THE AUSTRALIAN ARMY

Army

Land Warfare Doctrine 2-0

Intelligence
2018

This publication supersedes *Land Warfare Doctrine 2-0, Intelligence*, 2014.

Serving our Nation

Contents

Contents

Contents

Introduction 5

Chapter 1. Intelligence theory...7

Chapter 2. Intelligence cycle..11

Chapter 3. Intelligence responsibilities and organisation 15

Components...17

Intelligence staff 18

Chapter 4. Intelligence disciplines 23

Chapter 5. Intelligence activities 25

Conclusion 31

References 33

Endmatter 35

Illustrations..35

Tables 35

Introduction

> *'If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.'*
>
> ***Sun Tzu*[1]**

An intelligence failure is when intelligence is not timely, accurate or readily available for use by commanders. Such failures unnecessarily risk individual engagements, operations and blue force casualties. Meanwhile operational success is attributable to the targeted application of the complete Australian Defence Force, Australian whole-of-government and coalition intelligence apparatus (known as the intelligence enterprise), combined with the integration of intelligence and operations throughout the planning and operation cycle.

To ensure that Army remains a dominant land force, a focused intelligence enterprise that facilitates situational understanding and supports the commander in decision-making is required. *Land Warfare Doctrine 2-0, Intelligence* provides the foundation doctrine for that intelligence effort. This publication outlines the nature of intelligence support to land operations and the common construct for intelligence operations.

The principal audience of this publication is all members of the profession of arms. It has been written to provide a clear overarching understanding of intelligence operations in the land domain. Where greater detail on intelligence duties, roles and responsibilities is needed, *Land Warfare Doctrine 2-1, Intelligence Staff Duties* is to be read. Similarly, commanders, staff and intelligence professionals serving at joint headquarters or on joint task forces should read *Australian Defence Doctrine Publication 2.0, Intelligence*.

For the purpose of this publication the term 'threats' includes all enemies and adversaries that are active in the operating environment. The term 'hazards' refers to conditions or natural phenomena able to injure or kill, damage or destroy vital resources and institutions, or prevent achievement of the mission.

[1] Giles, L 2007, *The Art of War by Sun Tzu*, Special Edition, Special Edition Books, United States.

Chapter 1

Intelligence theory

Intelligence in a land context is the product of knowledge and understanding of the capabilities and intentions of an actual or potential threat or any other forces with which the Army is concerned, as well as the associated terrain and weather. Intelligence is fundamental to the planning and conduct of operations through all dimensions of conflict as it allows the commander to gain control of the threat and mastery of the environment, consequently reducing risk.

The development of effective intelligence first requires an understanding of its fundamental nature – its purpose and characteristics as well as its relationship with the commander and key staff.

Intelligence versus information

In different contexts the term ‘intelligence’ can refer to the organisation performing the intelligence staff function, the activity associated with the conduct of the intelligence function or, more commonly, the product or output that fulfils the role and aims of the function. There is an inherent distinction between information and intelligence:

- *Information.* Information is unevaluated data that has been processed to provide meaning but has not been analysed with respect to implications for the operation.
- *Intelligence.* Intelligence is the product of the processing of information concerning individual and group beliefs, customs and norms; foreign governments; hostile or potentially hostile forces or elements; and battlespace environments specific to areas of actual or potential operations. On all counts, intelligence provides an intended audience with a product which is designed to assist in the decision-making process and which directly impacts future actions. There are three types of intelligence:
    - *Baseline intelligence.* Baseline intelligence is intelligence on any subject that may be used as reference material for planning and as a basis for processing subsequent information or intelligence.
    - *Current intelligence.* Current intelligence is processed information that reflects the current situation at the strategic, operational or tactical levels.
    - *Estimative intelligence.* Estimative, or predictive, intelligence is that which is forward looking, identifying, describing and forecasting adversary capabilities and the implications for planning and executing Australian Defence Force operations.

The role of intelligence

The role of intelligence is to provide the commander with as thorough a knowledge of the battlespace as possible. Uncertainties and the fog of war have affected commanders throughout the history of warfare, impinging on clear decision-making and placing the outcomes of combat at risk. The ability to clear that fog and remove uncertainties through the provision of timely and accurate assessment is the mission of intelligence. Through good application of intelligence procedures commanders are provided with answers to their specific intelligence requirements, while accurate and timely situational assessment leads to decision superiority over the threat, the generation of tempo, and the ability, therefore, to seize and retain the initiative.

Intelligence informs the commander of changes to the threat and the environmental situation, enabling decision advantage and enhanced lethality.

Principles of intelligence

The organisation, activities and production of intelligence are optimised by several guiding principles. Fundamental to these principles is the fullest possible understanding of the adversary. This includes knowledge of the adversary’s goals, objectives, strategy, intentions, capabilities, method of operation, vulnerabilities, and sense of value and loss, combined with a clear understanding of the historical methods and means by which they have conducted full-spectrum war. Intelligence staff must understand the adversary’s character, culture and customs. They must develop and continuously refine their ability to think like the adversary in order to advise on the adversary’s likely perceptions, reactions and responses to friendly actions.

