions and intent;

b. assumptions made during the IPB process;

c. describing the significant characteristics of the environment;

d. a summation of threat COA using individual situation overlays, including recommendation of the most likely and most dangerous COA;

e. listing recommended PIR and high value targets; and

f. responses to any CCIR and information requirements (IR).

Step 2 – course of action development

3-10. During COA development, key staff will develop and refine the identification and placement of named areas of interest (NAI) and target areas of interest (TAI) pertinent for each COA. PIR associated with each COA of action are also listed and linked to the

appropriate NAI and/or TAI. The linkage of these outputs from the OPP and IPB is key to the effective functioning of the ISR plan.

3-11. **Commander's guidance.** The commander initially articulates what he believes to be appropriate courses of action for the given situation. This provides the operations staff with sufficient direction to further investigate likely courses of action.

3-12. **Operations staff action.** Operations staff create, test and develop these courses of action based on the commander's guidance at the completion of mission analysis.

3-13. **Intelligence staff action.** During COA development, intelligence staff provide input to the following:

a. a review of the situation and environmental characteristics, concentrating on those aspects that have changed since mission analysis;

b. a detailed description of each threat COA, in priority order, using an event overlay; and

c. an update of any responses to the CCIR and IR.

Step 3 – course of action analysis

3-14. During COA analysis (wargaming), the collection manager (or an appropriate representative) will note the key outcomes that impinge upon, or highlight critical aspects to the execution of the ISR Plan. It is during this phase of staff planning the key elements of the ISR Plan are updated and confirmed for each friendly COA. That is, confirmed PIR are appropriately linked with relevant NAI and TAI and in turn, the appropriate sensor platforms are identified to effectively carry out the tasks outlined within the ISR Plan.

3-15. **Commander's guidance.** As a result of wargaming, PIR, NAI, TAI, and significant branches and sequels to the threat and friendly COA are confirmed. From an ISR viewpoint, wargaming provides a modified event overlay that is the basis of the ISR Plan.

3-16. **Operations staff action.** Operations staff participate in the war game by 'playing' the friendly force for each COA along with their associated branches and sequels. COA modifications, battlefield operating systems and threat templates are subsequently refined and modified as appropriate.

3-17. **Intelligence staff action.** Wargaming is key to this phase of the OPP. Intelligence staff play the part of the threat commander. Within this staff, a key member (usually the collection manager or the commander of any attached surveillance and reconnaissance asset) plays the parts of those specialized collection assets. Intelligence staff must realistically represent threat actions and reactions to friendly operations regardless of what friendly forces would prefer the threat to do. This will reveal any weaknesses friendly courses of action may have. Intelligence staff input to this stage of the OPP typically includes:

a. a review of the situation and environmental characteristics, concentrating on those aspects that have changed since the COA development;

b. a detailed description of each threat COA, in priority order, using the modified event overlay (if required);

c. the significant threat actions and reactions considered for each friendly COA war gamed; and

d. an update of any responses to the CCIR and IR.

Step 4 – decision and execution

3-18. At the decision and execution phase, the ISR Plan is usually included as an annex to the Operations Order. It should be noted the ISR Plan is a dynamic product. Consequently, the detail within this document will continue to evolve once the operation commences. It is also common for the ISR Plan to be depicted graphically and briefed to key unit commanders (or their representatives) by formation staff.

3-19. **Commander's guidance.** The commander should finalize or modify PIR and essential elements of friendly information to allow intelligence, including collection management, and counter-intelligence staff work to be completed. Following a decision on which friendly COA is to be executed, surveillance planning groups and targeting boards are convened and the operations order is written and briefed to unit commanders.

3-20. **Operations staff action.** Operations staff will compare the strengths and weaknesses of each COA and brief the commander of their analysis in order for the commander to determine which COA is to be developed and implemented. During this stage, operations staff complete decision support overlays (DSO) and synchronization matrices for each COA.

3-21. Intelligence staff action:

a. a review of the situation and environmental characteristics, concentrating on those aspects that have changed since COA analysis;

b. a detailed description of the updated threat COA, in priority order, using a modified event overlay (if required);

c. finalizing/updating the ISR Plans for each friendly COA prior to their ratification by the commander; and

d. an update of any responses to the CCIR and IR.

Intelligence preparation of the battlefield

3-22. IPB commences on the receipt of orders, change in the enemy situation or a shift in the operational posture. If time permits, all aspects of the IPB process should be completed

prior to commencement of the OPP in order to allow for optimal intelligence input and for the initial IR to be determined.

3-23. While the process will remain the same, IPB will conducted with different emphasis and priorities in line with the situation and where on the spectrum of conflict the commander believes he is engaged. The examples presented are not exhaustive and do not represent the full range of possible outputs.

3-24 IPB is a systematic, process for analyzing the adversarial, non-participant and stakeholder environments, considered in the dimensions of space and time. When conducting an IPB assessments should be considered across the physical, human and informational domains.

3-25. The IPB is designed to support staff planning and prepare the foundations for informed military decision making. IPB is a processing medium through which intelligence staff provide an assessment of environmental effects on operations and an estimate of all stakeholders (and in particular adversary) capability and intent.

3-26. IPB incorporates all intelligence product development and interpretation directed to support planning. Additionally, IPB interaction with the OPP creates the commander's IR, which drive collection, processing and dissemination within an operational context.

3-27. IPB helps the commander apply maximum combat power (whether this be kinetic or non-kinetic) at decisive points in space and time by describing:

a. the operating environment (human, physical and informational) and the effects of that environment on both friendly and adversary operations;

b. the adversary's likely COA, including adversary intelligence collection activities, the adversary's center of gravity and the adversary's critical vulnerabilities (CV);

c. other stakeholders likely COA, including intelligence collection activities, their center of gravity and critical vulnerabilities; and

d. managing collection to meet the commander's decision requirements relative to gaps in knowledge or the triggering of the commander's decision points.

3-28. Outputs and inputs. IPB outputs constitute the intelligence inputs and include:

a. Assessment of the operational environment.

b. **Intelligence estimate.** The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the COA open to the enemy or potential enemy and the order of probability of their adoption.

CHAPTER 4

DIRECTION

Introduction

4-1. The first and most important step of any intelligence support is clear direction from the commander. Commander's use the operational planning process (OPP) to continuously design and conduct operations. The commander cannot successfully accomplish the activities involved in the operations process without information and intelligence. The design and structure of intelligence operations support the commander's OPP by providing him with intelligence regarding the enemy, the area or operation (AO) and the situation. This is a continuously developing process and this direction needs to be regularly reviewed throughout the intelligence process.

4-2. Direction will also be received from higher level headquarters (HQs)/national chains and this will affect the intelligence activity that can be undertaken. Additionally, direction will be given to subordinate units as necessary.

Commander's critical information requirements (CCIR)

4-3. The operations process and the intelligence cycle are mutually dependent. The commander, through the operations process, provides the guidance and focus through CCIRs (priority intelligence requirements (PIRs), essential elements of friendly information (EEFI) and friendly force information requirements (FFIRs)) that drives the intelligence process. The intelligence process provides the continuous intelligence essential to the operations process.

Intelligence requirements (IR)

4-4. IR are questions whose answers fill gaps in the commander's knowledge and understanding of the environment or adversary forces. IR should be associated with decision points relating to friendly course of action (COA). The commander's IR will vary according to the level of command, the nature of operations, the environment, the characteristics of the threat and the commander's mission. Because of their importance, IR have a stated priority in the task of planning and decision making. However, certain IR may be allocated a priority according to the significance of the decision they support. Such IR are often referred to as priority IR (PIR).

Establishing intelligence requirements

4-5. IR may be generated from two sources. They arise directly when the commander poses questions that require responses from the intelligence staff, or they may be identified as part of the intelligence estimate. Regardless of who initiates IR or how they are identified, they are 'owned' by the commander who must approve them.

Information requirements

4-6. Once the IR are determined and prioritized by the commander, the intelligence staff decide how the commander's IR are to be met by determining what information is required. Information requirements are simply the elements of information needed to produce the intelligence that will answer the question posed by the IR. An IR may generate multiple information requirements or, if the IR itself is a simple one, it may translate directly into a single information requirement. Information requirements may be identified by discussion with the HQ staff, as a result of an intelligence estimate, or as a result of the intelligence preparation of the battlefield (IPB) process. Gaps in the knowledge base of intelligence staff will of themselves generate information requirements. However, such information requirements should be prioritized and resourced in accordance with their value against the commander's potential requirements. In other words, intelligence staff do not collect for their own benefit.

Linking requirements and intelligence assessments

4-7. **Initial guidance.** Early in the direction phase, in response to the commander's initial requirements, the intelligence staff undertakes IPB from existing information and intelligence. This serves to guide the next iteration of the intelligence cycle in addressing the specific requirements of the current mission and is therefore considered at the start of the direction phase of the intelligence cycle. IPB helps the commander apply maximum combat power at decisive points in time and space by:

a. continually describing the operating environment and the effects of that environment on both friendly and adversary operations;

b. determining and updating the adversary's likely COA, including adversary intelligence collection activities; and

c. continually assisting in the planning of collection activities to confirm unknown information, associated with a COA, about the environment and threat.

Information requirements management (IRM)

4-8. IRM is the task that accomplishes the following: analyzes information requirements and intelligence gaps; evaluates available assets internal and external to the organization; determines gaps in the use of those assets; recommends intelligence, surveillance, and reconnaissance (ISR) assets controlled by the organization to collect on the CCIR; and submits requests for information (RFI) for adjacent and higher collection support.

Intelligence responsibilities

4-9. Higher level plans, intelligence support plans or intelligence annexes to operation orders (OPORD) will also designate areas of intelligence responsibility for subordinate commands. This will include reporting requirements and the potential allocation of resources to enable collection against higher tasks.

CHAPTER 5

COLLECTION

General

5-1. Collection is defined in AAP-6 – NATO Glossary of Terms and Definitions - as 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. It is a continuous activity that is controlled and coordinated at the highest practical level through an all-source cell (ASC).

Collection management (CM)

5-2. CM links the commander's direction with the collection process to manage the gathering of information and intelligence to meet the commander's critical information requirements (CCIR). CM is the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection sources and agencies (SANDA), monitoring results and re-tasking, as required. The process is sequential and iterative and ensures the most effective use of intelligence surveillance and reconnaissance (ISR) systems available to the force. This in turn gives the commander the best possible understanding of the battlespace to enable him to identify and exploit threat vulnerabilities and windows of opportunity.

Characteristics of collection

5-3. **Redundancy.** Central to collection is the principle of redundancy. Duplicate or different assets capable of answering the information requirement (IR) can compensate for the loss or failure of one collection asset. Through layering, different types of collection capabilities can be tasked to provide information from one source type that can be tested or confirmed by others.

5-4. **Timeliness.** Collection planning must consider the time in which assets can collect information. Their ability to report it, the time required for processing and the time required by a commander to make and execute a decision based on this information or intelligence, are also major considerations.

5-5. **Indicators.** Depending on the nature of the IR, the results could generate new IRs that may be expressed as indicators. Indicators are defined as items of information which reflect the intention or capability of an adversary or potential adversary to adopt or reject a course of action (COA). There are two broad, inter-linked types of indicators relevant to the land environment:

a. **Combat indicators.** Combat indicators are those which reveal the type of operation or COA which the adversary is preparing to conduct. Each type of operation across the spectrum of operations will require specific and characteristic preparations

or events. These preparations and events, identified in advance of the operation or action, constitute indicators.

b. **Identification indicators.** Identification indicators are those which enable the identity and role of a formation, unit or installation to be determined from its organization, tactics or equipment. An example is signature equipment only a specific type of unit is known to hold.

Collection planning

5-6. **Collection plan.** The collection plan methodically captures information to satisfy all the IRs. It links the CCIRs with priority intelligence requirements (PIR), IRs and combat indicators to named areas of interest (NAI) and the time needed to task SANDA effectively. Collection planning considers the capability, limitations and availability of SANDA which can satisfy the information gap. This will include consideration of which SANDA are organic to the command and directly taskable, and which are non-organic and from whom information may be requested. Effective collection planning is directly related to the implementation of the intelligence principles of centralized control, systematic exploitation, responsiveness and source protection.

5-7. **Types of intelligence collection.** The disciplines that support intelligence collection (described in more detail in Annex A of this chapter) are listed below:

a. signals intelligence (SIGINT);

(1) communications intelligence (COMINT); and

(2) electronic intelligence (ELINT);

b. human intelligence (HUMINT);

c. counter-intelligence (CI);

d. imagery intelligence (IMINT);

e. geospatial intelligence (GEOINT);

f. measurement and signature intelligence (MASINT);

g. open source intelligence (OSINT); and

h. technical intelligence (TECHINT)

Collection process

5-8. The collection process comprises two primary concepts as follows:

a. **Requirements management.** Requirements management is the process of converting the IRs of the commander and staff into those of the intelligence staff. These assessments are continuously updated based upon collection results and changes to the operational concept. In addition to the IRs of his own commander, the requirements and collection manager receives requests for information (RFI) from higher or flanking formations. Effective requirements management results in a clear, concise and achievable 'what to collect'.

b. **Collection co-ordination.** Collection co-ordination defines how collection resources are employed to satisfy requirements. Collection co-ordination includes:

(1) the exploitation of sources by collection agencies; and

(2) the delivery of the information obtained to the appropriate processing unit or agency for use in the production of intelligence.

