Contents

Army

Land Warfare Doctrine 6-0

Signals
2018

This publication supersedes *Land Warfare Doctrine 6-0, Signals*, 2008.

Contents

Serving our Nation

Contents

Introduction

As described in *Land Warfare Doctrine 1, The Fundamentals of Land Power*, war remains violent, dynamic, unpredictable and chaotic. At the same time the conduct of war continues to evolve due to political imperatives, the environment, cultural norms and technology. Increasingly, warfare is being waged by information- and technology-enabled military forces in land, sea, air, space and cyberspace environments. Each of these environments is becoming more crowded, connected, lethal, collective and constrained due to urbanisation, the proliferation and democratisation of technology, the increased lethality of weapons systems, and changing social expectations. Operating in this context requires an Army that is multiskilled, flexible, adaptable, well educated and trained, and doctrinally prepared.

This environment is particularly challenging for the Army signals capability. Army signals practitioners, both Royal Australian Corps of Signals and all-corps signallers, fight within and through cyberspace and the electromagnetic spectrum. This is an increasingly complex environment that is in a continual contest across the spectrum of conflict and unbounded by geographic borders. The environment demands a signals capability that is threat focused, dynamic, technically adept and tactically astute, as well as capable of working with joint, coalition and interagency partners. More broadly, there is a requirement for increased digital literacy across the force in order to realise the opportunities presented through the introduction of enhanced information warfare capabilities.

The document provides a common understanding of the Army signals capability by detailing the foundation concepts of signals applicable to all-corps and specialist signallers, and those who wish to understand how best to employ the capability. It also considers the current and near-future environment and positions Army to take best advantage of technological advances, recognising both opportunities and threats.

This edition of *Land Warfare Doctrine 6-0, Signals* contains four chapters. Chapter 1 details the foundation concepts for the Army signals capability by describing the operational context, defining the Army signals mission sets, discussing cyberspace operations and detailing the signals principles. Chapter 2 focuses on the outputs of the Army signals capability through an examination of the 10 enduring and complementary signals functions. Chapter 3 examines signals planning, emphasising the importance of integrating communications and electronic warfare planning into the staff planning process. Finally, Chapter 4 addresses the relationship between headquarters staff and signals leaders, advisers and specialist staff. Chapter 4 also describes the application of technical control in a signals context.

As mentioned in *Land Warfare Doctrine 1, The Fundamentals of Land Power*, doctrine serves to assist the institution to learn, anticipate and adapt.[1] This document provides both the philosophical foundation for the Army signals capability and the basis for professional discourse and debate. Through such discourse, signals practitioners can ensure that the capability remains forward looking, relevant, adaptable and effective.

[1] Cohen EA and Gooch J 2011, *Military Misfortunes: The Anatomy of Failure in War*, 2nd revised edition, The Free Press, New York.

Chapter 1

Signals

Overview

The introduction of enhanced information warfare[1] capabilities into the Australian Defence Force is integral to the modernisation and future operational capability of the force. These capabilities provide significant opportunities for enhanced synchronisation, understanding, protection and precision, but also introduce new risks and potential vulnerabilities. Responding to this change requires an improved level of digital literacy across the force, particularly in Army, given an increased reliance on non-specialist signallers such as regimental signallers and mission system operators. Improvement in digital literacy across Army is enhanced by a common understanding of the Army's signals capability.

This chapter outlines the foundation concepts for the Army signals capability. It firstly describes the operational context, before detailing the Army signals mission sets, discussing cyberspace operations and outlining the signals principles. The chapter aligns with joint doctrine, noting that some of Army's terminology and functional groupings differ from those of the other Services.

Context

Land Warfare Doctrine 1, The Fundamentals of Land Power recognises that the nature of war and conflict has not changed. As a struggle of political and human will, it remains violent, dynamic, unpredictable, chaotic and difficult to control. At the same time the conduct of war – its character – continues to change based on desired political objectives, human interaction, cultural norms, environment and technology.[2] The changing character of war is further described in Army's *Future Land Warfare Report*. This document describes five meta-trends that are expected to influence the conduct of war over the next few decades:

- *Crowded.* This trend relates to the creation of complex human, informational and urban physical terrain due to factors such as urbanisation, population growth, resource scarcity and political instability.

[1] Information warfare is defined as actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.

[2] *Land Warfare Doctrine 1, The Fundamentals of Land Power* [Chapter 1].