Commander’s role. The commander provides direction for the intelligence effort and determines priority intelligence requirements. That prioritisation then drives the intelligence effort and stimulates intelligence, surveillance and reconnaissance processes to satisfy collection requirements.

Centralised 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 staff and agencies.

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

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

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

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

Timeliness. Information or intelligence must be available in a timely fashion to enable maximum benefit from its use.

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 that are inevitable in assessments and must not imply a false degree of confidence.

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 a rapid and flexible response to queries.

Source protection. In the information collection process 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 the dissemination of intelligence, sources and methods must be protected to avoid compromise and the subsequent loss of collection ability.

Balance. The principle of ‘balance’ in intelligence is multifaceted, from the balanced structure of intelligence specialities versus combat intelligence staff through to an appropriate balance being struck between the requirement to protect sources and at the same time ensure the widest possible dissemination of intelligence to those with a ‘need to know’. Balance is also required between collection and production and between competing customer demands. A balance must also be struck and a clear distinction made between fact and judgement (assessment) in intelligence reporting.

User awareness and confidence. Intelligence organisations and staff need to liaise closely with customers in order to ensure that their requirements are clearly understood and continue to be met in a timely and preferred manner. Intelligence organisations and staff must have a high degree of confidence that customer requirements are being met, not only in terms of the finished product but also in terms of collection requirements being satisfied and intelligence databases being maintained to support the intelligence capability.

Characteristics of effective intelligence

Effective intelligence is intelligence that meets the commander's needs and supports the commander's mission, concept of operations and information requirements. To this end, intelligence products must meet the following requirements:

- *Relevance.* Intelligence must support the commander's mission, concept of operations and information requirements.
- *Usability.* Intelligence products must be in a format that can be easily used and highlights the significance of the information or intelligence they contain.
- *Timeliness.* Intelligence products must be available in sufficient time to enable decisions to be made and executed.
- *Accuracy.* Intelligence should be cross-referenced against reporting for context and validation, with suitable indications of the intelligence staff's confidence in the assessment provided.
- *Objectivity.* Intelligence must be unbiased, undistorted, and free from influence or constraints. Intelligence methodology and products must not be directed or manipulated to conform to a desired result, preconceptions of a situation or an adversary, a predetermined objective or an institutional position.
- *Availability.* Intelligence must be readily available to those who need it.
- *Completeness.* Intelligence should be as complete as possible, based on all the information available to answer customers' requirements, and provide a full understanding of the situation.
- *Clarity.* Intelligence should be clearly presented to avoid the chance of misinterpretation by the user.
- *Format.* Intelligence analysis must be presented and transmitted in a format that can be integrated quickly and sustainably into each target node within the battlespace. Bearer constraints and data storage capacity at each supported node must be understood to ensure that reports reach the target audience within the required time frame and without degrading or overwhelming information technology systems throughout the battlespace.

Chapter 2

Intelligence cycle

The intelligence cycle (see Figure 2–1) 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 involves four phases of activity:

- direction
- collection
- processing
- dissemination.

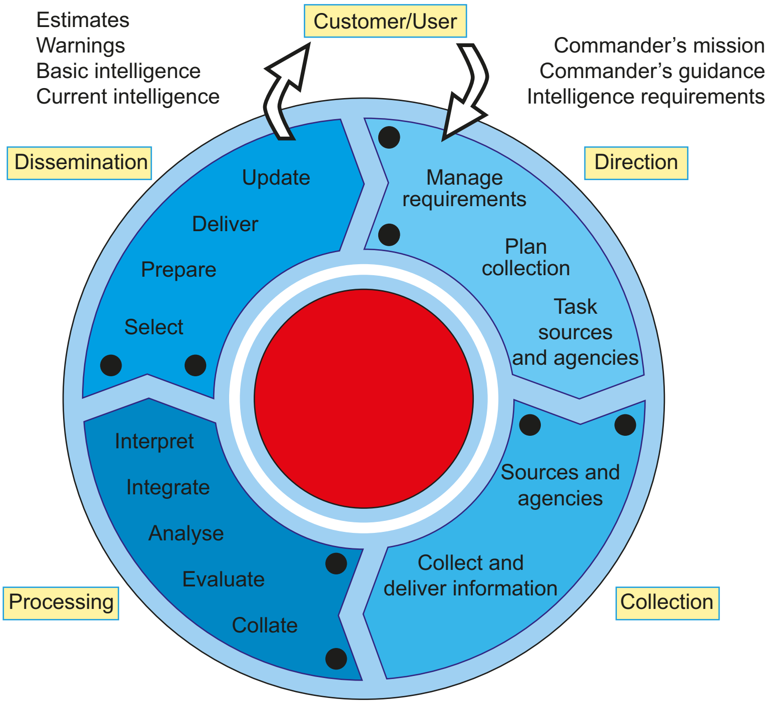

Figure 2–1: The intelligence cycle

The purpose of 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 of the battlespace. Intelligence preparation of the battlespace is the intelligence staff process designed to provide critical inputs to staff planning, known as the military appreciation process. Its principal function is to analyse the operational environment, provide the intelligence estimate, and assist in collection planning. Intelligence preparation of the battlespace is discussed in detail in *Land Warfare Doctrine 5-1-4, The Military Appreciation Process*.

The intelligence process 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.