5-9. **Synchronization.** Synchronization co-ordinates planned collection with the output and intent of IPB in a continuous process, ensuring the employment of collection capabilities meets with the intent of the collection plan. The process of synchronization co-ordinates the commander's timelines, from the decision support template (DST), with the projected enemy activities along with the SANDA and surveillance capabilities available. It builds on the intelligence line of the operations synchronization matrix and may be displayed graphically or as a traditional plan.

5-10. **Continuous collection planning.** The collection plan and synchronization matrix must be continually updated and adjusted to keep both requirements and collection synchronized. Satisfied requirements must be removed from the plan and matrix, and assets redirected. New requirements will also be constantly processed.

5-11**. Summary.** There will be other assets outside of the military chain that can provide valuable sources of intelligence and information. The information collection systems available to an ABCA coalition force will need to be coordinated in a holistic fashion and integrated within the construct of a coalition force ISR capability. At the core of this capability will be intelligence staffs that will provide the necessary information collection planning, collection management and analytical support to the mission. A dynamic, system of systems ISR approach will enable the coalition force commander to influence the decision-action cycle of his adversary while maintaining his own operational tempo. As such, a thorough understanding of the characteristics of ISR capabilities is desirable at all levels of command.

Annex:

A. Intelligence, Surveillance and Reconnaissance (ISR) Collection Capabilities

INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR) COLLECTION CAPABILITIES

1. This Annex provides a general description of selected intelligence, surveillance and reconnaissance (ISR) collection capabilities. Specific information can be provided by deployed, specialist intelligence personnel as required. The product of the collection capabilities will be turned into fused intelligence, and are categorized as follows:

a. **Intelligence.**

(1) **Signals intelligence (SIGINT).** The generic term used to describe communications intelligence (COMINT) and electronic intelligence (ELINT) when there is no requirement to differentiate between these two categories of intelligence or to represent fusion of the two.

(2) **COMINT** is intelligence derived from electromagnetic (EM) communications and communications systems by other than intended recipients.

(3) **ELINT** is intelligence derived from EM and non-communications transmissions by other than intended recipients.

(4) **Human intelligence (HUMINT).** A category of intelligence derived from information collected from and provided by human sources, HUMINT activities are broken down into a number of discrete elements. These elements may be conducted at the same time but must be co-coordinated within the HUMINT capability as well as within ISR as a whole. Because of their diversity, a CJ2X function may be required to coordinate and deconflict HUMINT activities.

(4) **Counter-intelligence (CI).** CI is defined as those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations, or by individuals engaged in espionage, sabotage, subversion or terrorism.

(5) **Imagery intelligence (IMINT).** IMINT is 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 aerial and space platforms. It can include full motion video (FMV), synthetic aperture radar (SAR), ground moving target indication (GMTI) and still imagery.

(6) **Geospatial intelligence (GEOINT).** GEOINT is the analysis and exploitation of geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the earth. This can encompass imagery.

(7) **Measurement and signature intelligence (MASINT).** MASINT is scientific and technical intelligence obtained by the qualitative analysis of technical data associated with any source, emitter or sender.

(8) **Open source intelligence (OSINT).** OSINT is the intelligence derived from the analysis of data and information from open source material within the global information environment.

(9) **Technical intelligence (TECHINT).** TECHINT is intelligence concerning foreign technological developments and the performance and operational capabilities of foreign material, which have, or may eventually have, a practical application for military purposes.

b. **Ground surveillance**

(1) **Long range patrols.** Long range patrols provide intelligence and sustained covert surveillance and observation behind adversary lines. They have a wide-ranging surveillance function but can also provide target acquisition (TA) for strike assets as well as battle damage assessment (BDA). They are normally small in size and are, by virtue of their covert nature and limited mobility, best suited to observing named areas of interest (NAI), target areas of interest (TAI) and decision points (DP).

(2) **Unattended ground sensors (UGS).** UGS are capable of remotely monitoring adversary activities by electro-optical, electro-magnetic, magnetic, acoustic, seismic and thermal means. They can be deployed by various means and may provide accurate indications of direction and density, as well as GPS-assisted location determination. Easily transportable, they can be quickly deployed throughout the coalition force battlespace.

(3) **Surveillance and target acquisition (STA) systems.** STA systems provide direct support to indirect fire systems. They are coupled closely to artillery systems through the targeting process and specific Communication Information Systems (CIS). Their primary purpose is to carry out TA, however this information is also an important element of the overall ISR capability and contributes to the intelligence effort.

(4) **Persistent surveillance.** Recent operations have used aerostats and mast mounted surveillance systems in a persistent surveillance role. This is an area of surveillance that is likely to endure.

c. **Reconnaissance.**

(1) **Ground based reconnaissance**. Ground based reconnaissance gives depth, endurance and resolution to the ISR mix and remains effective when technical capabilities are constrained by contested battlespace and/or weather. Collection assets should be deployed without rigid adherence to templates; rather they should be packaged to provide broad utility across a spectrum of

requirements. While continuing to collect information, these reconnaissance assets may also be used in the counter-reconnaissance role, attempting to deny information to the adversary and 'shaping' adversary forces to coalition force advantage.

(2) **Engineer reconnaissance.** Engineer reconnaissance identifies changes to natural and man-made features caused by battle damage or natural weather effects (such as flooding).

(3) **Chemical, biological, radiological and nuclear (CBRN) reconnaissance.** A directed effort to determine the nature and degree of CBRN hazards through the employment of reconnaissance, survey and surveillance, which can exploit both surface and air assets.

d. **Airborne surveillance and reconnaissance.**

(1) Air and aviation assets can be used in a surveillance and reconnaissance role as part of the capabilities available to a coalition force. Their employment in an ISR role cannot be guaranteed as they may not be permanently assigned to land forces, air component staffs are able to brief fully on their capabilities and tasking cycles.

(2) Unmanned aerial systems (UAS) are a highly flexible asset, with a variety of sensors well suited to roles in support of ISR requirements. It is vital that UAS are seen as part of a 'system of systems' and are but one element of the ISR effort supporting other sensors and strike systems.

(3) Coalition force commanders and subordinate commanders will most likely have access to strategic level space-based surveillance systems that may be capable of providing near real time (NRT) imagery and SIGINT support. This imagery and SIGINT would play an important role in cueing other sensors within the theater of operations as well as aiding intelligence staffs at various levels with their respective collection planning and analysis.

CHAPTER 6

PROCESSING

General

6-1. Processing is the production of intelligence through the collation, evaluation, analysis, integration and interpretation of information and other intelligence. While the phases of the processing step may be concurrent, any one piece of information or combat information is processed through the following phases:

a. Collation involves the logging, recording and meta-tagging incoming information. It includes database integration, geodetic storage, map and chart marking, electronic or manual filing, and cross referencing.

b. Evaluation is the appraisal of an item of information in terms of its credibility and the reliability of the reporting sources and agencies (SANDA). Evaluation is done progressively through the processing phase as new information is compared to processed information to determine similarities or differences.

c. Analysis is the separation of information into its component parts.

d. Integration is the grouping of related elements of analyzed information with the aim of establishing patterns and relationships.

e. Interpretation is the phase in which the meaning or implication of information is determined. This interpretation is done in relation to current knowledge.

Processing systems

6-2. The processing system may be as simple as a well marked map with overlays based on estimates, the collection plan and geographic characteristics, supported by a sheaf of log sheets in a binder. Alternately, it may consist of a complex computer system with interactive databases, a geographic information system (GIS) and a digital imagery catalog. Whatever system is used, it should ensure a logical flow of activity takes place in the intelligence office and all steps in the processing step are completed.

6-3. The requirements for a processing system are:

a. a system for recording the receipt of information;

b. a method which uniquely tags each piece of information for accounting, retrieval and integration purposes;

c. a system for the visual display of spatially related information including:

(1) locations;

(2) military symbology; and

(3) a legend;

d. a system for the recording and display of non-spatially related information including order of battle (ORBAT), equipment, and biographical data, as well as the linkages between people, organizations and events;

e. a system for the storage of structured textual information;

f. a system for the storage of unstructured textual information; and

g. a system which allows the cross referencing of information to information or intelligence in any format.

6-4. Collation involves the following activities:

a. logging and recording;

(1) acknowledgement of receipt (if required);

(2) manipulation into a suitable form (if required);

(3) tagging; and

(4) recording in the intelligence log;

b. dissemination of time critical information;

c. display (if required); and

d. filing.

Dissemination of time critical information

6-5. The collation process must identify and disseminate information which is of immediate and obvious significance. This dissemination takes precedence over the administrative aspects of the collation sub-phases.

Evaluation

6-6. The aim of evaluation is to determine the likelihood a piece of information is correct. By assessing the credibility of the information and the reliability of the reporting SANDA, intelligence staff can judge how much weight to give the information during integration and interpretation.

6-7. Evaluation is conducted using the Admiralty Grading System. This system is an alphanumeric indication of the degree of confidence that may be placed in an item of information. The system indicates the degree of reliability of the SANDA, expressed as a letter ranging from A to F, and the degree of credibility of the information, expressed as a number ranging from 1 to 6. The combination of a letter and number is the evaluation grading for each item of information. The Admiralty Grading System is explained in table 6-1.

Admiralty Grading System			
Reliability of Source		**Credibility of 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 6-1: Admiralty Grading System

6-8. **Explanation of sources and agencies reliability gradings.** The degrees of confidence for SANDA reliability as assessed as follows:

a. completely reliable refers to a tried and trusted SANDA which can be depended upon with confidence;

b. usually reliable refers to a SANDA which has been successful in the past but for which there is still some element of doubt in a particular case;

c. fairly reliable refers to a SANDA which has occasionally been used in the past and upon which some degree of confidence can be based;

d. not usually reliable refers to a SANDA which has been used in the past but which has proved more often than not unreliable;

e. unreliable refers to a SANDA which has been used in the past and has proved unworthy of any confidence; and

f. reliability cannot be judged refers to a SANDA which has not been used in the past or for which there is insufficient information to make an assessment.

6-9. **The evaluation of sources and agencies reliability.** SANDA reliability should be evaluated according to the type of information reported and the circumstances in which it was collected. The collection manager (CM) maintains SANDA profiles which provide a history and aggregated reliability evaluation. The evaluation of a SANDA should include the following factors:

a. **Capability.** Did the SANDA have the access and opportunity to collect the information first hand? For technical SANDA, were the equipment performance characteristics appropriate for the task and consistent with the reported results?

b. **Origin.** If the reporting SANDA is relying on second hand observations, is the original SANDA of the information identified, and how many intermediaries (opportunities for transmission error) has the information passed through? Has the reporting SANDA provided fact or hearsay?

c. **Competence**. Is the SANDA competent, by virtue of training, experience or knowledge to report and comment accurately on the sort of information provided? To what degree could the SANDA be subject to deception? To what degree has the SANDA made assessments from information? Is the distinction between fact, conclusion and assessment?

d. **Objectivity.** Is there potential for bias, emotion or prejudice to have colored or distorted the reported facts and inferences?

e. **Motivation.** What motivated the report? Is loyalty or integrity an issue?

f. **Performance record.** How reliable has the SANDA been in the past?

6-10. **Explanation of sources and agencies credibility gradings.** The credibility of an item is an assessment of its accuracy. While it is not always possible to state whether information is true or false, the relative accuracy of an item may be assessed by comparing it with confirmed or unconfirmed information. Determination of credibility should not be based on the assessed course of action (COA) or the expected pattern of events but on what fact indicates is actually occurring. The intelligence principle of objectivity is paramount. The degrees of confidence for information credibility are:

a. Confirmed by other SANDA refers to information that is the same as information from a different SANDA.

b. Probably true refers to information whose credibility is supported by the quantity and quality of previously received information.

c. Possibly true refers to newly reported information that does not conflict with the previously reported behavior pattern of the threat but for which there is insufficient confirmation to establish any higher degree of likelihood.

d. Doubtful refers to information which tends to conflict with the previously reported or established behavior pattern of the threat.

e. Improbable refers to information which contradicts previously reported information or conflicts with the established threat behavior pattern to a marked degree.

f. Truth cannot be judged refers to any new piece of information for which there is no basis for comparison with any known threat behavior pattern. This rating should only be used when the accurate use of a higher rating is impossible.