- *Connected.* This refers to the increasingly interconnected nature of global economic, social and communications systems.
- *Lethal.* This refers to the increasing effectiveness of methods and systems used to inflict death and destruction, and the proliferation of these capabilities across traditional boundaries. This trend recognises the ease with which operating methods and tactics are disseminated across geographic borders.
- *Collective.* This trend relates to the increase in national and global sharing and security arrangements in response to common threats.
- *Constrained.* The restrictions and limitations on the generation of forces and the conduct of land operations are increasing due to recruitment and financial pressures as well as the expectations of a more socially aware population.

Operating in an environment defined by these meta-trends requires the employment of the full range of joint and coalition effects. As a consequence, Army expects to operate within a joint force as normal practice. Within this joint force, Army will continue to apply a manoeuvrist philosophy, one that aims to shatter the adversary's moral and physical cohesion through orchestrated actions across multiple lines of operation to a single purpose. This approach seeks to create a turbulent and rapidly deteriorating situation with which the adversary cannot cope.[3]

Army's concept of manoeuvre occurs within and across the physical, information and cognitive dimensions.[4] Army signals missions lie mainly in the information dimension, fighting through and within cyberspace and the electromagnetic spectrum. Cyberspace and the electromagnetic spectrum are influenced by the same meta-trends outlined in the *Future Land Warfare Report*, becoming increasingly converged, congested (crowded), constrained, connected and contested. Further, the democratisation of communications technology means that the Australian Defence Force may have limited advantage in this area, and that any advantage that is achieved will be hard-won and often fleeting. The complexity of the environment will also make it difficult to predict the second- and third-order effects from actions taken through cyberspace and the electromagnetic spectrum. This environment is one of continual contest, across the spectrum of conflict and unbounded by geographic constraints.

The operational environment, Army's warfighting philosophy, and the implications of fighting within and through cyberspace and the electromagnetic spectrum demand that the Army's signals capability be threat focused, dynamic, technically adept and tactically astute. It must be able to operate in a complex, congested and highly contested electromagnetic spectrum and cyberspace environment against peer or near-peer competitors. Signals must enable, and contribute to, Army's manoeuvrist approach through the provision of agile, secure, responsive and

[3] ibid [Chapter 3].

[4] ibid.

robust communications and electronic warfare capabilities that are tailored to support the commander’s plan. These capabilities must be networked with joint force and coalition partners to enable orchestration of land, joint, coalition and interagency effects across the battlespace domains. The rapid and effective exchange of information and intelligence across the force is critical, allowing commanders to grasp fleeting opportunities for success.

The Army signals capability requires a threat focus, anticipating that the use of cyberspace and the electromagnetic spectrum is under constant threat, whether in barracks, on exercise or on operations overseas. There is a continual contest for access, control and dominance. A focus on the enduring and future cyberspace and electromagnetic spectrum threats is fundamental to the planning and conduct of operations, the design and conduct of individual and collective training, and capability development.

Due to the uneven nature of modernisation across the force and the pace of technological change, Army signals staff need to manage a mix of legacy and new equipment along with service- and platform-specific systems. The pace of technological change will continue to challenge Army’s equipment procurement processes, the ability to attract and retain skilled staff, and the ability to provide contemporary technical training. Meeting these demands will rely on well-trained Army signals personnel and educated (‘digitally literate’) commanders and staff, as well as the continued refinement of operational processes.

Definition

The Army signals capability is a combination of people[5], systems and processes that deliver communications, electronic warfare and cyberspace operations capabilities to Army and the broader Australian Defence Force.

Mission sets

The Army signals mission sets articulate the signals capability’s contribution to Army’s mission. The statements are simple descriptions; however, the mission sets themselves are complex, challenging and far-reaching.

The Army signals capability encompasses three mission sets:

- *Communications.* This refers to the provision of highly agile, secure, capable, robust and reliable communication and information systems to support Army and Australian Defence Force strategic, operational and tactical command and control requirements.

[5] Includes both Royal Australian Corps of Signals (communications and electronic warfare) and all-corps communications/informational technology personnel.

- *Electronic warfare.* This refers to the provision of highly agile and capable intelligence collection, and strike capabilities to support Army and Australian Defence Force strategic, operational and tactical intelligence requirements and joint fires.
- *Cyberspace operations.* This refers to the employment of cyberspace capabilities with the primary purpose of achieving objectives in or through cyberspace.

Communications

The communications mission set provides a secure and reliable communications and information system in support of commanders at all levels. This mission set ensures that commanders have a flexible and robust network at their disposal during training and on operations. The network is the commander's tool to assimilate information and to exercise authority and direct forces over large geographic areas and a wide range of conditions. The network architecture allows collaboration among commanders and staff, as well as joint and coalition partners, enabling shared situational awareness and synchronised action.