Direction

As intelligence facilitates operations and the commander directs operations, the commander correspondingly provides direction to the conduct of intelligence collection operations (intelligence). This connection ensures that intelligence is an inherent and essential responsibility of command.

Commander's guidance and direction is necessary to ensure that intelligence operations support the mission, intent and concept of operations. This direction is most often given as a series of questions, known as information requirements, concerning adversaries, hazards and/or the environment.

The intelligence cycle forms the framework of the intelligence system.

Collection

Collection is the synchronised exploitation of sources and agencies to meet a commander's information requirements. Successful collection activities result in the timely reporting of relevant and accurate information, which supports the production of intelligence.

Collection is a continuous activity and is controlled and coordinated at the highest practical level using a collection management system specific to the theatre of operation. Collection activities must be methodically planned to ensure the best use of scarce collection assets. The specifics of collection management are provided in *Land Warfare Doctrine 2-1, Intelligence Staff Duties* and *Australian Defence Doctrine Publication 3.7, Collection Operations*.

Processing

Processing is the production of intelligence through the collation, evaluation, analysis, integration and interpretation of collected information and existing intelligence. This involves analysts making assessments and recommendations in response to information requirements or anticipated requirements.

Collation. Collation involves the logging and recording of incoming information to ensure its accessibility for future use and exploitation. This includes database integration, geodetic storage, map and chart marking, electronic or manual filing and cross-referencing.

Evaluation. Evaluation is conducted using the Admiralty Grading System (see Table 2–1) and determines the likelihood that a piece of information is correct through assessing the credibility of the information and the reliability of the reporting source or agency. The Admiralty Grading System is an alphanumeric system that indicates the degree of reliability of the source or agency as a letter ranging from A to F, and the degree of credibility of the information as a number ranging from 1 to 6. The combination of a letter and number provides an assessed evaluation grading for each item of information.

Table 2–1: 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

Analysis. Intelligence analysis is the process by which collected information is examined in detail, its component facts are separated from inference, and it is integrated with existing information to facilitate intelligence production.

Intelligence analysis involves critical and creative thinking that is disciplined and self-reflective. Such analysis embraces ambiguity: it recognises and mitigates biases, challenges assumptions, and continually learns. Analysts actively share and question information, perceptions and ideas to better understand situations and produce intelligence.

Integration. Integration involves the consolidation of component parts of information, isolated during the analysis, with other information and previously produced intelligence. This process of grouping like fact or inference reveals patterns and relationships that form 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 of information from a wide range of sources and agencies, and is often referred to as fusion.

Interpretation. Interpretation is crucial as it is the overall assessment activity of the intelligence process. 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.

Dissemination

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. Commanders require intelligence products on time and in an appropriate format to facilitate situational understanding and support decision-making. The timely dissemination of intelligence may be critical to the success of operations.

Select. The selection of relevant information and intelligence requires thorough knowledge of the commander's information requirements, the operational plan and the situation. Intelligence staff must be aware that the absence of information or intelligence about threats or the environment may be as worthy of selection for dissemination as its presence.

Prepare. 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 a compromise may be needed between medium and content to ensure timely delivery. Where possible, intelligence should be sanitised in accordance with security instructions to allow dissemination to the lowest practical level, and downgrading instructions should be included.

Deliver. The intelligence principle of timeliness encompasses not only the time required for processing and dissemination but also 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 needs to be passed by the fastest means possible, basic intelligence will usually be of low priority. Information and intelligence should be disseminated by secure means consistent with its security classification and the intelligence principle of source protection. Distribution within a hierarchical system requires that the originator determines who is to receive the intelligence and by what means. While a fully functional distributed system or pull system provides instant access to any product in the system, the originator's responsibility for dissemination does not extend beyond placing the intelligence onto the system within the required time frame.

Chapter 3

Intelligence responsibilities and organisation

Intelligence activity has three key aspects or components:

- the intelligence staff functions encompassing the intelligence staff process that provides input to decision-making processes, intelligence planning, liaison, requirements, collection management and the management of intelligence assets and operations
- the production function, also referred to as the ‘agency function’, which involves the output of intelligence products (in the land environment this is considered part of the staff function)
- the conduct of intelligence operations encompassing those operations conducted by intelligence personnel for information collection or counterintelligence purposes.

Framework

The intelligence architecture constitutes the organisational framework, infrastructure and arrangements necessary to support these three key components. Well-considered intelligence architecture will identify functions, personnel resources and systems in advance of operational deployment and will be articulated in the intelligence support plan.

The planning and design of the intelligence architecture must be conducted in conjunction with the planning of the particular campaign, operation or activity that it is supporting. Additionally, the structure must be flexible to meet the changing operational requirements. The resulting intelligence arrangements must describe requirements for intelligence staffing over each operational phase, the tasking authorities for all collection operations and processing activities, and the links to superior, subordinate and flanking commands.

The division of responsibilities between the Australian intelligence community (a detailed synopsis of which can be found in *Australian Defence Doctrine Publication 2.0, Intelligence*) and strategic, operational, theatre and tactical headquarters is important when considering early deployment, collection planning, intelligence support plans, command relationships and intelligence crossover points, and intelligence, surveillance and reconnaissance support plans.