6-11. **Independent evaluation.** Reliability and credibility must be considered and assessed independently. For example, information which is assessed as being probably true and is reported by a usually reliable SANDA is given a B2 evaluated grading; information from the same SANDA, about which the truth cannot be judged, is given a grading of B6.

Analysis

6-12. Doctrinally, analysis is the detailed examination of information and its separation into component fact or inference. However, the term 'analysis' is also colloquially used as a generic term for the processing step of the intelligence cycle. Even within intelligence staffs, the term 'analyst' refers to a person who conducts all the phases of the processing.

6-13. Analysis involves the recognition and extraction of component fact or inference from often complex reports. Even a simple report will usually contain information components indicating time of report, time of incident, location, nature of activity and extent of activity. Each fact or inference needs to be isolated so that it can be integrated and interpreted.

Integration

6-14. Integration involves the consolidation of component parts of information, isolated during the analysis step, with other information and previously produced intelligence. This process of grouping like fact or inference reveals patterns and relationships which are the basis for subsequent interpretation. Integration may be a quick mental process involving the addition of one piece of new information to an existing intelligence picture, or it may be a lengthy process of merging a large amount of data. The most reliable intelligence is developed through the integration, in this context often referred to as fusion, of information from different SANDA.

Interpretation

6-15. The last phase of the processing step, interpretation, is the most important. Automated processing systems can conduct a significant amount of collation, analysis and integration, however, interpretation requires the input of the human mind. Interpretation is essentially a mental discipline and should be based on known information and intelligence, experience, common sense and logic. From a military perspective, interpretation requires a thorough knowledge and understanding of the threat.

6-16. In practice, interpretation is the drawing of inferences and making of assessments from reported information. These inferences and assessments can be wrong or can be misled by deception. In situations where no interpretation is possible, further collection should be conducted.

6-17. **Degree of Confidence.** Assessments are not rated using the Admiralty Grading System. Instead they are qualified by terms such as 'probable', 'likely', 'possible' or 'unlikely'. In all cases the commander needs to be made aware of uncertainty and, where appropriate, of alternate interpretation.

CHAPTER 7

DISSEMINATION

General

7-1. Dissemination is the timely conveyance of information or intelligence, in an appropriate form and by any suitable means, to those who need to use it. The frequency of routine dissemination should be established so it is consistent with the commander's decision-making process, the staff working routine and the flow of other intelligence reporting.

7-2. Dissemination includes both the ‘push’ of information/intelligence to anticipated users and the access (‘pull’) of information/intelligence by users from information repositories that sit inside or outside of the immediate headquarters (HQ) (including open sources). Any coalition intelligence architecture must be able to support both of these methods.

7-3. In line with the principles of intelligence, particularly accessibility, it is fundamental to the success of coalition operations that the broadest possible sharing of intelligence information is achieved. Coalition intelligence organizations must provide intelligence information in a way that maximizes its value to the coalition members at all levels. The intent is that intelligence sharing must be the rule rather than the exception. See Annex A to this chapter.

Select

7-4. Selection of relevant information and intelligence requires thorough knowledge of the commander's intelligence requirements (IR), the operational plan and the situation. Intelligence staff must be aware that the absence of combat indicators, information or intelligence about threats or the environment may also lead to assessment of enemy intent and must be reported as such. The following factors should be considered when selecting information and intelligence for dissemination and access:

a. answers to IR;

b. answers to requests for information (RFI);

c. indicators of unusual or unexpected adversary activity, including location, size, movement and activity;

d. indicators of friendly and adversary deception activities; and

e. indicators of friendly operations security (OPSEC) breaches.

7-5. The intelligence/intelligence surveillance and reconnaissance (ISR) architecture should, as far as possible, enable all staff functions to search for and then access relevant information/intelligence held throughout all levels of the coalition.

7-6. There are numerous methods and techniques for disseminating and accessing information and intelligence. The appropriate technique in any particular situation depends on many factors such as capabilities and mission requirements. Possible dissemination methods and techniques include access to federated databases, direct electronic dissemination (a messaging program); dissemination via chat rooms; instant messaging; web posting; printing the information and sending it via courier; or putting the information on a compact disc and sending it to the recipient.

7-7. In particular, when posting information to a website, the intended recipients must be notified when new or critical information has been posted; simply posting information to a website does not ensure the intended user has received it.

Prepare

7-8. **Choice of suitable media.** The choice of the most suitable means for dissemination will depend on the type of intelligence being disseminated, time constraints, the available means of communication and the recipient's requirements. Reports must be concise, but not at the expense of relevant material, and there may need to be a compromise between medium and content to ensure timely delivery. Dissemination may be:

a. verbal;

b. written;

c. graphic; and

d. multi-media.

7-9. Intelligence should be classified at the lowest level and downgrading instructions should be included. In other words, intelligence production should be informed by a policy of ‘write to release’. Where possible, intelligence should be sanitized in accordance with security instructions to allow dissemination to the lowest level. Refer to Annex A of this chapter for more on ‘write to release’.

Deliver

7-10. The principle of timeliness not only includes the time required for processing and dissemination, it also includes consideration of the time necessary to make and execute a decision based on the received information or intelligence. While current intelligence will often have immediate tactical or operational value and require to be passed by the fastest means possible, basic intelligence will usually be of lower priority for transmission.

7-11. Dissemination of information and intelligence should be by secure means consistent with its security classification and the intelligence principle of source protection. Sensitive sources and agencies (SANDA) should establish rapid sanitization procedures to allow risk management of the dissemination of time critical information.

Intelligence products

7-12. Intelligence products are all forms of outputs of the intelligence cycle including textual and graphic. They encompass intelligence reports (INTREP), summaries (INTSUM), assessments, oral briefings, plans, annexes to operation orders and intelligence databases to name a few. These outputs contribute to the continuous updating of the common operational picture (COP).

Briefings, orders and reports

7-13. Briefings permit the discussion and clarification of information, intelligence and assessments. They are quick, and when appropriately supported by briefing aids, are easy to assimilate. Verbal briefings should:

a. follow the appropriate format;

b. be focused on the requirements of the customer(s);

c. clearly differentiate between fact and assessment; and

d. cover only the period since the last briefing to the same customer(s).

7-14. The function of the brief will vary depending on the customer requirements, however they are usually one of the following:

a. **Information brief.** Information briefs are designed to provide information and basic intelligence and are often referred to as a 'background brief'. An assessment is not required in an information brief, however, where it is likely to be of value to the audience, regardless of how broad it may be, it should be included.

b. **Decision brief.** Decision briefs are used in situations that require a command decision. Intelligence staff may use a decision brief when seeking assets for collection tasks.

c. **Mission or task brief.** Mission or task briefs are briefs used to verbally task SANDA. This brief is detailed in intelligence staff processes (not yet published).

d. **Staff brief.** Staff briefs are scheduled periodically to inform the commander and for the exchange of information between staff to ensure a coordinated effort. Staff briefs differ from other briefs in that all the functional staff elements brief sequentially. The chief of staff usually presides over the staff briefing while the commander provides guidance and makes decisions as required. The frequency, timings and sequence of staff briefings is stated in standing operating procedures (SOP). Types of staff briefings include:

(1) **Intelligence/update brief.** These briefings are scheduled, regular briefings usually held at least once a day to update the commander and staff on the situation and to brief future intentions. In this brief, intelligence staff provide

information on events during the period and predictive threat and environmental assessment.

(2) **Staff assessments.** A staff assessment involves staff presenting assessments in their area of responsibility, culminating in a commander's decision to adopt a specific course of action (COA). The most common forms of staff assessment are the intelligence preparation of the battlespace (IPB) briefs which are given as part of the operational planning process (OPP).

(3) **Orders.** Intelligence staff will be required to provide annexes to written orders and briefings on the intelligence aspects of a commander's verbal orders, such as the collection plan.

e. **Handover/takeover brief.** During operations and exercises, HQ staff employ a shift system of duty. A handover/takeover brief is used to ensure continuity of knowledge and assessment.

f. **Back brief.** Is a brief in which staff state their understanding of orders and instructions and the implications of such.

7-15. **Preparation of a brief.** All intelligence briefs must conform to the principles of accuracy, brevity and clarity. In addition, they must use correct military terminology, distinguish between fact and assessment, focus on the function of the brief, and, where possible, be predictive.

7-16. **Coordination.** The intelligence staff should co-ordinate the contents of their brief with other staff functions, primarily operations staff, to ensure that there is no duplication and there are no events of which the other is unaware. Preferably, intelligence and operations staff members will rehearse their briefs together.

7-17. **Orders and reports.** The formats for orders and reports will be stated in SOP, which will include the format, and notes on the compilation of the written intelligence orders for the following products:

a. intelligence estimate including:

(1) analysis of the operational environment;

(2) analysis of the situation, stakeholders and threat forces including center of gravity construct;

(3) threat group capability analysis; and

(4) COA analysis;

b. intelligence support plan or intelligence annex to the operations order (OPORD);

c. intelligence reports (INTREPS); and

d. Intelligence summaries (INTSUMS).

Annex:

A. Implement the Write to Release Approach in the ABCA Armies

IMPLEMENTING THE WRITE TO RELEASE APPROACH IN THE ABCA ARMIES

Introduction

1. In line with the principles of intelligence, particularly accessibility, it is fundamental to the success of coalition operations the broadest possible sharing of intelligence information is achieved. Coalition intelligence organizations must provide intelligence information in a way that maximizes its value to the coalition members at all levels. The intent is intelligence sharing must be the rule rather than the exception.

2. A key requirement for all coalition intelligence organizations must be to provide accurate, relevant and timely intelligence information to users at the earliest point where they can understand and effectively use it. In order to be effective, whenever possible, intelligence content must be separated from sensitive sources and methods, while still providing users with sufficient context and background.

3. Information sharing remains a key area of interoperability concern. While interoperability of systems is the main area of concern, the classification and subsequent dissemination of intelligence product is also a concern. This involves two related issues: intelligence product is produced without a thorough understanding of who requires the information and/or it is being over-classified. One solution is to emphasize the 'write to release' approach in intelligence production, which although current policy within ABCA nations, is not universally applied.

Aim

4. The aim of this Annex is to raise the awareness of intelligence policy makers, intelligence supervisors and intelligence producers of current issues and to make recommendations regarding 'write to release' in order to improve information sharing amongst ABCA nations.

Scope

5. This Annex will address the considerations for utilizing the 'write to release' approach, identify methods and training requirements and make recommendations that will influence the ABCA nations to adopt practices consistent with the 'write to release' policy. The report does not address the detail of the sanitization or tearline reporting processes as these are covered by existing national agency rules.

Definitions

6. **'Write to release':** A general approach whereby intelligence reports are written in such a way that sources and methods are disguised so the report can be distributed to users or intelligence partners at lower security levels. In essence, 'write to release' is proactive sanitization that makes intelligence more readily available to a more diverse set of users. The

term encompasses a number of specific implementation approaches, including sanitized leads and tearline reporting.

7. **Tearline reporting:** An automated or manual technique for separating an intelligence report into multiple portions separated by machine-or-human-readable tearlines. A tearline section is the area in an intelligence report or finished intelligence product where the sanitized version of a more highly classified and/or controlled report is located. The sanitized information within the tearlines contains the substance of the more detailed information without identifying the sensitive sources and methods, allowing wider dissemination of the substantive intelligence information to authorized users.

8. **Intelligence producers.** In this report the term intelligence producers includes all those intelligence personnel who are involved in the production of intelligence reports or assessments at all levels. It is a wider term than analyst and is written to encompass everyone from the writer of a report/assessment to those that authorize the release of reports/assessments.

Considerations

9. Although there are no definitive procedures for ‘write to release’, there are a number of considerations that need to be adopted in order to ensure that the concept is embedded in ABCA practice.

10. **National constraints.** The applicability of the ‘write to release’ approach in terms of who can implement it and where depend on national rules and regulations.

11. **Risk.** The ‘write to release’ approach aims to balance the requirement of greater intelligence information sharing with the need to protect sources and methods. Although the need-to-know principle must always be considered, reports need to be written for the widest dissemination to account for all possible audiences. Seeking perfect protection from the risk of unintended disclosure by restricting information sharing will result in an unacceptable increase in the risk of failing to provide users all relevant intelligence information. The user requirements become the basis for need-to-know determinations. Users, in turn, must ensure that access to intelligence information is limited to those who need it.

12. **Understand the intended audience**. The intelligence producer must understand the user requirements for the intelligence information and then determine whether the user requires the highly classified information or whether an assessment can be produced that is persuasive and accurate without it.

13. **Avoid over–classification.** Over-classification of intelligence product limits the utility of the information and may result in it not being disseminated to all those that need to know it. Intelligence producers must ensure the classification of any products produced is assessed on a case-by-case basis and not the result of default settings.