Fundamental to the provision of communications support is effective signals planning and the active management of the communications network at all levels. Effective planning and management allows for the provision of accurate, timely and assured information to the commander and staff.

Electronic warfare

The electronic warfare mission set provides an intelligence collection and fires capability in support of the commander's manoeuvre plan. It also includes all-corps actions taken to defend against adversary use of the electromagnetic spectrum. It enables the projection of power in and through the information domain.

Specialist electronic warfare capabilities focus on responding to the commander's priority information requirements, feeding collection outputs into the broader intelligence cycle. Electronic warfare also seeks to identify and target critical vulnerabilities in adversary command and control systems, with the objective of disrupting command and control and denying the adversary the ability to control the tempo of operations or to coordinate an effective response to friendly actions. There are three main types of electronic warfare activities[6]:

- *Electronic protection.* These activities involve actions to protect personnel, facilities and equipment from any effects of friendly or adversary use of the electromagnetic spectrum. Electronic protection is an all-corps responsibility.
- *Electronic support.* These activities involve actions to search for, intercept, locate, record and analyse radiated electromagnetic energy for the purpose

[6] Referred to as 'electronic warfare divisions' in *Australian Defence Doctrine Publication 3.5, Electronic Warfare.*

of exploiting this energy in support of military operations. The principal role of electronic support is to inform the intelligence cycle.

- *Electronic attack.* These activities involve the use of electromagnetic energy, directed energy or anti-radiation weapons to attack personnel, facilities or equipment with the intent of degrading, neutralising or destroying adversary combat capability. It provides a joint fires effect.

Strategic enablers. Specialist land electronic warfare capabilities can provide access to significant joint, national and coalition assets across these electronic warfare activities. This can provide an operational effect far beyond the capabilities of the individual element deployed.

Given the close linkages with joint and national capabilities, the sensitivity of the specialist capabilities and the limited electronic warfare resource, active planning and management of the specialist electronic warfare capability is critical. *Australian Defence Doctrine Publication 3.5, Electronic Warfare* details the electronic warfare roles, tasks and planning considerations.

Cyberspace operations

Cyberspace is defined as a global domain within the information environment consisting of an interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems and embedded processors and controllers, and their resident data.

More broadly, cyberspace can be seen as a domain that consists of an interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, software, embedded processors and controllers, other devices (phones, radio) and their resident data, used to store, modify, exchange, process and collaborate on information. Cyberspace includes non-physical components such as policy, governance, standards, management, operations and human capital.[7]

Information technology networks are ubiquitous in all but the most underdeveloped nations, and as such they present opportunities to access, exploit and control adversary information. Conversely, Army’s increased reliance on information technology and technology-enabled systems and platforms challenges our ability to protect friendly information. The synchronised approach to these two challenges is the conduct of cyberspace operations.

Cyberspace operations see the employment of cyberspace capabilities with the primary purpose of achieving objectives in or through cyberspace. There are three types of cyberspace missions:[8]

- *Offensive cyberspace operations.* These operations are conducted to project power against adversaries in or through cyberspace.

[7] Army Headquarters, *Land Cyberspace Operations Strategy*.

[8] ibid, p. 8.

- *Defensive cyberspace operations.* These operations are threat-focused measures that seek to preserve friendly use of cyber capabilities and protect networks.
- *Cybersecurity operations.* These operations are network-centric measures taken to design, build, configure, secure, operate, maintain and sustain a secure network environment, including measures to harden and protect Defence networks and resident data, mission systems and sensors, and to educate the people who use them.

The signals capability contributes to cyberspace operations through:

- the design, deployment, operation, maintenance and protection of Army networks and mission systems through which Army conducts cyberspace operations
- the preservation of the commander's use of cyberspace capabilities, including actions to re-establish, resecure, reroute, reconstitute or isolate degraded or compromised local networks
- specialised contributions to elements of defensive and offensive cyberspace operations
- input into cyberspace awareness, intelligence, planning and targeting processes
- the conduct of individual training and education on cyberspace operations.

Signals principles

The signals principles draw from operational experience and form a set of considerations applicable to any signals plan. The weight given to each principle depends on the circumstances, and their application requires military judgement.

Support the chain of command. Signals must support the commander's intent and concept of manoeuvre and enable the orchestration of combat functions. This includes the use of signals capabilities to manoeuvre through and within the electromagnetic spectrum and cyberspace to enable or provide manoeuvre effects. Signals elements must be able to adapt to changing command structures, developing information requirements and rapid regrouping.

Integration. In an increasingly connected environment where operating as part of a joint force is the norm, the Army signals capability must ensure integration with joint and coalition partners both in the design, deployment and operation of communications networks and in the conduct of cyberspace and electronic warfare operations. Integration efforts reduce points of failure, support effective information flows and can provide access to significant specialist capabilities.