Early deployment. Deployment of the full intelligence support elements may be phased, but the commander of a joint interagency task force or task group must ensure that there is a viable intelligence organisation at the outset of an operation, and the operational movement plan must reflect this need. Where operations or contingency planning is constrained by limited information, the early deployment of collection assets is often vital. Such deployment may need to precede the deployment of the main force.

Collection planning. Effective collection planning requires the capabilities, limitations and availability of the collection assets to be balanced against the requirement to answer the commander’s information requirements. This is achieved through the implementation of the intelligence principles of centralised control, systematic exploitation, responsiveness and source protection. These principles will ensure that collection planning is provided the benefits of an economy of effort, the control of source workload, and ongoing source evaluation and development. Collection planning is a continuous process and one that requires agility and responsiveness to changing information requirements, a changing operational situation and ongoing environmental impacts on collection.

Intelligence support plan. The intelligence support plan is the medium for articulating the intelligence architecture and directing the intelligence effort appropriate to meet the threat and information requirements identified in the intelligence preparation of the battlespace. The intelligence support plan may be issued separately or as an intelligence annex to an operation order or operations instruction. In addition to establishing the intelligence architecture, liaison, the reporting framework and coordination arrangements, the intelligence support plan focuses, prioritises and initiates intelligence and counterintelligence activity in support of identified information requirements and counterintelligence aims. Counterintelligence guidance may be issued separately in a counterintelligence plan. In short, the intelligence support plan must provide enough specific information for subordinate, lateral and supporting commands to start operating.

Command relationships. The division of staff and production responsibility between each level of command and national agency needs to be clearly articulated in the intelligence support plan. This plan includes assignment of responsibility for the production of estimates, plans and threat assessments. As the operation progresses through various phases, the division of responsibility will change. This occurs at what are known as intelligence crossover points.

Intelligence crossover points. An intelligence crossover point is the nexus at which one component of an intelligence system assumes primacy. Crossover is recognition that, as the activity or operation matures; the most appropriate organisation to conduct various parts of the intelligence cycle will change. This change is best effected if it is agreed in advance and promulgated in the intelligence support plan. Acceptance of primacy for intelligence support to an activity at the operational level may not equate to primacy for analysis and production at the strategic level.

Intelligence, surveillance and reconnaissance support plan. The intelligence, surveillance and reconnaissance plan is an integrated function of intelligence and plays a vital role in meeting the commander’s requirements. It articulates where deployed land intelligence, surveillance and reconnaissance assets fit into the larger Australian intelligence community and the coalition intelligence, surveillance and reconnaissance enterprise. It also provides a systemic approach to intelligence, surveillance and reconnaissance in support of a tactical commander's requirements. Although this architecture is variable for each deployment, its conceptual framework is described in *Australian Defence Doctrine Publication 3.7, Collection Operations* and *Land Warfare Doctrine 2-2, Intelligence, Surveillance and Reconnaissance*.

Components

Defence intelligence system

Intelligence staff and agencies at all levels operate as part of a distributed intelligence system; that is, each element contributes information and intelligence to the system according to its capabilities and allocated responsibility for intelligence production. The various elements also draw on the system according to their needs.

The defence intelligence system encompasses joint, single-Service and Defence intelligence elements, activities and procedures. It spans the spectrum of command and the spectrum of conflict by providing an intelligence capability and structure to support operations in peace, crisis and conflict.

Land intelligence

Although land intelligence support is available to commanders at all levels, its composition and capabilities are dependent on the objectives and constraints of each specific mission and may consist of all or any of the following:

- *Specialist intelligence.* During major conflict or prolonged operations offshore or in defence of Australia, a specialist intelligence capability may need to be deployed in support of the commander. Such intelligence support is known as an intelligence support element, and it must be provided without detriment to the commander's combat intelligence capability. If required, an intelligence support element could be combined with Royal Australian Navy and Royal Australian Air Force specialist intelligence capabilities into a force intelligence group.
- *Combat intelligence staff.* Like their strategic and operational counterparts, tactical intelligence organisations and staff provide combat intelligence support to the tactical commander. In contrast, however, these intelligence staff and organisations will usually not be joint. The composition of the tactical combat intelligence capability will be determined by the level and organisation of the headquarters it supports.
- *All-source cell.* The mission of the all-source cell is to focus collection resources and to produce and disseminate intelligence to support the commander's decision-making process. The all-source cell works for the senior intelligence officer at the supported headquarters, who directs its

effort according to the commander’s guidance. The all-source cell supports current operations and contingency planning simultaneously.

Intelligence staff

Functions

The intelligence staff are responsible for assessing the capabilities, vulnerabilities and intentions of entities outside the positive control of friendly forces. They are also responsible for providing specialist and combat intelligence advice to planning.

Intelligence staff must at all times provide predictive, comprehensive and unbiased assessments. Intelligence staff are vital to the process of ensuring that decision-makers at all levels are aware of the facts, assessments and gaps in intelligence.