14. **Maximum use of multiple sources (collateral).** The operational environment provides an ever-growing volume of data and information available from numerous sources, from which analysts can develop intelligence products. As well as producing more robust assessments, the use of multiple sources may allow the same assessments to be developed from a lower classified or less-sensitive source, thus widening the utility of the product.

Methods

15. Although there are no definitive methods for 'write to release' there are a number of means that can be utilized:

a. **Use of tearline reporting.** Tearline reporting has been developed in order to allow more highly classified material to be released at a lower level. The maximum use of tearline reporting by intelligence producers will aid the 'write to release' approach.

b. **Use of paragraph classifications.** The use of individual paragraph classifications instead of only classifying the overall document allows intelligence producers and users to more readily utilize the information within the product for further assessment or dissemination.

c. **Use of annexes.** If intelligence products cannot be produced at a lower more releasable level, then it may be more appropriate to produce the product at a lower level using annexes as the means of containing the higher classified material.

Training

16. **Training.** The 'write to release' approach is an art more than a science. Despite this the concept can be and needs to be taught in all intelligence training.

17. **General concept.** In order to embed the 'write to release' approach in the intelligence community culture, training needs to be conducted at a number of levels. The intent of 'write to release' training is all intelligence producers, and wherever possible commanders, understand the requirement to produce intelligence products for the widest possible dissemination. The training needs to focus on two areas: developing this culture and mindset in the intelligence producers; and providing the means intelligence products can be written to release. This training can be accomplished by incorporating this philosophy into institutional and force training at all levels and in all environments.

a. **Baseline training.** The intent of baseline training is all analysts understand the need that all relevant intelligence information must be readily available to users that need it; and have exposure to the means of achieving it.

b. **Continuation training.** The intent of continuation training is to build on the increased experience of analysts as they progress. This training should be focused on

expanding the range of means of writing to release and be based on ongoing real world examples.

c. **Mission specific training.** The intent of mission specific training is to ensure all intelligence producers are aware of the user requirements of the mission and the specific 'write to release' concepts of the mission. Mission specific training should build on baseline and continuation training and should be closely linked to mission rehearsal.

Conclusion

18. Information sharing remains a key area of interoperability concern. The 'write to release' approach provides a way to alleviate the problem. ABCA nations must ensure the 'write to release' approach is fully understood and integrated into both training and operational environments at all levels in order to improve information sharing.

CHAPTER 8

INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS

General

8-1. Noting there are varying terms for information operations/influence activities among ABCA nations for the purpose of this CIH the term information operations (IO) will be used.

8-2. Intelligence support is required to conduct IO; particularly in support of planning coordination, deconfliction and employment of military disciplines available to achieve IO effects. This chapter will focus on intelligence support to operations security (OPSEC), psychological operations (PSYOPS), deception, electronic warfare (EW), and physical destruction. In addition this chapter will consider intelligence support to key leader engagement (KLE) and to security sector reform (SSR).

8-3. The disciplines listed above can stand alone, but are most effective when integrated to form an over-arching IO approach. IO is underscored by intelligence, which is the key element in the planning and conduct of both offensive and defensive IO operations. Intelligence, as a product, supports IO no differently to the intrinsic support provided to all operations. Planning for IO cannot be conducted without intelligence on adversary information and information systems, perceptions, and critical vulnerabilities in their command and control process. Additionally, each capability used in an IO context will have separate and continuous intelligence support requirements. Some examples of which are:

a. the updated psychological profiles of adversary commanders;

b. an ongoing estimate of the degree of cohesiveness among factions within an insurrectionary movement and monitoring adversary; and

c. neutral media to support the ongoing assessment of the effects of an IO campaign.

Intelligence support to information operations planning

8-4. Intelligence support to IO planning is conducted as part of the intelligence preparation of the battlefield or battlespace (IPB) process. One of the key outputs from IPB is an analysis of the desired objectives and/or end states of stakeholders. These desires are usually **categorized** relative to broad capability. The categories may be elements of national power such as politics, economics, military and society. Capability analysis processes within IPB also provide detail on stakeholder capacity and intent to conduct or sustain defensive and offensive IO.

8-5. Intelligence support will aim to define critical nodes and vulnerabilities within the adversary's decision making process; these include the key personnel, equipment, procedures and protocols involved in the transfer of information required for successful command and control. Such intelligence support will orient key aspects of the operations plan towards the systematic disruption and degradation of the adversary's ability to make

timely and informed decisions. Friendly force staff advice, linked to intelligence advice on adversary courses of action and counter-intelligence advice on the threats to security, provide the operations planning process with the background to protect and enhance our own decision making. Accurate, timely and directed intelligence provides the foundation on which IO are based.

8-6. Intelligence provides the essential basis for planning IO through the following considerations:

a. The understanding of the perceptions of the adversary, neutrals and local populations and their susceptibilities to influence.

b. The adversary commander's freedom of action and the freedom of action allowed to subordinates.

c. Adversary IO capability, intent, morale and vulnerability to offensive IO.

d. Command and control (C2) aspects such as key personnel, target audiences, headquarters (HQ), communications nodes, databases or intelligence collection systems. C2 nodes that appear in more than one adversary course of action should be highlighted for targeting.

e. Assessments of friendly vulnerability to adversary IO.

Intelligence support to operations security

8-7. OPSEC - an operations responsibility - seeks to reduce or deny the adversary information concerning friendly dispositions, capabilities, vulnerabilities and intentions both on training and operations.

8-8. Intelligence support for OPSEC planning focuses on the capabilities and limitations of the adversary's intelligence surveillance and reconnaissance (ISR) systems, including the adversary's decision cycle and any bias towards certain information/intelligence collectors or disciplines in order to reduce the vulnerability of friendly C2 assets and installations to attack.

Intelligence support to psychological operations

8-9. PSYOPS - an operations function - aims to influence adversary attitudes and behavior, thereby affecting the achievement of military objectives. It has the potential to damage the adversary C2 chain by lowering morale, instilling fear and breeding distrust. Intelligence input to all aspects of PSYOPS is substantial.

8-10. The intelligence staff work closely with the PSYOPS staff to plan PSYOPS operations and effectively integrate these with the other IO elements. Equally, it may be desirable in support of PSYOPS to reveal certain aspects of friendly dispositions, capabilities and intentions.

8-11. PSYOPS requires basic intelligence on the cultural, religious, social and economic aspects of the target country/population and its government/leadership, communications and media.

8-12. Intelligence contributes to the development of psychological assessments, which look to identify target audiences within the opposing force, and those factors most likely to influence their attitudes and behavior in favor of the Commander's mission. The conditions and attitudes of target groups are likely to change as the situation develops. Current all source intelligence, in particular human intelligence (HUMINT) and signals intelligence (SIGINT), is therefore vital; both in the planning phase, and then throughout the execution of PSYOPS, to assess the effectiveness of current campaigns, to reinforce success and to re-allocate limited resources, if the desired effect is not being achieved. Defensively, the intelligence staffs also monitor the effect of the adversary's PSYOPS on ABCA troops.

8-13. Intelligence support to deception. Intelligence supports deception, an ops function, by **analyzing** the adversary's ISR capabilities and identifying his perception of the battlefield and any changes to it. It also includes the adversary's own deception doctrine, tactics/procedures, capabilities and intentions. During the execution of deception operations the adversary's response must be monitored to determine effectiveness.

Intelligence support to electronic warfare

8-14. Intelligence support to electronic warfare (EW) includes determining and presenting the adversary's EW systems and their information system infrastructure, to include:

a. potential use and effectiveness against friendly equipment;

b. critical adversary information systems and C2 nodes;

c. adversary's C2 system vulnerabilities; and

d. the means they use to protect their C2 systems.

Intelligence support to physical destruction

8-15. The focus of intelligence support is to provide details of target types, locations, movement, assessment of possible collateral damage, and the capability through battle damage assessment (BDA) to assess the effectiveness of targeting. There is a requirement for close integration with national targeting priorities. An assessment must also be made, with CJ2 advice, on the balance of advantage of destruction against exploitation, including the development of a no-strike (both passive and active measures) targeting list.

8-16. **Intelligence support to key leader engagement (KLE).** KLE includes engagement between commanders and local persons of influence across a variety of areas. Considerable intelligence effort may be required to help shape KLE. This may include personality profiles and network analysis.

8-17. **Intelligence support to security sector reform (SSR).** SSR involves the development of all aspects of host nation security forces. SSR staff elements will be supported by similar products. This will include reliability assessments of key host nation forces.

Cultural awareness in information operations planning

8-18. The importance of military forces being able to understand the nuances of culture in terms of their impact on the conduct of military operations and the determination of opportunities and vulnerabilities, is critical in the context of current and probable future operations involving ABCA Armies.

Annex:

A. Example Cultural Factors

EXAMPLE CULTURAL FACTORS

Reference:

A. ABCA Standard 2066 (Cultural Awareness Tactics, Techniques and Procedures (TTP)) dated March 2007

General:

- Socio-cultural system
- Cultural history
- Shame and honor concepts
- Tribal/Clan/Group dynamics
- Urban/rural divide
- Social identity
- Role of religion
- Formal political system
- National
  - Representatives
  - Ministries/Departments
- Regional
  - Representatives
- Local
  - Representatives
- Political parties
- Bureaucracy
- Geopolitical boundaries

Ethno-religious groups:

- Primary groups
- Religious structure
  - Patronage networks
  - Charities
- External links
- Tribes/Clans/Groups
- Tribe
  - Sub-tribe
  - Clans
  - Sub-clans
  - Families
- Non-traditional groupings
- Patronage networks

- Outside influences
  - Foreign groups (non-criminal)
  - Internally Displaced Persons
  - Foreign NGOs
  - Foreign governments
  - Relationship with border countries
- Interactions
- Visiting
- Greetings
- Work
- Gifts
- Taboos
- Weddings and Funerals
- Blood money (or related concept)
- Showing Respect
- Gender Roles

Security:

- Policing
- Judicial system
- Penal system
- Criminal activities
  - Narcotics-trafficking
  - Black market
  - Smuggling
  - Routes
  - Commodities
- Front companies
- Intimidation and extortion
- Kidnapping, theft, murder, etc.
- Ordnance and military supplies
- Unexploded ordnance available
- Weapons, explosives markets
- Weapons smuggling routes

Economy:

- Imports and exports
- Social isolation legacy?
- Agriculture
- Barter economy
- Trading companies
- Business law, banking, contracts, insurance
- Employment rates and impact on population/perceptions
- Labor force occupation and demographics
- Local businesses and companies
- Income demographics
  - Major sources
  - Per capita income
- Coalition government projects
- Natural resources

Services:

- Hospital and clinics
  - Availability of advanced services
  - Number, quality and type
  - Education of staff
- Education
  - Quality and type
  - Number of schools and availability
  - Ages taught, types
- Government wages
- Water
- Sewer
  - Age and quality of system
  - Open system and health effects
  - Map of sewers
- Ice factory or common home refrigeration?
  - Impact on food storage, quality of life
- Electricity
  - Availability by zone, by Kilowatt per/hour
  - Sources and production plants
  - How are the plants powered?
  - Distribution networks and administration
- Subsidized goods
  - Gas?
  - Cooking oil?
  - Food?
  - Impact of change in subsidies
- Government improvement projects
  - Ongoing, planned
  - Rate success
- Public Safety
- Armed Forces

Information environment:

- Formal communication
  - Broadcast media
  - Print media
  - Newspapers
- Freedom or lack thereof
  - Trust in the media
  - Connection to government or opposition
- Fliers/handouts
- Outdoor media (banners, ads)
- Websites and Internet availability
- Impact of Internet by zone
- Information Communication
- Authority figures (Family, religious, group)
- Rumor centers (tea shops, markets, taxis)
- Telecommunications
- Cell phone nodes and availability
- Text messaging capable?
- Availability and use of email

Major resources:

- Drinking water
  - Reservoirs
  - Pumping stations
  - Pipelines
  - Water treatment plants
- Oil and fuel
  - Sources
  - Pumping stations
  - Pipelines
  - Refineries
- Gas stations
  - Distribution locations
- Agricultural
  - Irrigation paths
  - Chemicals
- Communications
- Telecom systems
  - Internet cafes
  - Courier routes

Key individuals:

- Religious
- Tribal
- Community
- Political
- Educators
- Medical
- Business
- Military

The following templates should be used to guide considerations of specific individuals and groups in the battlespace:

Template: for each group:

- Where do they get their security?
- Where do they get goods, services and wages?
- What ideologies resonate with them?
- Who are the traditional authority figures they look to for direction?
- Who are they allied with?
- What is important to them?
- Cultural narratives

Template: for each leader:

- Where does his authority come from?
- Coercive force?
- Economic incentive and disincentive?
- Ideology?
- Charisma?
- Traditional Authority?
- Who is he allied with?
- What are the reasons for that alliance?

Template: for each person working with the coalition:

- Where do he and his family get their security?
- Where do he and his family get goods, services and wages?
- What ideologies resonate with him?
- Does he look to a traditional authority figure for guidance?