Reliability. Continuity of command requires reliable signals services that can provide the endurance needed from land-based systems, including land-based collection activities. A reliable system that provides a minimum of nodes and facilities is usually preferable to a more elegant technical solution that is more difficult to recover in a complex environment. This principle is particularly important for tactical systems.

Flexibility. Signals plans must be flexible enough to support rapid regrouping and unexpected circumstances. Signals operations must enable the commander to seize fleeting opportunities for success, and support the adaptability of combined arms teams. Planners should consider the allocation of discrete and complementary signals capabilities to the commander's reserve. Signals plans and personnel must retain the flexibility to meet changing priorities and to respond in an agile manner to higher priority strategic tasking.

Survivability. Signals capabilities need to be robust and resilient to survive the hostile environment, and to recover quickly from technical faults or adversary disruption. Planners need to consider threat actions and ensure that recovery, continuity and destruction plans are in place as appropriate. Signals platforms and personnel should have physical protection commensurate with the supported force and their task. Attention needs to be paid to the adequate protection of vulnerable nodes such as retransmission detachments and electronic warfare collection assets.

Mobility. At all levels of command, the mobility of signals assets must be commensurate with that of the supported force. Assets and personnel require sufficient mobility to rapidly deploy, establish and redeploy in support of the commander's scheme of manoeuvre. Sufficient mobility also aids in the protection of critical assets. The design of scalable signals capabilities can support increased mobility.

Security. Confidentiality, availability and integrity of information and equipment are fundamental to the signals mission. Information assurance activities, cybersecurity operations, electronic protection and physical security activities are critical to ensuring that commanders and staff are confident that the information gained, stored and disseminated through signals assets is reliable.

Simplicity. Simple signals plans are more likely to withstand operational stresses. A simple plan is more readily understood, disseminated and implemented, and will better support mission command. Clear and understandable plans will also allow for more effective reorganisation and, where necessary, transition between force rotations.

Capacity. Communications networks must have sufficient capacity to deal with required information flows and to react to spikes in demand. The system should allow for a prioritisation of services when required. Reserves of equipment, personnel and bandwidth allow for surges in capacity.

Quality. The quality of services provided by the Army's signals capability must be sufficient to ensure the integrity of information and that there is no loss in meaning during transmission. Data or systems must remain appropriately responsive to the requirements of commanders and other decision-makers.

Economy. While planning should aim to match capacity with demand, signals assets will remain finite resources, and the effective prioritisation of manpower and equipment, sound information management processes, and integration with joint networks/capabilities will be required. An economical approach to signals support also allows the establishment of reserves of equipment, personnel and bandwidth.

Interoperability. The importance of joint, coalition and interagency coordination demands an effective information exchange. This will remain a key technical and process challenge due to service stovepipes, security requirements and national boundaries. Interoperability planning must commence with a clear and logical understanding of information flow requirements, and an awareness of technical and procedural solutions.

Anticipation of requirements. Anticipation of requirements allows for adequate preparation of long lead-time capabilities, enables effective joint support, and provides appropriate warning for reorganisation and relocation. The ability to anticipate requirements depends on sound signals-to-staff relationships, active involvement in the commander’s planning process, and effective branch and sequel planning within the planning process.

Chapter 2

The signals functions

The signals functions describe the outputs required of the Army signals capability regardless of where on the spectrum of conflict the operation or activity occurs (see Figure 2–1). The functional grouping provides a holistic view of the outputs generated by several discrete capabilities and activities. While described as 10 discrete functions, they are complementary and mutually supporting. The emphasis on a particular function may depend on the type or phase of an operation; however, each operation will require the integrated conduct of each function.