Responsibilities

Intelligence staff are responsible for the following tasks:

- the management and coordination of the intelligence function
- the provision of relevant, usable, timely and accurate intelligence on adversaries and environment by:
  - maintaining basic and current intelligence records
  - preparing intelligence and counterintelligence inputs to the military appreciation process
  - preparing and managing a collection plan
  - processing collected information, combat information and intelligence
  - disseminating information, combat information and intelligence
- the control of attached intelligence units and intelligence representatives
- the provision of policy advice and training on all aspects of combat intelligence and specialist intelligence
- the provision of intelligence support to information operations planning, including:
  - nodal analysis products as required
  - psychological activities
  - electronic warfare
  - physical destruction
  - deception

  - operations security
  - advice and warnings on security threats to materiel and personnel
- the coordination of language interpretation
- liaison with allied and other service and civilian intelligence agencies
- advice on and management of arrangements for the preliminary exploitation of captured personnel, documents and materiel.

Relationships

Intelligence staff at all levels must create and maintain positive working relationships across all groups and individuals, as follows:

- *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 at a headquarters, and must gain and maintain the commander's confidence by providing timely and effective intelligence.
- *Operations and plans staff.* The relationship between the intelligence and operations staff is symbiotic. Intelligence staff need to understand both current and planned operations in order to focus their efforts and anticipate information requirements. Similarly, operations staff rely on intelligence staff to provide the advice required on the threat and the environment for the planning and conduct of operations. This is most evident in the close relationship between operations and intelligence staff during the intelligence, surveillance and reconnaissance and targeting effects working groups. The co-location of operations, plans and intelligence staff is vital.
- *Combat service support staff.* Intelligence support for combat service support includes the provision of basic intelligence on the area of operations and the conduct of counterintelligence activities in the rear area in support of force protection and rear area security. The advice of combat service support staff may be required during assessment of the threat's logistics capability and the subsequent creation of a logistical intelligence product.
- *Combat arms staff.* As all forms of offensive action, including manoeuvre, fire planning, close air support, electronic attack, reconnaissance and psychological operations, must be synchronised within the headquarters, the relationship between the intelligence and operations staff cannot be understated. The ability to cultivate and foster clear lines of communication with combat arms staff will greatly assist the intelligence staff to refine threat capability and limitation assessments and to target collection operations.
- *Artillery staff.* Artillery intelligence results from the collection and processing of all available information on adversary indirect fire systems. Artillery staff in a surveillance and target acquisition role, including intelligence, are usually part of the offensive support cell at task force level and above. The surveillance and target acquisition staff 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 all-source cell. As part of this interface, the surveillance and target acquisition officer is usually located in the all-source cell to allow the rapid engagement of identified targets.

- *Engineer staff.* Engineer intelligence provides information on and assessments of terrain, the effects of weather on terrain, and adversary engineer capabilities, including mobility, countermobility and survivability. Hence, engineer staff support terrain analysis, and these efforts should not be duplicated between engineering and intelligence staff. At planning or orders groups, the engineer's brief should detail specific aspects of terrain that are critical to operations. At task force level and above, an engineer intelligence liaison officer will normally be appointed and acts as the principal engineer adviser to the intelligence staff.
- *Geomatic engineers and military geographic information staff.* Geomatic engineers have the capability to prepare and provide terrain information for intelligence and other purposes, including intelligence preparation of the battlespace. Geomatic engineers can provide the battlespace visualisation tools that enable the depiction of adversary schemes of manoeuvre and vulnerabilities. Military geographic information provides a critical input for the generation of a fused spatial intelligence product that underpins all command support systems and processes. The high-volume printing capability of geomatic engineer assets may also be employed in the production of psychological operations material.
- *Military police staff.* Military police are a valuable source of information due to their tasks of criminal investigation, escort of prisoners of war, liaison with civil police and refugee screening operations. It should be noted that military police investigations are conducted from a different perspective from counterintelligence activities. Military police will seek to solve a crime and lay charges. Counterintelligence personnel seek to neutralise threats to security and exploit the situation to counter hostile intelligence collection, espionage, sabotage, subversion or terrorism. This may involve controlling rather than punishing those involved. Commander's guidance must be sought to determine the desired outcome.
- *Electronic warfare staff.* At battalion level and above, an electronic warfare liaison officer will normally be attached when an electronic warfare asset is in support. The electronic warfare liaison officer is the electronic warfare adviser for the commander and, in this capacity, also provides electronic warfare advice to the intelligence staff. The intelligence staff support direction of the electronic warfare collection effort and advice on battlespace constraints to electronic warfare. Most electronic warfare efforts, however, are in electronic support which, as a primary sensor system, is driven by the collection requirements of the collection manager. Hence, electronic warfare has a close tasking association with intelligence staff, and their processed product (through embedded intelligence operators supporting electronic warfare activity) is fused in the all-source

cell. At task force level, an electronic warfare coordination centre will be established in the all-source cell. The electronic warfare coordination centre is responsible for the coordination and dissemination of electronic warfare products and signals intelligence.

Liaison

Intelligence liaison staff are an underpinning concept in ensuring the smooth and timely passage of information and intelligence between:

- flanking headquarters
- coalition partners
- police
- local authorities
- civilian intelligence organisations
- other government or non-government groups.