Template: for each former detainee:

- Reason for detention and release
- Information obtained and usefulness
- Family, tribal, religious or gang affiliation
- Interests: see for each person working for the Coalition

CHAPTER 9

GEOSPATIAL SUPPORT TO INTELLIGENCE

Geospatial support

9-1. **Context.** Geospatial support is fundamental to the planning and conduct of operations. In this handbook geospatial support is addressed specifically to the intelligence function. Further reading relative to geospatial support can be found in the ABCA Coalition Operations Handbook COH (ABCA Publication 332 Edition 5).

General

9-2. Geospatial support is the collection, processing, management, exploitation, analysis, production, presentation and dissemination of geospatially referenced information to enable the commander and staffs during the planning, decision making and conduct of operations. It can also include meteorological and oceanographic information.

9-3. Geospatial support provides focused operational and tactical support to the force commander and his staff providing the following functional tasks:

a. terrain analysis and visualization;

b. geospatial data management;

c. geospatial data production;

d. geospatial data dissemination ;

e. geospatial data acquisition and collection (including geodetic and field survey);

f. geospatial advice; and

g. geospatial system support.

9-4. In the context of ABCA, geospatial support is an engineer function.

Geospatial support to intelligence

9-5. Geospatial support to intelligence contributes to the conduct of intelligence preparation of the battlefield or battlespace (IPB) through the provision of physical terrain analysis and visualization and through the provision of Geospatial Information.

9-6. An element of geospatial support personnel, ordinarily a military geospatial information (MGI) team, will provide support to intelligence by being embedded within the All Source Cell (ASC).

9-7. Geospatial support facilitates the exploitation and analysis of all source intelligence (eg, measurement and signature, signals intelligence, human intelligence and imagery

intelligence) with geospatial information to describe, assess and visually depict physical features and geospatial referenced activities on the earth and is provided as an element of a fused product.

9-8. As an output, geospatial support integrates geospatial information with intelligence outputs. When integrating these outputs, it can provide an enhanced and value-added product to assist with decision making as it fuses accurate geospatial foundation products together with timely intelligence.

Summary

9-9. The responsibility for providing geospatial support, in this context geospatial information, to national component forces resides with the respective nations. However, efficiencies and synergies can be gained from coordinating this support, such as the sharing of geospatial data sets and products across the coalition, which supports a shared situational awareness and avoids duplication of work. In a coalition the synchronization of geospatial support and geospatial intelligence responsibilities coordinated at the highest possible level and depends on the interoperability of national geospatial information. Dividing these responsibilities is a high priority. Commanders must address them early in the planning process as geospatial data provision takes considerable effort and time, particularly when operating in areas where current geospatial data do not exist.

Checklist

9-10. Geospatial support to intelligence concept should be integrated with the Geospatial Support Concept checklist per COH Chapter 10, Geospatial Support. Key elements for consideration for Geospatial support to intelligence not included in the COH are:

- What is the security level of the geospatial personnel and systems operating within the ASC?
- Are the geospatial personnel on a standalone or networked systems?
- What are the processes for data sharing between geospatial and non-geospatial databases?
- What is the command relationship of the geospatial personnel working within the ASC?

CHAPTER 10

INTELLIGENCE SUPPORT TO TARGETING

General

10-1. Intelligence provides the fire support coordinator, information engagement officer, electronic warfare (EW) officer, and the information operations officer with information and intelligence for targeting the adversary's forces and systems with direct and indirect lethal and nonlethal effects. It includes identification of the adversary's capabilities and vulnerabilities to support the targeting process. Intelligence ensures the intelligence, surveillance and reconnaissance (ISR) plan supports the finalized targeting plan.

10-2. Intelligence support to target development provides systematic analysis of adversary forces and operations to determine high-value targets (HVTs) (people, organizations or military units), high payoff targets (HPTs) (people, organizations or military units), systems and system components for potential attack through maneuver, fires, electronic means, or information engagement or operations.

10-3. Intelligence support to target detection establishes procedures for dissemination of targeting information. The targeting team develops the sensor and attack guidance matrix to determine the sensor required to detect and locate targets. Intelligence places these requirements into the intelligence, surveillance and reconnaissance (ISR) synchronization plan for later incorporation into the ISR plan.

10-4. **Collateral damage.** The increasing international public sensitivity to civilian casualties and collateral damage makes intelligence support to targeting even more crucial as a function, as all targets now require detailed confirmation and re-validation before they are attacked. Intelligence support also has a key role in advising operations staff on weapons effects and subsequent battle damage assessment (BDA) with regard to collateral damage.

10-5. Intelligence analysis establishes the adversary center of gravity, critical vulnerabilities, system models, behavioral dispositions, dependent infrastructure, HVTs and second order effects, thus providing an essential foundation to friendly operations planning and hence the targeting process. Target systems analysis and nodal analysis, conducted within the intelligence preparation of the battlefield or battlespace (IPB) process, not only examines in detail how an adversary's decision making and support systems work, but provides judgments on where they are vulnerable, what they are vulnerable to, how long repairs take, what redundancy is available and systems effects. Additionally, ongoing assessments of adversary capability and intent provide an insight as to the success of friendly targeting activity.

Targeting process

10-6. The targeting process can be characterized by four inherently intertwined functions; decide, detect, deliver and assess (however this is currently under review and may include, in

the future, the modified process of find, fix, finish, exploit and assess). This process helps the commander determine which attack option will be used to engage targets, and which assets will engage them. At all levels of command the planning associated with a successful targeting effort requires close interaction between the commander, operations staff, offensive support planners and intelligence staff.

Decide

10-7. Together, during the decide function, the commander and offensive support staff decide:

a. what targets are to be acquired;

b. when they are to be acquired;

c. what is required to defeat the target; and

d. what damage assessment is required.

10-8. This step identifies threat targets of value and includes:

a. **Developing the target List.** This includes:

(1) **Determining HVTs.** HVT are those assets that the adversary commander requires for the successful completion of his mission.

(2) **Determining HPTs.** HPTs are those high value targets that must be acquired and successfully attacked for the success of the friendly commander's mission.

b. **Target selection standards.** Target selection standards are criteria, applied to adversary activity (acquisitions and battlefield information), used in deciding whether the activity is a target. Target selection standards break nominations into two categories: targets and suspected targets. Targets meet accuracy and timeliness requirements for attack. Suspected targets must be confirmed before any attack. Target selection standards are developed by the fire support element (FSE) or offensive support cell and are given to the intelligence staff. Intelligence analysts use target selection standards to identify targets forwarded to an FSE. Intelligence analysts evaluate the source of the information as to its reliability and accuracy, confirm the size and status of the activity meet the target selection standards, and then compare the time of acquisition with the dwell time which is the length of time a target is doctrinally expected to remain in one location.

c. **Collection plan.** Targets selected should have information requirements developed for unknown or uncertain details. These information requirements are

developed into collection requirements in the Collection Plan and are satisfied through co-ordination with, and tasking of, appropriate sources and agencies.

d. **Attack guidance matrix.** The Attack Guidance Matrix describes which targets are HPTs. It also identifies when and how those targets should be attacked and finally any restrictions placed on attacking those targets.

Detect

10-9. The collection and timely reporting of combat intelligence is key to the success of all targeting missions. The intelligence staff focuses collection (ISR) efforts on named areas of interest (NAI) and target areas of interest (TAI) developed during the IPB process. The IPB products, the Situational Template and the Event Template, help the intelligence staff determine where and when the threat targets can be acquired. The commander develops information requirements that support the detection of threat targets. The organic collection assets available at different levels of command will vary from nation to nation but will consist of a variety of ground and air, manned and unmanned, surveillance and reconnaissance platforms and sensors. Some will provide broad area coverage and others very limited geographical coverage.

10-10. Collection assets generally become more limited at the lower the level of command. Therefore, the intelligence staff must carefully select which asset is assigned to cover which NAI. The intelligence staff should carefully consider the capabilities of his collection assets prior to tasking them. When formulating the Collection Plan, the intelligence staff emphasize depth and redundancy. Depth and redundancy allow targets to be tracked throughout the operation. When a target is first detected, it is immediately passed to the targeting team. The targeting team determines if the target is a high payoff target or if the target meets the engagement criteria. Close coordination is required between the intelligence staff and FSE to ensure all identified targets that meet the targeting criteria are passed accordingly to the element that will affect the target.

10-11. **Deliver.** The delivery activity involves executing the missions decided on by the commander.

Assess

10-12. The assess activity occurs continuously throughout an operation. During assessment, collectors and analysts evaluate the operation’s progress. They adjust the intelligence synchronization plan and analyses based on this evaluation. In addition to assessing changes to their own operations, intelligence personnel look for reports indicating effects on all aspects of the operational environment, including insurgents and civilians. Relevant reporting can come from any intelligence discipline, open sources, or operational reporting. Commanders adjust an operation based on its effects. They may expand the operation, continue it as is, halt it, execute a branch or sequel, or take steps to correct a mistake’s damage. Therefore, an accurate after-action assessment is very important. Metrics may include the following:

a. changes in local attitudes (friendliness towards coalition and host nation (HN) personnel);

b. changes in public perceptions;

c. changes in the quality or quantity of information provided by individuals or groups;

d. changes in the economic or political situation of an area;

e. changes in adversary patterns;

f. captured and killed adversaries;

g. captured equipment and documents;

h. functional damage or degradation assessment ; and

i. assessment of collateral damage.

10-13. **BDA reporting.** For specific lethal operations the effective conduct of BDA requires the timely reporting of the results of these assessments to higher command. BDA reporting consists of three phases by which physical, functional and target system damage assessments are conveyed to all levels of command. The analysis contained in the reports must be read in conjunction with intelligence assessments on the likely adversary response. BDA reports attempt to answer to the following questions:

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

b. What residual capability remains?

c. What level of collateral damage was inflicted?

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

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

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

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

10-14. **First phase reporting.** First phase reporting of mission results is conducted as soon as possible after mission completion, providing commanders with an immediate assessment

that facilitates rapid decisions on the other aspects of combat assessment. First phase reporting is an initial analysis, based primarily on visual or electromagnetic observation of the indicators of effects and is often derived from a single source. The reports from this phase state whether a target was engaged or message received by the intended audience and include, if possible, an initial estimate of effects.

10-15. **Second phase reporting.** Second phase BDA amplifies the initial analysis and, critically, draws on all-source intelligence and operational data to determine the level of perception alteration or physical and functional damage to a target. Second phase reporting will also make an initial estimate of the impact on the target system.

10-16. **Third phase reporting.** Third phase BDA produces a target system assessment by fusing all BDA reporting with the experience of subject matter experts. This provides the commander with an estimate of the remaining capabilities of the targeted system.

CHAPTER 11

INTELLIGENCE SUPPORT TO FORCE PROTECTION

General

11-1. Force protection is the protection of deployed or deploying forces. Measures to counter threats require to be introduced as a result of an ongoing threat assessment process undertaken by the CJ2/intelligence, surveillance and reconnaissance (ISR) staff in conjunction with counter-intelligence (CI) and security intelligence activities. In addition, staffs must consider the force protection implications of working alongside non-adversary groups and the exchange of information with media, non-governmental organizations and other such groups.

11-2. Intelligence support to force protection is based upon a balanced threat assessment resulting from accurate and timely all-source intelligence. This assessment forms the basis for selection of force protection measures. The threat assessment is a continual process. As the situation changes or new intelligence is received, force protection measures must be reviewed and adapted to the new situation and take into account the impact that these may have on information operations (IO) effects.

11-3. In the contemporary operating environment intelligence support to force protection represents a substantial focus of effort. This includes both intelligence and ISR assets in support of activities such as counter-improvised explosive device(s) (C-IED), biometrics, forensics, base protection and convoy operations (eg, route clearance). Other governmental and non-governmental entities are also a major focus for force protection intelligence support.

11-4. As part of mission command, subordinate commanders are to be directed to conduct local reviews and implement operational security (OPSEC) measures, although the overall coordination of force protection will remain under the control of the lead nation headquarters (HQ). It should be remembered the threat could change rapidly; therefore flexible force protection measures are required. In addition, force protection utilizes risk management, not risk elimination, within the context of the campaign end-state. Intelligence support informs these risk decisions.

Counter-intelligence/counter-intelligence surveillance target acquisition and reconnaissance

11-5. A key component of force protection is counter-intelligence/counter-intelligence surveillance target acquisition and reconnaissance (CI/C-ISR). CI/C-ISR protects friendly information while targeting adversary intelligence collection and has both a defensive and offensive function. It is a multi-disciplinary activity that counters the complete range of adversary intelligence collection operations (eg, counter-human intelligence (C-HUMINT), counter-signals intelligence (C-SIGINT), and counter- imagery intelligence (C-IMINT)). It requires coordination and implementation across staff, functional and national boundaries to avoid conflicts of purpose, achieve economy of effort and allow proper source management and development.

11-6. **CI/C-ISR outputs.** The output from CI/C-ISR enables friendly forces to gain dominance over adversary intelligence collection operations. These outputs may include indicators of adversary intent, identified opportunities for exploitation of the adversary's intelligence system and the adversary's capability to conduct all-source intelligence collection. Conversely CI/C-ISR supports the establishment of effective defenses that protect friendly information, forces, personnel, equipment or facilities. These outputs fall into four main areas, these are:

a. **Security intelligence.** This is a specific intelligence output focuses on the identity, capabilities and intentions of hostile organizations or individuals who are or may be engaged in espionage, sabotage, subversion or terrorism. This is key to countering adversary asymmetric activities.

b. **OPSEC measures.** Understanding adversary ISR capabilities and intent assists with the determination of the specific OPSEC measures that might be used to counter those capabilities.

c. **Counter measures to adversary ISR.** C-ISR tasks are those undertaken to degrade opposing forces surveillance, target acquisition and reconnaissance capability. These measures are focused on countering an adversary's intelligence gathering activities and may include input into own deception, Targeting or information operations. In a conventional operation, physical destruction and denial of service may be appropriate. In stability operations, such action may be inappropriate and intelligence staff may need to advise on actions to disguise or screen friendly actions, or confuse opposing force collection.

d. **Monitoring force protection and OPSEC measures.** This helps determine the effect of the force protection and OPSEC measures adopted.

11-11. **CI estimate.** The CI estimate assesses the capabilities and vulnerabilities of the adversary intelligence system and its intentions to exploit friendly vulnerabilities. The estimate is an iterative process that is used to support and inform intelligence preparation of the battlefield or battlespace (IPB), IO, and force protection planning. The CI estimate needs to focus on multi-discipline threats. A CI estimate should:

a. review the situation;

b. provide analysis of the adversary ISR capabilities, intentions and vulnerabilities;

c. consider adversary ISR courses of action (COAs), including likely collection requirements and operations; and

d. recommend CI related targeting options and counter measures to plans and ops tasks, including but not limited to, OPSEC planning and measures to defeat critical elements of the adversary ISR system.

11-12. **CI plan.** The CI plan evolves from the CI estimate and staff interaction with the planning process. The CI plan is produced specific to the level of command and its content is

therefore likely to differ. The CI plan must specify CI tasks, reporting chains, liaison responsibilities, restrictions or legal constraints to CI activities or operations.

11-13. **Coordination and deconfliction.** Co-ordination and de-confliction are essential to ISR but particularly to CI/C-ISR. There will, for instance, be a continual tension between the use of ISR staffs and collection capabilities for general intelligence requirements, as opposed to those for CI/C-ISR. Coordination must occur across staff and functional boundaries where necessary. Particular care must be taken with the co-ordination of HUMINT collection capabilities. Some HUMINT operations are intrusive or particularly sensitive and will require specific approval from nominated commanders, with political sanction possibly being required.

Operational security

11-14. OPSEC seeks to reduce or deny the adversary information concerning friendly dispositions, capabilities, vulnerabilities and intentions both during training and operations. Whilst OPSEC remains the responsibility of the operations staff, it encompasses elements of physical, personnel and field security, as well as communications security, computer security and emission control, which will be supported by the Intelligence staff. In addition, it will include aggressive action against adversary ISR assets. The OPSEC plan will often incorporate psychological operations (PSYOPS) or deception to direct the adversary's attention away from major preparations, movements or other vital parts of an operation that cannot be hidden, and electronic warfare (EW) and physical destruction to counteract or destroy key adversary ISR capabilities. OPSEC may also be influenced by public information and the media.

11-15. Intelligence support for OPSEC planning focuses on the capabilities and limitations of the adversary's ISR capabilities, including the adversary’s decision cycle and any bias towards certain information/intelligence collectors or disciplines. Staff should task their integral Intelligence assets to test the effectiveness of the OPSEC plan once created.

11-16. **Camouflage, concealment and deception.** Intelligence provides key input into the determination of camouflage and concealment and deception measures. The ability to effectively counter adversary surveillance protects all force elements by making the locating and targeting of friendly forces more difficult. Counter-surveillance measures should be part of each formation’s standing operating procedures (SOPs), but overall direction for a coalition operation would normally come from the lead nation headquarters (HQ). This direction is derived from intelligence based on the adversary’s assessed ISR capability.

11-17. **Security of information.** Close co-operation with local/host nation intelligence and security personnel will involve sharing classified information/intelligence. Where the ABCA force uses command information systems (CIS), it must be decided if access to the system is to be given to local/host nation personnel, or whether selected information is to be released via liaison personnel. ABCA field security elements will provide security advice and have an important liaison function. They should be deployed to work with the local/host nation intelligence and security forces.

CHAPTER 12

ELECTRONIC WARFARE

General

12-1. Electronic warfare (EW) is military action that exploits electromagnetic (EM) energy to provide situational awareness and achieve offensive and defensive effects (NATO ATP 3.6.3). EW contributes to both combat and combat support operations in the electromagnetic environment (EME). The effects of operations in the EME must be fully integrated into the battlespace. There are clear linkages between the EW, intelligence, surveillance and reconnaissance (ISR), Counter-radio controlled improvised explosive device (C-RCIED), and the navigation and communications communities. The goal is for these relationships to be routinely strengthened and formalized in capability planning and standing operating procedures (SOP)/tactics techniques and procedures (TTP) development through exercises and experimentation and in operations at all levels, but particularly at the tactical level. The EW Coordination Cell (EWCC) provides the commander with a means to plan, manage, deconflict, integrate, coordinate, control, evaluate and execute EW.

Electronic warfare definitions and capabilities

12-2. **Electronic attack (EA).** EA is the use of EM energy for offensive purposes. EA is employed to destroy, neutralize, deny, degrade, disrupt or deceive an adversary's capabilities and diminish their opportunities to shape or exploit the operational environment. The application of EA is also a form of fires in offensive operations. EA supports exploitation (eg, the 'herding' of communications onto channels more easily exploited or negated). EA is complementary to physical attack. It can engage some targets which cannot easily be engaged by fire, notably area targets (such as communications net) which are not precisely located, or elements of a command and control (C2) system which are moving frequently. EA can cause enemy indecision, confusion or untimely action and should be closely coordinated with the fire plan to achieve the best effect. EA includes directed energy (DE) such as EM pulse and high-power microwaves.

12-3. **Electronic defense (ED).** ED is the use of EM energy to provide protection and ensure effective friendly use of the EM spectrum. In some ABCA nations, the use of EM energy for protection is called defensive electronic attack and ensuring effective friendly use of the EMS is called electronic protect. As a coalition, ABCA, like NATO, will use ED. ED has a key role in defeating RCIEDs and potentially other types of explosive devices. The protection of airborne, sea-borne and increasingly land fighting vehicles relies on ED systems to defeat incoming radio frequency (RF), infra red (IR) and laser guided weapons. Area protection systems such as counter-rocket artillery mortars rely on EM systems such as counter-battery radar and may employ EW with other ISR systems to detect, locate and attack adversaries prosecuting rocket, artillery and mortar attacks.

12-4. **Electronic surveillance (ES).** ES is the use of EM energy to provide situational awareness and intelligence (NATO). The US calls this electronic warfare support while Canada, Australia, and New Zealand call it electronic support. ES is focused on providing

immediate situational awareness and indicators and warning (I&W) of operational activity. ES is not solely concerned with communications but with any EM emission.

Electronic surveillance and signals intelligence

12-5. ES and signals intelligence (SIGINT) are complementary capabilities that differ principally on the basis of their command and control. Where differences between ES and SIGINT arise, they are primarily in relation to the national legal authorities under which their operations are conducted. ES can be a source of SIGINT. Conversely, ES resources may draw upon SIGINT technical data in the performance of ES functions. SIGINT is both an activity (collection of communications intelligence (COMINT) and electronic intelligence (ELINT)) and a product (signals intelligence). ES is a tactical action involving the intercept, processing, exploitation and dissemination of signals, and is a subset of EW. Planners should integrate ABCA SIGINT capabilities into an integrated EW/SIGINT collection plan. Coalition and national regulations strictly govern the transfer of information between coalition force components requiring continual support from national agencies/organizations. A key challenge in information sharing is the management of spectrum information of varying sensitivities, security classifications and caveats.

Information exchange requirements

12-6. Land forces participating in multinational EW operations must exchange EW information with other forces. The information exchange mechanisms must be capable of vertical and horizontal dissemination across all EW task units and intelligence centers. The EWCC will be responsible for coordinating this exchange. Exchanging SIGINT information requires care to avoid violating established security rules. The policy and relationship between EW and SIGINT within ABCA are set out in respective ABCA national policies. While national SIGINT reporting procedures remain extant, there is a requirement for the exchange of SIGINT at the tactical level. Further details are located in the ABCA Standard 2098 Electronic Warfare Operations[1].

Summary

12-7. ABCA Armies must exploit opportunities within the electromagnetic spectrum to attack adversaries, protect friendly forces and partners and continue to build EW capabilities that project EM dominance over adversary efforts. Commanders have to exercise, employ and manage the control of their EW capabilities like any other weapon system. EW activities must be integrated and synchronized with all other battlespace effects in support of operations. EW requires continuous coordination and deconfliction by the EW staff and synchronization with the supporting staff elements (such as spectrum management staff). EW is a key enabler of maneuver, and the provider of situational awareness and force and platform protection. There has been a dramatic increase in the use of EM devices for social, commercial and military purposes, the latter resulting in a significant increase in the number of potential target sets for EW.

Annex:

A. Electronic Warfare Planning and Coordination Checklist

[1] Standard under recommendation for ratification as at Sep 13.

ELECTRONIC WARFARE PLANNING AND COORDINATION CHECKLIST

Planning

a. How will electronic warfare (EW) support the commander's scheme of maneuver?

b. What is the coalition's EW planning and execution coordinating body and who will be the liaisons?

c. What EW collaboration is required with non-ABCA nations and the host nation?

d. What national-level agencies are conducting EW in the coalition area of operation?

e. What EW capabilities are available from joint or other partners?

f. What EW assets are in theatre/may be pushed down or tasked?

g. What is the deployment time frame for EW assets?

h. What are the EW pre-deployment considerations to include EW training requirements?

i. What effect will EW operations have on the host nation and other partners?

j. What are the secondary effects of EW jamming that must be considered?

k. What is the current electromagnetic (EM) operational environment in the area of responsibility to include host nation infrastructure and adversary capabilities?

l. What are the rules of engagement for the coalition applicable to EW?

m. What are the EW effects request procedures from lower echelons?

n. What is the electronic attack or jamming control authority and procedures?

Command and control

a. What are the command and control relationships for coalition EW assets?

b. What is the commander's guidance and rules of engagement for EW?

c. What are the national caveats with regard to EW?

d. What is the tasking process for using coalition assets to support EW operations?

e. What is the procedure to request non-organic capabilities in support of EW?

f. How best can EW capabilities be task organized?

Coordination

a. What are the coalition, host nation and adversary electronic order of battles (EOB)?

b. How will spectrum management coordination and deconfliction be conducted to facilitate EW?

c. What is the information flow requirement for dissemination of EW information to tactical commanders?

d. What are the information flow requirements between non-ABCA member EW capabilities?

e. How will the EW information flow requirements be achieved?

f. How can EW support the commander's Intelligence requirements?

g. Where do I need to place EW liaison officers in non-ABCA member or joint units?

Security considerations

a. What are the EW classification/releasability issues with non-ABCA member units?

b. What are the constraints on the use of EW systems in a coalition environment?

What the restrictions placed on the conduct of EW by coalition national agencies?

CHAPTER 13

BIOMETRICS SUPPORT TO INTELLIGENCE

General

13-1. Commanders are employing biometric capabilities with increasing intensity during operations to identify insurgents, verify local and third-country nationals accessing bases and facilities, and link people to events. Biometrics systems are employed to disrupt threat forces freedom of movement within the populace and to positively identify known threat forces and personnel. These systems collect biometric data and combine them with biographic and contextual information to produce an electronic biometric dossier on the individual. Affixing an individual's identification using his or her unique physical features and forensically linking this identity to the individual's past activities and previously used identities provide more accurate information about the individual. For example, during counterinsurgency operations, biometric collections and forensic exploitation of improvised explosive devices, cache sites, safe houses and vehicles provide commanders additional tools to separate insurgents and criminals from the populace.

13-2. The requirements of national data protection and data control legislation mean that in an ABCA coalition environment, force elements from individual countries will collect, normalise, process, store and disseminate biometric data on separate national systems; the sharing will occur on a national level.

Definitions

13-3. The term *biometric* relates to measurable physical characteristics unique to individuals; commonly used modalities are fingerprints, facial, iris, DNA. The activity *biometrics* is the deliberate, often automated, use of these characteristics to identify individuals, typically for the purpose of security and intelligence.