Military intelligence officers on secondment to an external organisation are by definition not dedicated liaison officers. However, the military intelligence officer develops knowledge of the area of operations, the population, the infrastructure and the threat which can be passed to the appropriate military intelligence staff. In contrast, an intelligence liaison officer is attached out of the parent intelligence organisation for intelligence liaison duties. The intelligence liaison officer provides a link for the commander and would normally deploy into the area of operations prior to the deployment of units to ensure the timely and accurate reciprocal flow of intelligence.

Chapter 4

Intelligence disciplines

Intelligence disciplines are highly specialised areas of the intelligence enterprise that may be single-Service or joint in nature and are able to be deployed as standalone capabilities or within an integrated, multidiscipline intelligence entity. Each discipline provides unique aspects of intelligence support.

Human intelligence

Human intelligence is a category of intelligence derived from the collection of information provided by human sources. Human intelligence operations are often highly sensitive and focus on determining threat capabilities, characteristics, vulnerabilities and intent. More information is contained in the following publications:

- *Land Warfare Procedures - Intelligence 2-1-2, Interrogation*
- *Land Warfare Procedures - Intelligence 2-1-4, Source Operations Handbook*
- *Land Warfare Procedures - General 2-1-6, Tactical Exploitation*.

Geospatial intelligence

Geospatial intelligence is a category of intelligence that concerns the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict geographically referenced features. Geospatial intelligence supports operations by providing a geospatial understanding of the physical operating environment. More information is contained in *Australian Defence Doctrine Publication 2.3, Geospatial Information and Services*.

Counterintelligence

Counterintelligence is that aspect of intelligence devoted to identifying, assessing and counteracting the threats to security posed by hostile intelligence entities engaged in covert activity such as espionage, sabotage, subversion or terrorism. Counterintelligence neutralises intelligence collection on friendly forces through counterintelligence operations and investigations. Counterintelligence force elements support the commander through defensive and offensive core functions to detect, identify, exploit and deny an adversarial intelligence collection effort. More information is contained in:

- *Australian Defence Doctrine Publication 2.1, Counterintelligence and Security*
- *Land Warfare Procedures - Intelligence 2-1-5, Field Security*.

Open-source intelligence

Open-source intelligence is the reporting derived from information collected from sources readily available to the general public. Although this not a standalone intelligence specialty, it is required in all intelligence force elements to support the commander and the mission. Publically available data, facts and information often provide the foundation for intelligence analysis and assessment. They may also answer existing requests for information and enhance collection through the confirmation of single-source information or supporting background information (biographical, cultural or geospatial).

Technical intelligence

Technical intelligence is intelligence derived from the collection, processing, analysis and exploitation of equipment and material. Specialists incorporate the complementary capabilities of biometrics, cyber-enabled intelligence, document and media exploitation, and forensics to develop this intelligence. Weapons technical intelligence concerns the capability and specifications of adversary weapons systems. It provides pointers to help develop countermeasures to neutralise that capability. More information is contained in *Australian Defence Doctrine Publication 2.4, Exploitation*.

Joint disciplines

Several additional intelligence disciplines operate solely in the joint domain and not at the single-Service level. These disciplines are covered in more detail in:

- *Australian Defence Doctrine Publication 2.0, Intelligence*
- *Australian Defence Force Publication 2.0.1, Intelligence Procedures*.

Chapter 5

Intelligence activities

The intelligence activities detailed in this chapter are in addition to the activities conducted by combat intelligence staff and are conducted by intelligence personnel for information collection or counterintelligence purposes. The activities covered are:

- source operations
- counterintelligence
- field security
- exploitation
- psychological operations
- screening and debriefing activities
- regional intelligence.

Source operations

Source operations refer to the acquisition of intelligence through liaison and human source exploitation. This is achieved using specialist personnel deployed to support a commander in the conduct of operations. The early deployment of source operators will significantly assist the deployed force commander and their supporting staff in receiving early warning of impending threats to the deployed force that are of a local nature.

Subsequent source operations will ensure that the understanding and awareness of the situation in the area of operations concerned is continually updated. This is achieved primarily through the continuing development of community contacts.

The size and composition of the deployed force, the nature of the operation, the commander's mission, the complexity of the battlespace, and the capability and intent of the threat force will determine the composition and structure of the deployed source operations element.

Source operations are not conducted in isolation. They form part of the coordinated intelligence effort, which includes field security, operations security, exploitation, electronic warfare and information actions.

Counterintelligence

Counterintelligence is that aspect of intelligence devoted to neutralising the effectiveness of hostile foreign intelligence service and insider threat activities, and to the protection of information against espionage, individuals against subversion and installations, and equipment, records or materiel against sabotage. This is achieved through both defensive and offensive means throughout the continuum of conflict by specially trained personnel to support the conduct of Australian Defence Force operations. Counterintelligence complements operations security, electronic warfare, psychological operations and operational deception, and is one of the contributors to information actions.

Counterintelligence is a multidiscipline function designed to detect, identify, assess, counter, neutralise, exploit or control activities of adversary collection assets, and incorporates counter–human intelligence, counter–signals intelligence and counter–imagery intelligence at all levels of operation from national to tactical.

Counterintelligence is both a defensive and offensive component of operations. Defensive counterintelligence focuses on protective security measures such as physical security or personnel security, and is primarily in the field security domain. In contrast, offensive counterintelligence is focused on the conduct of operations with the specific aim of exploiting, neutralising or degrading an adversary's ability to collect, process and disseminate intelligence.

The linkage between counterintelligence and field security can be quantified thus: counterintelligence is outward in its focus, identifying and exploiting an enemy's intelligence, surveillance and reconnaissance capability; while field security is inward in its focus, providing advice on operations security, movement security, personnel security and counter-sabotage security.

The application of both offensive and defensive counterintelligence measures from the earliest aspects of an operation will allow the Australian Defence Force to disrupt adversary collection efforts and deny adversary commanders access to valuable intelligence that would enable the execution of successful operations against the Australian Defence Force.

As an operation matures, the continued employment of counterintelligence measures will contribute significantly to the ongoing force protection of deployed Australian Defence Force elements in a given area of operations through the monitoring of the intelligence threat and the development of timely and appropriate courses of action. Counterintelligence activities may include:

- the continued development and maintenance of counter–human intelligence networks
- surveillance
- countersurveillance
- support to security investigations
- interagency liaison
- the development of counterintelligence countermeasures as part of the military deception counterintelligence effort.

Both counterintelligence and intelligence processes are central to achieving security as they identify actual and potential espionage (including intelligence collection), sabotage, subversion, and terrorism. Counterintelligence activities also counteract such threats and, in addition, allow them to be manipulated or controlled. Security is achieved through the collective measures of the friendly force, through implementation of protective security measures and the conduct of operations security and counterintelligence processes.

Field security

'Field security' is an umbrella term describing the local security support provided by intelligence personnel within an area of operations or rear area. It includes:

- the provision of advice and supervision of operational security
- movement security
- personnel security
- counter-subversion security
- field censorship.

Field security (also known as protective security) is the provision of physical security advice and security intelligence support to the deployed commander in an operational environment. This support is achieved through the collection and analysis of security intelligence as well as the provision of protective security and operations security advice.

Field security is not conducted in isolation. It forms part of a coordinated intelligence effort, which includes:

- specialist counterintelligence assets
- field intelligence
- exploitation
- electronic warfare
- information operations.

The composition and structure of the deployed force, the nature of the operation, the commander's mission, and the sophistication, capabilities and intent of the threat force will determine the composition and structure of a deployed field security element.

The utilisation of field security staff at all stages of the planning process will ensure effective application of the appropriate protective measures for a deployed force and its commander.

The field security and specialist counterintelligence capabilities are not automatically amalgamated as a single capability brick. The conduct of field security activities will generally cue follow-on specialist counterintelligence operations. This may lead to a subsequent joint field security/counterintelligence activity.

Exploitation

The exploitation of personnel, materiel and documents is a source of potentially valuable information. Every effort should be made to exploit these sources to the fullest extent.

The aim of exploitation is the timely extraction of information of intelligence value from personnel, materiel and documents, and the efficient dissemination of that product.

Operational experience has highlighted the value of exploitation operations and rapid dissemination of the intelligence obtained. It is important that exploitation operations are carefully planned and executed to ensure that the maximum amount of information is obtained in the minimum amount of time.

While exploitation is primarily an intelligence responsibility, its effectiveness will depend greatly on the cooperation of non-intelligence staff and units in facilitating the collection, safe custody, administration and rapid evacuation of captured personnel, documents and materiel.

Psychological operations

Although psychological operations fall within the remit of the intelligence staff, they are an operations function within information actions. They are not classified as intelligence activities under the definition, but as a user of intelligence and a contributor of information, and should be considered as both a customer and a source.

From studies of modern history, it is widely recognised that the psychological dimension of conflict is as important as the physical. When imposing national strategic and military objectives upon a target area, that audience’s perceptions and attitudes have the ability to shape the outcome of a conflict or war.

The aim of psychological operations is to influence and shape the attitudes and behaviour of a target area in an effort to persuade adversary, neutral and friendly parties to behave favourably in accordance with national and military objectives. Psychological operations operate as a continuum, functioning during peace, conflict and war.

Psychological operations support all types of military activities within an operation, including conventional warfare, peace support and Special Forces activities. In doing so, they create a force-multiplication effect while also providing a degree of force protection to deployed units and various stakeholders.

Psychological operations are recognised as an essential element in national and military conflicts and operations. They are also a critical element of information operations and provide commanders with a non-lethal means of persuading belligerents to behave in a favourable manner in the achievement of national goals. Psychological operations should be considered as critical elements of manoeuvre within a nation’s combat power. The psychological impact of the battlespace is an important consideration in the planning of any military or diplomatic activity. Through the effective employment of psychological operations, a commander can achieve a decisive tactical advantage.

Screening and debriefing

Screening refers to the process of identifying who has information required by commanders (articulated in the intelligence collection plan) and who is willing to provide that information within the time frames set by the intelligence collection manager. The purpose of screening is to identify individuals or groups who are of interest to human intelligence collection and counterintelligence activities.

Debriefing is the process by which information is elicited from individuals who are willing to voluntarily provide information in response to questions asked or, in the case of exploitation, people whose will to resist the questioning process has been broken. The purpose of debriefing is to systematically extract information of value to commanders at all levels from civilians and military personnel who have been identified by the screening process as having the required information.