13-4. Forensic science or *forensics* is the multidisciplinary collection of scientific and technical procedures used to provide a method of identifying and linking people, places, things and events. It is used to recover and analyse trace samples from materiel to identify latent fingerprints, DNA profiles and characteristics of individuals at a scene or event.

13-5. Biometrics enabled intelligence (BEI) is the information associated with and/or derived from biometric signatures and the associated contextual information that positively identifies a specific person and/or matches an unknown identity to a place, activity, device, component, or weapon.

13-6. Biometrics and forensics are combined together with other exploitation capabilities to derive intelligence about an individual's identity; combined they enable a deployed force to accurately identify or verify an individual, who may not wear the uniform of an enemy, from amongst a population and deprive them of their anonymity.

ABCA common biometrics functions

13-7. Whilst each nation conducts the process on their own different equipment, the ABCA nations have agreed five common functional activities required in order to provide biometrics support to intelligence and enhance interoperability:

a. **Collection function.** Force elements require a method of physically collecting biometric data from an individual in a military operation; at its simplest form, this can be traditional ink based fingerprinting, at a more advanced level it is often based on an electronic device that is able to directly capture an individual's biometric information.

b. **Communication function.** Biometric data will normally be collected at multiple distributed points in a theater of operations; robust communications allows for the flow of captured data to a central storage facility and for the flow of information about individuals of interest back to the tactical operator. It can consist of logistic functions where physical items, electronic media or enrolments need to be moved, but in most cases it is the ability for electronic devices to be directly connected to a network bearer.

c. **Matching and storage function.** Normalizing is the process of translating a biometric file into a standard format and specified level of quality. Data is compared with other biometric holdings and forensically derived data, for storage, subsequent exploitation and sharing across the ABCA intelligence community. This may be conducted on a standalone computer database managed by dedicated specialists; however, this function is optimised by a networked reach-back facility with a specialist data repository capable of automated matching and watchlist generation.

d. **Exploitation function.** The exploitation function is enabled by biometrics to contribute to Identity Intelligence. As part of a fused intelligence product it provides decision and targeting support to the commander. At the elementary level this can be achieved in an all source intelligence cell, supplemented by specialists, through a technical facility with scientists, forensic technicians and dedicated intelligence analysts.

e. **Sharing function.** Intra-ABCA sharing allows exploitation to span national boundaries in support of coalition operations and mission success. In order for sharing to occur seamlessly, nations need to conform to the format and processes of the agreed ABCA Standards (currently the US DoD EBTS), associated application profiles, and procedures. Due to individual nation's data sharing legislation it is impracticable to share biometric data as an open automated community. Sharing can be conducted nation-to-nation using bilateral agreements, however as the functionality develops in nations the first point of sharing is likely to be with the US DoD ABIS.

Support to intelligence

13-8. Intelligence-related functions biometrics can support or enhance include: intelligence analysis (including link and pattern analysis); forensic analysis; site exploitation; base access

and local security (to include screening of foreign-national and local-employee hires); force protection; interrogation and detention tasks; high-value target (HVT) confirmation (including high-value individuals and individuals killed in action); population control or census (screening, enrolling, and badging tasks); human intelligence (HUMINT) and counter-intelligence (CI) vetting of sources. Three intelligence products that leverage biometrics are:

a. Biometrics named areas of interest (NAI) are created as part of the standard IPB process. Fused biometric and forensic data informs commanders of the most operationally pertinent locations to conduct biometric collections to effectively capture targets of significance.

b. The Biometric Intelligence Analysis Report (BIAR)[1] is an intelligence product that associates a match between biometric data and an individual in the biometrics database. It is produced by sorting, analysing, and linking the match, the individual's history, and all sources of intelligence. The BIAR contains the identification, background, and assessment of the intelligence value of an individual or operational area of interest. The report is produced from all forensics derived latent marks, other high-threat matches, and matches from specified mission areas.

c. A biometrics enabled watch lists (BEWL) is a compiled lists of individuals of interest. Unlike traditional watch lists (ie, BOLO[2]), a BEWL is created using captured biometric data which can be provided to ground forces and stored electronically on the portable electronic equipment. This enables tactical operators to screen, verify and positively identify individuals when encountered on the ground or at entry control points. The BEWL will contain guidance regarding the subsequent action to be taken, this is often based on categories of response but could be thematic or entirely subject based. A key benefit in intelligence terms is that the BEWL, potentially containing tens of thousands of individuals of interest, can be shared across unit, formation, national and international boundaries, enabling ABCA nations operating in a coalition environment to identify individuals regardless of geography.

Checklist

13-9. Key items for consideration for biometrics support to intelligence:

a. What are the national policies on collection, analysis, fusion, and dissemination of biometrics information?

b. What are the national caveats on data sharing, internally in the coalition, and externally with the host nation?

c. Have the biometrics communications and information systems requirements been made known to the coalition J6 planners?

[1] The Biometric Intelligence Analysis Report (BIAR) is a US product and can be made available to ABCA nations via US Combatant Commanders or US Army National Ground Intelligence Center.
[2] BOLO – Be on the lookout

d. Who will be responsible for managing, including updating and maintaining, the theatre BEI process and production of BEWLs?

e. What are the specific standards, profiles, concept of operations (CONOPS), standard operating procedures (SOPs), intelligence reports and theater standing orders for biometrics? If not present, who can provide?

f. What type of biometrics training/education, at various administrative levels, exists within the military formation?

g. Will in-theater biometric information/data be available to support pre-deployment training?

h. Who will provide the authoritative source for biometrics

CHAPTER 14

HUMAN TERRAIN

General

14-1. Recent experience across the full spectrum of military operations has shown commanders require an understanding of human terrain (HT). In contemporary operations ABCA Armies require the capability to analyze all relevant factors including, but not limited to, political, military, economic, sociological, infrastructure, informational, physical space and time (PMESII-PT) aspects, in order to assist the commanders in the development of knowledge and understanding of the operational environment (OE). This non-traditional threat, non-traditional environment is known as human terrain.

Definitions

14-2. **HT.** Is defined as the social, political, economic and infrastructural environment, belief systems and forms of interaction, of the people who can affect the environment in which soldiers operate.

14-3. **HT analysis (HTA).** Is the analytical process through which an understanding of HT is developed and maintained. It is a continuous process that informs the intelligence preparation of the battlefield (IPB). The output of this process provides understanding and situational awareness to the commander in relation to the OE.

14-4. **HT mapping.** The process of rendering to a geographic map those comparatively static demographic features (eg, population density, age distribution, distribution of income), social features (eg, kinship, ethnicity, religions), or the location of physical items of symbolic and ideological importance (eg, churches, mosques, cemeteries) of a culture. This process seeks to apply collated data on current institutions, historical institutions, spheres of influence, external factors influencing the OE, demographics, social organizations, area, infrastructure, religious factors, key individuals, cultural nuances, societal norms, tolerances and preferences and popular attitudes to geospatial data systems and products as they relate to HT.

14-5. **HT information/data.** Any piece of information, narrative, evidence, statistic or empirical measure, acquired from traditional or non-traditional means, able to be processed into providing HT understanding to the commander.

Human terrain analysis process

14-6. The HTA process is conducted to give the local commander and their troop's greater understanding of the HT and their area of operations. At all levels the standard analytical tools and methods to be used are outlined in JDP 5-00 Campaign Planning (UK) and JDP 3-40 Security and Stabilization: Military Contribution (UK) as well as other single nation equivalent doctrine. These include:

a. **Thematic analysis.** Analyzing information according to themes identified either in the question or the data collected.

b. **Center of gravity analysis.** Used to identify the main area of interest of a group and in so doing highlight potential areas of exploitation.

c. **Strengths, weaknesses, opportunities and threats (SWOT) analysis.** Aimed primarily at groups of people and particularly belligerents. The location population can be subjected to SWOT analysis to improve the understanding of HT.

d. **Network analysis.** Used to identify a network or liaison system between groups of people or individuals.

e. **Pattern analysis.** Used to identify activity patterns including meetings and movements.

f. **Temporal analysis.** Used to establish the relative or comparative timing of activities or incidents.

g. **Geospatial analysis.** Used to identify geographical and physical patterns in activities.

h. **Belief mapping.** Belief mapping is a process to develop an understanding of how a community is organized and what makes it work.

Human terrain and intelligence preparation of the battlefield

14-7. HT is embedded within the IPB from the earliest stages of development. A series of HT overlays and diagrams can be developed during the define the battlefield environment step of IPB, using HTA techniques. The HTA is explained to the commander using the PMESII-PT operational variables and ASCOPE[1] civil considerations.

Human terrain products

14-8. There are a wide variety of HT products available to commanders that can be tailored to individual or operational need. Most important are those that enable decision making. All HT products should be made widely available and written for release across the coalition. Two examples of HT products are an assessment on influential leaders in a district with a high insurgency threat and an association matrix.

Human terrain model

14-9. A HT model is a product of HT mapping that diagrammatically represents HT over which effects based overlays can be placed. It graphically depicts a variety of HT factors derived from PMESII-PT operational variables that can include: human relationships, tribal affiliations and political influences, enabling the Commander to decide how best to affect them.

[1] Areas, structures, capabilities, organizations, people and events within an OE.

Tasking and collection

14-10. Specific HT requests are promulgated as a standard part of the request for information (RFI) process and tasked to sources and agencies (SANDA) including provincial reconstruction teams (PRTs), civil military cooperation (CIMIC) groups, mentoring and liaison teams and female engagement teams (FETs) as required. This pool of sources is not limited to conventional sources and could include any combination of sources within an OE.

14-11. Tasking authority for HT collection resides within respective chains of command. As with any intelligence, surveillance and reconnaissance (ISR) asset, collection management should be conducted through the collection coordination intelligence requirements management (CCIRM) process. HT collectors follow the collection plan; however, they need the freedom to use non-traditional channels to acquire HT information.

14-12. There may be certain legal, ethical and security consideration to the collection of some elements of the HT information. As with traditional HUMINT collection, broader HT collection must be de-conflicted through the J2X. Within a coalition environment care must also be taken to deconflict HT tasking between national elements.

14-13. Certain nations have the ability to reach back to academic professionals who have the ability to provide analytical support to deployed HTT. This information should be shared with coalition partners.

Responsibilities

14-14. The employment of dedicated HTTs does not remove the requirement for military forces to understand the nuances of culture as it pertains to the OE. It is important that HTTs engage with all elements deployed to educate military personnel on the role and function of HTTs and what they can provide to command teams.

14-15. HTA is designed to be compliant with the intelligence cycle and existing collection management (CM) mechanisms operating through or in close conjunction with the J2 staff. It is vital that HTA be command led and tasked through the CM process.

GLOSSARY OF TERMS AND ACRONYMS

TERM	ACRONYM	DEFINITION
Access		The function of drawing on available information and intelligence.
Acoustic intelligence	ACINT	Intelligence derived from the collection and processing of acoustic phenomena (NATO AAP-6 – NATO Glossary of Terms and Definitions).
Admiralty Grading System		An alphanumeric indication of the degree of confidence that may be placed in an item of information.
Acoustic weapon locating	AWL	
All source cell	ASC	
All source intelligence		Intelligence produced using all available sources and agencies (AAP-6).
Analysis		In intelligence usage, a step in the processing phase of the Intelligence Cycle in which information or intelligence is subjected to review in order to identify significant facts for subsequent interpretation. See also - Intelligence Cycle (AAP-6).
Areas, structures, capabilities, organizations, people and events	ASCOPE	
Area of intelligence interest	AII	The area concerning which a commander requires intelligence on those factors and developments likely to affect the outcome of his current and future operations. (AAP-6)
Area of intelligence responsibility	AIR	The area allocated to a commander for which he is responsible for the provision of intelligence within the means at his disposal. (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)
Avenue of approach	AA	Ground that normally includes a number of mobility corridors, over which forces can advance to contact.
Area of operations	AO	
Basic intelligence		Intelligence, on any subject, which may be used as reference material for planning and as a basis for processing subsequent information or intelligence (AAP-6).
Battle damage assessment	BDA	
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.
Biometric Intelligence Analysis	BIAR	The Biometric Intelligence Analysis Report (BIAR) is a

TERM	ACRONYM	DEFINITION
Report		US product and can be made available to ABCA nations via US Combatant Commanders or US Army National Ground Intelligence Center.
Biometrics enabled intelligence		
Center of gravity	COG	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)
Chemical, biological, radiological and nuclear	CBRN	
Coalition		A grouping of nations or forces, usually on a temporary basis, for the accomplishment of a stated goal.
Coalition intelligence fusion center	CIFC	The ABCA CIFC is a '5 EYES' organization within a land component HQ.
Coalition Intelligence Handbook	CIH	
Coalition Health Interoperability Handbook	CHIH	
Coalition Logistics Handbook	CLH	
Coalition Operations Handbook	COH	
Coalition intelligence architecture		The ABCA Coalition Intelligence Architecture will consist of the personnel, organizations, policy and procedures, information technology (IT) and communications and other means of dissemination to effect the complete execution of the intelligence cycle and other processes.
Collation		In intelligence usage, 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. See also Correlation and Intelligence Cycle (AAP - 6).
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)
Collection assets		
Collection management	CM	In intelligence usage, the process of converting Intelligence Requirements into Collection Requirements establishing, tasking or co-ordinating with appropriate collection sources or agencies, monitoring results and retaking, as required (AAP - 6).
Collection plan		A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and re-quests to appropriate agencies (AAP-6).
Combat information		That frequently perishable data gathered in combat by, or reported directly to, units which may be immediately used in battle or in assessing the situation. Relevant data will simultaneously enter intelligence reporting channels (AAP-6).