Screening and debriefing can be tailored to provide support to a variety of scenarios and may be conducted in support of strategic, operational and tactical objectives. For instance, a debriefing element could be tailored to debrief Australian nationals returning from an area of interest in a relatively benign environment, such as a domestic or international airport. Alternatively, the same element could be structured to provide screening support to a cordon-and-search vehicle checkpoint or refugee/line crossing in a tactical environment. Accordingly, the size and scope of screening and the intelligence support provided will vary.

Within the context of land intelligence collection, both screening and debriefing can be conducted by personnel from the intelligence unit who have been trained to conduct:

- tactical questioning
- field intelligence
- exploitation
- field security
- counterintelligence, or
- regional intelligence.

In all cases, screening and debriefing are either primary or secondary tasks for each of those intelligence collection capabilities.

Regional intelligence

Regional intelligence is not a new form of intelligence activity and has existed in one form or another since the Navy Coastwatchers of the South-West Pacific and South-East Asia during World War II.

Regional intelligence is an approved collection activity conducted as part of a coordinated intelligence surveillance and reconnaissance plan. It is undertaken by

Australian Defence Force intelligence operators in northern Australia and Australian offshore territories. These operators are focused primarily on defence of Australia tasks, but their activities may also include Defence Force aid to the civil community and Defence Force assistance to the civil power.

Regional intelligence is usually conducted in order to collect intelligence over broad areas. However, it is also suitable for collection of specific information from focal areas. Regional intelligence shares many features of source operation activities and gains its information from a variety of community contacts and civilian agencies. It is capable of providing low-cost intelligence collection to both tactical and operational level commanders who are conducting broad area surveillance tasks.

Regional intelligence is based almost entirely on the intelligence gained from interaction with the local community and the raising and exploitation of civilian reporting networks. Regional intelligence is differentiated from source operations by the fact that collection and contact are more overt.

Regional intelligence tasks are currently performed by all three Services of the Australian Defence Force. Navy inshore coastal operations, Air Force air base reporting networks and Army North Force and Pilbara Regiment capabilities all perform regional intelligence collection tasks.

Regional intelligence can be conducted by suitably trained members of the Australian Defence Force, acting overtly, during peacetime or periods of heightened tension.

Conclusion

> *'It's right to learn, even from the enemy.'*
>
> ***Publius Ovidius Naso ('Ovid')***[1]

While the commander directs the deployment of forces, it is timely, accurate and reliable intelligence that enables the Army to conduct unified land operations and provides the commander with the necessary awareness to maintain decision superiority.

Intelligence facilitates sound decision-making by reducing uncertainty about adversary capabilities and intentions and helping to clear the fog of war.

Although intelligence is seen to be the realm of the intelligence professional, it is inherently the responsibility of command and requires the commander's direct involvement in all phases. Without close and continuous guidance, the intelligence enterprise will lose its effectiveness and will be under-utilised, risking operational success.

A competent commander recognises that obtaining actionable intelligence is a team effort, operations and intelligence are inseparable, and the successful conduct of operations is driven and shaped by effective intelligence.

[1] 'Ovid' 8 AD, *Metamorphoses*, trans Melville, AD, introduction and notes Kenney, EJ, 2008, Oxford University Press, United Kingdom.

References

Australian Defence Doctrine Publication 2.0, Intelligence

Australian Defence Doctrine Publication 2.1, Counterintelligence and Security

Australian Defence Doctrine Publication 2.3, Geospatial Information and Services

Australian Defence Doctrine Publication 2.4, Exploitation

Australian Defence Doctrine Publication 3.7, Collection Operations

Australian Defence Force Publication 2.0.1, Intelligence Procedures

Giles, L 2007, *The Art of War by Sun Tzu*, Special Edition, Special Edition Books, United States

Land Warfare Doctrine 2-1, Intelligence Staff Duties

Land Warfare Doctrine 2-2, Intelligence, Surveillance and Reconnaissance

Land Warfare Doctrine 5-1-4, The Military Appreciation Process

Land Warfare Procedures - Intelligence 2-1-2, Interrogation

Land Warfare Procedures - Intelligence 2-1-4, Source Operations Handbook

Land Warfare Procedures - Intelligence 2-1-5, Field Security

Land Warfare Procedures - General 2-1-6, Tactical Exploitation

‘Ovid’ 8 AD, *Metamorphoses*, trans Melville, AD, introduction and notes Kenney, EJ, 2008, Oxford University Press, United Kingdom

Endmatter

Doctrine Online

This and other doctrine publications are available via the Doctrine Online website located at: *http://drnet.defence.gov.au/ARMY/Doctrine-Online/Pages/Home.aspx*. Paper copies may be out of date. Doctrine Online is the authoritative source for current doctrine. Users are to ensure currency of all doctrine publications against the Doctrine Online library.

Images and multimedia

Images and multimedia in this publication are Commonwealth copyright or otherwise authorised by the owners for doctrine purposes. Online versions may contain multimedia which can be accessed from *Doctrine Online*.

Gender

This publication has been prepared with gender-neutral language.

Illustrations

Figure 2–1: The intelligence cycle 11

Tables

Table 2–1: Admiralty Grading System..13