TERM	ACRONYM	DEFINITION
Combat service support	CSS	
Combined		In concert with the forces of another nation of the NATO Alliance.
Commander's critical information requirements	CCIR	
Communications and information systems	CIS	Assembly of equipment, methods and procedures, and if necessary personnel, organized so as to accomplish specific information conveyance and processing functions (AAP-6).
Communications intelligence	COMINT	Technical material and intelligence information derived from electromagnetic communications and communications systems (eg morse, voice, teleprinter, facsimile) by other than intended recipients (AAP-6).
Computer security		
Concept of operations	CONOPS	A clear and concise statement of the line of action chosen by a commander in order to accomplish his mission (AAP-6).
Conventional directed activity	CDA	
Correlation		In intelligence usage, the process which associates and combines data on a single entity or subject from independent observations, in order to improve the reliability or credibility of the information (AAP -6).
Counter-espionage		Action designed to detect and counteract espionage (AAP-6).
Counter-intelligence	CI	Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion or terrorism (AAP-6).
Counter-intelligence, surveillance and reconnaissance (ISR)		Activities undertaken to identify, quantify, determine the intent of, and counteract an adversary's ISR capability.
Counter-improvised explosive device	C-IED	
Counter-sabotage		Action designed to detect and counteract sabotage (AAP-6).
Counter-subversion		Action designed to detect and counteract subversion (AAP-6).
Counter-surveillance		All measures, active or passive, taken to counteract hostile surveillance (AAP-6).
Counter-terrorism		Action designed to detect and counteract terrorism.
Course of Action	COA	
Current intelligence		Intelligence which reflects the current situation at either strategic or tactical level (AAP-6).
Deception		Those measures designed to mislead the enemy by manipulation, distortion or falsification of evidence to induce him to react in a manner prejudicial to his interests (AAP-6).

TERM	ACRONYM	DEFINITION
Decision line	DL	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.
Decision point	DP	A point on the ground where a commander must make a decision if he is to effect a result at a particular Target Area of Interest.
Directed energy weapons	DEW	
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)
Electro-magnetic environment	EME	
Electro-magnetic spectrum	EMS	
Electronic counter measures	ECM	That division of EW involving actions taken to prevent or reduce an enemy's effective use of the EMS through the use of electromagnetic energy (AAP-6).
Electronic intelligence	ELINT	Technical material and Intelligence Information derived from electromagnetic non-communications transmissions (e.g. radar, navigational aids, jamming transmissions) by other than intended recipients (MC 101).
Electronic protection measures	EPM	That division of EW involving actions taken to ensure effective friendly use of the EMS despite the enemy's use of electromagnetic energy (AAP-6).
Electronic support measures	ESM	The division of EW involving actions taken to search for, intercept and identify electromagnetic emissions and to locate their sources for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving electronic countermeasures, electronic protective measures and other tactical actions (AAP-6).
Electronic warfare	EW	Military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum and action to retain its effective use by friendly forces (AAP - 6).
Emission control	EMCON	Selective control of emitted electromagnetic or acoustic energy (AAP-6).
Espionage		The collection of information by secret means for intelligence purposes
Evaluation		In intelligence usage, a step in the processing phase of the intelligence cycle constituting appraisal of an item of information in respect of (a) the reliability of the source and (b) the credibility of the information.
Field human terrain (HUMINT) team	FHT	
Field security		

TERM	ACRONYM	DEFINITION
Force protection		Force protection is the means, resources and measures available to the commander to protect his assets. It is a national responsibility which commences at the strategic level and extends down to the operational level, through to the tactical. The Joint Force Commander applies force protection within his area of responsibility in cooperation with the host country and allied forces. Means, resources and measures of security are essential in achieving force protection.
Foreign intelligence service	FIS	
Geospatial intelligence	GEOINT	
Geographic information system	GIS	
Hostile intelligence services	HIS	These are the enemy's or the potentially hostile forces intelligence services.
Host nation	HN	
Human intelligence	HUMINT	A category of intelligence derived from information collected and provided by human sources (AAP-6). HUMINT can be achieved either in a covert (clandestine) or in a non-covert operation.
Human terrain analysis	HTA	
High payoff targets	HPTs	High value targets that must be acquired and successfully attacked for the success of the friendly commander’s mission.
High value target	HVT	
Imagery intelligence	IMINT	Imagery intelligence is derived from imagery acquired by photographic, radar, electro-optical, infra-red and thermal sensors, which can be ground based, sea borne or carried by overhead platforms.
Indicators and warning	I&W	
Information		Unprocessed data of every description which may be used in the production of intelligence. See also Intelligence Cycle (AAP - 6).
Information operations	IO	
Information requirements		Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander (AAP-6).
Integration		In intelligence usage, a step in the processing phase of the intelligence cycle whereby analyzed information and/or intelligence is selected and combined into a pattern in the course of the production of further intelligence See also Fusion (AAP -6).
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).
Intelligence cycle		The sequence of activities whereby information is

TERM	ACRONYM	DEFINITION
		obtained, assembled, converted into intelligence and made available to users (AAP-6). This sequence comprises the four phases of Direction, Collection, Processing and Dissemination.
Intelligence collection plan	ICP	
Intelligence estimate		The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption (AAP-6).
Intelligence management plan	(IMP)	
Intelligence preparation of the battlefield/space	IPB	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.
Intelligence preparation and monitoring of the battlespace	IPMB	
Intelligence requirements	IR	Those items of intelligence required by a commander in order to conduct current operations and to plan future ones.
Intelligence, surveillance and reconnaissance	ISR	See below
Intelligence, surveillance, reconnaissance and target acquisition.	ISTAR	The co-ordinated acquisition, processing and dissemination of timely, accurate, relevant and assured information and intelligence which supports the planning, and conduct of operations, targeting and the integration of effects.
Interpretation		In intelligence, the final step in the processing phase of the intelligence cycle in which the significance of information and/or intelligence is judged in relation to the current body of knowledge. The term can also be used in its more usual sense of translating raw data into a more intelligible form - for example as in imagery interpretation. See also Intelligence Cycle (AAP - 6)
Joint integrated prioritized target list	JIPTL	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.
Joint target list	JTL	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.
Measurement and signature intelligence	MASINT	Scientific and technical intelligence derived from the analysis of data obtained from sensing instruments for

TERM	ACRONYM	DEFINITION
		the purpose of identifying and distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification (AAP-6).
Military intelligence	MI	
Military geospatial information	MGI	
Mobility corridor	MC	An area of ground which the maneuver capability of particular forces being considered can equate to its doctrinal norms.
Named area of interest	NAI	An area or point from which intelligence could confirm or deny the threat's intentions or limitations.
National intelligence cell	NIC	
Near real time		Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communications and automatic data processing. This implies that there are no significant delays. See also real time (AAP-6).
Near real time	NRT	
Operational environment	OE	
Operational security	OPSEC	
Observation posts	OP	A post from which military observations are made, or fire directed and adjusted on the basis of observation (AAP-6).
Open source intelligence	OSINT	Intelligence derived from publicly available information, as well as other unclassified information that has limited distribution or access (AAP-6).
Operational command	OPCOM	The authority granted to a commander to assign missions or tasks to subordinate commanders, to deploy units, to reassign forces, and to retain or delegate operational and/or tactical control as may be deemed necessary. It does not of itself include responsibility for administration or logistics (AAP-6).
Operational control	OPCON	The authority delegated to a commander to direct forces assigned so that the commander may accomplish specific missions or tasks which are usually limited by function, time or location; to deploy units concerned, and to retain or assign tactical control of those units. It does not include authority to assign separate employment of components of units concerned. Neither does it, of itself, include administrative or logistic control (AAP-6).
Operational level of command		The level of war at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objectives within theaters or areas of operations. (AAP-6)
Operations security	OPSEC	The process which gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the

TERM	ACRONYM	DEFINITION
		dispositions, capabilities, and intentions of friendly forces (AAP-6).
Order of battle	ORBAT	The identification, strength, command structure and disposition of the personnel, units and equipment of any military force. (AAP-6)
Peace support operations	PSO	Multi-functional operations involving military forces and diplomatic and humanitarian agencies. They are designed to achieve humanitarian goals or a long term political settlement and are conducted impartially in support of an appropriate mandate. Includes peacekeeping, peace enforcement, conflict prevention, peacemaking, peace building and humanitarian operations. (UK definition)
Personnel security		
Physical security		That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage and theft (AAP-6).
Political, military, economic, sociological, infrastructure, informational, physical space and time	PMESII-PT	
Priority intelligence requirements	PIR	Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision making (AAP-6).
Processing		The conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation (AAP-6).
Protective security		The organized system of defensive measures instituted and maintained at all levels of command with the aim of achieving and maintaining security (AAP-6).
Psychological operations	PSYOPS	
Real time		Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. See also near real time (AAP -6).
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 (AAP-6).
Request for information	RFI	
Rules of engagement	ROE	Directives issued by competent military authority which specify the circumstances and limitations under which force will initiate and/or continue combat engagement with other forces encountered. (AAP-6)
Sabotage		The intentional destruction, disruption or disabling of

TERM	ACRONYM	DEFINITION
		equipment, material or facilities by or for a hostile element.
Security		The condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure. The term is also applied to those measures necessary to achieve this condition and to the organizations responsible for those measures (AAP-6).
Security intelligence	SI	Intelligence on the identity, capabilities and intentions of hostile organizations or individuals who are or may be engaged in espionage, sabotage, subversion or terrorism (AAP-6).
Signals intelligence	SIGINT	A generic term used to describe COMINT and ELINT when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two (MC 101).
Situational awareness	SA	The understanding of the operational environment in the context of a commander's (or staff officer's) mission (or task). (UK definition)
Source		In intelligence usage, a person from whom, one thing from which, information can be obtained (AAP-6).
Sources and agencies	SANDA	
Strategic intelligence		Intelligence which is required for the formation of policy and military plans at national and international levels (AAP-6).
Subversion		Action designed to weaken the military, economic or political strength of a nation by undermining the morale, loyalty or reliability of its citizens (AAP-6).
Standing operating procedures	SOP	A set of instructions covering those features of operations which lend themselves to a definite or standardized procedure without loss of effectiveness. The procedure is applicable unless ordered otherwise.
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)
Surveillance		The systematic observation of aerospace, surface on subsurface areas, places, persons or things by visual, aural, electronic, photographic or other means (AAP-6).
Surveillance and target acquisition	STA	
Synthetic aperture radars	SAR	
Tactical command		
Tactical control	TACON	
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)
Tactics, techniques and	TTP	

TERM	ACRONYM	DEFINITION
procedures		
Target		In intelligence usage, a country, area, installation, agency or person against which intelligence activities are directed (AAP-6).
Target acquisition	TA	The detection, identification and location of a target in sufficient detail to permit the effective employment of weapons (AAP-6).
Target area of interest	TAI	An area where the commander can influence the battle by destroying, delaying or disrupting threat or targeted forces.
Target intelligence		Intelligence which portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance (AAP-6).
Targeting		The process of selecting targets and matching the appropriate response to them taking account of operational requirements and capabilities.
Task force	TF	
Tearlines		An automated or manual technique for separating an intelligence report into multiple portions separated by machine-or-human-readable tearlines. A tearline section is the area in an intelligence report or finished intelligence product where the sanitized version of a more highly classified and/or controlled report is located.
Technical intelligence	TECHINT	Intelligence concerning foreign technological developments and the performance and operational capabilities of foreign material, which have or may eventually have a practical application for military purposes. (AAP-6)
Terrorism		The unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, ethnic, religious or ideological objectives. (AAP-6)
Unattended ground sensors	UGS	
Unmanned aerial vehicle	UAV	A powered aerial vehicle that does not carry a pilot, uses aerodynamic forces to provide vehicle lift and can fly autonomously or be piloted remotely. (UK definition)
Weapon locating radar	WLR	

Solving Coalition Interoperability since 1947

Visit www.abca-armies.org to get your copy