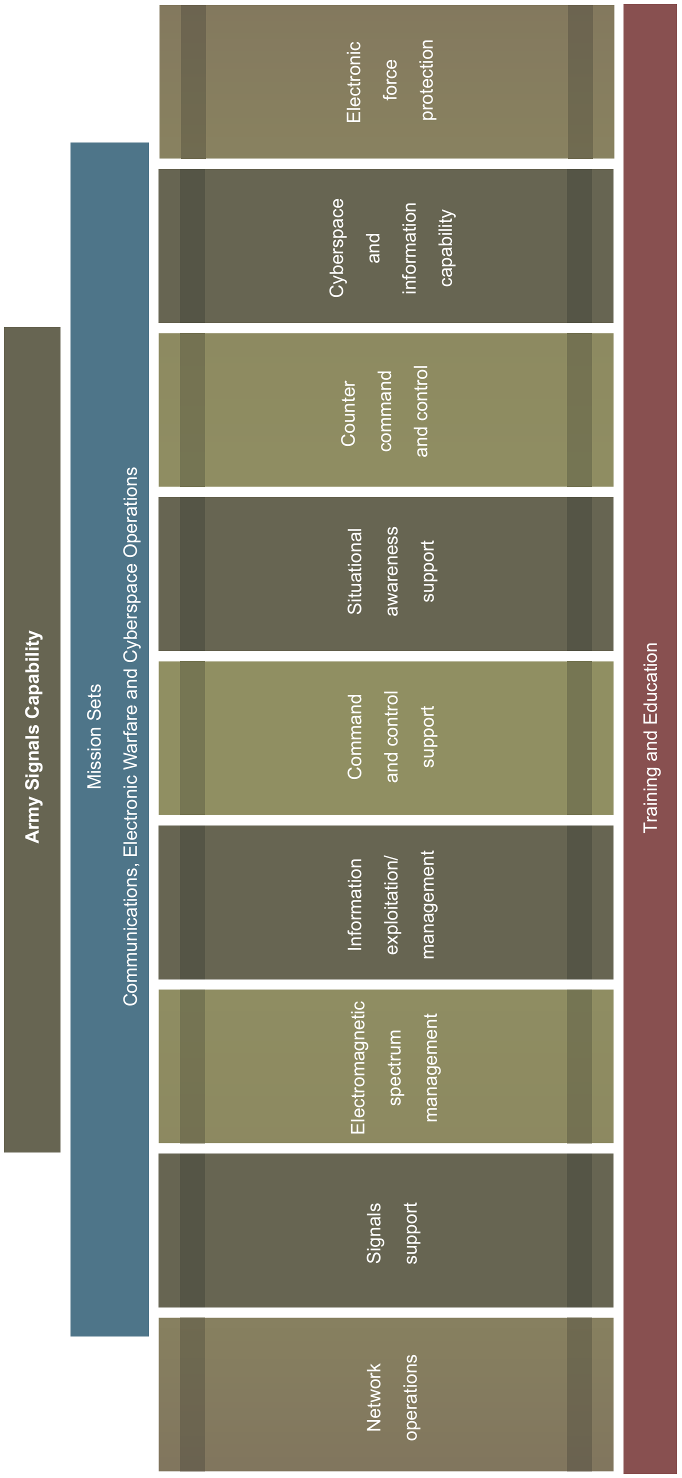
Army Signals Capability
Mission Sets
Communications, Electronic Warfare and Cyberspace Operations
Network operations
Signals support
Electromagnetic spectrum management
Information exploitation/ management
Command and control support
Situational awareness support
Counter command and control
Cyberspace and information capability
Electronic force protection
Training and Education

Figure 2–1: The signals functions

Command and control support

Command and control support activities include signals staff advice to commanders, the planning and provision of rapidly deployed, accurate, robust and secure command and control systems, and the dynamic management of these systems to support land forces within a joint, coalition or interagency force. This function also includes electronic warfare support to command and control through a range of inputs into the supporting intelligence cycle.

One of the key activities within command and control support is the provision of signals staff support by the supporting signals organisation. This can be a regimental signals officer within an infantry battalion or a signals staff cell formed at a major headquarters. At each level, however, the signals element provides a principal adviser to the commander and ensures that accurate and timely support is available to headquarters staff and subordinate organisations.

The integration of signals staff into the commander's staff planning process enables the provision of effective signals input, as discussed in Chapter 3. Such integration is critical to ensure a tight coupling of the signals plan with the commander's manoeuvre concept, and enables signals staff to anticipate future requirements. The relationship between signals staff and the headquarters staff is crucial to this process, as discussed in Chapter 4.

Command and control support also includes the provision of accurate, robust and secure communications systems for command and control during training and operations. These systems require the security, capacity and redundancy to withstand rapid reorganisation and must be able to support joint, coalition or interagency elements. System design must also consider the constant threat of cyberspace and physical exploitation, denial, degradation or destruction.

The provision of effective command and control networks requires the detailed and dynamic management of the system and a sound anticipation of changes to command and control requirements and threat actions. Active management requires a keen appreciation of the commander's plan, an awareness of the electromagnetic system environment, a sound understanding of the network capabilities and status, and an appreciation of the threats to the network. At the technical level, it requires the ability to monitor the network, the ability to assign priority to information types, and sufficient network redundancy and capacity.

Electronic warfare contributions to the intelligence cycle also support the command and control of the force. In particular, electronic warfare collection operations focus on answering the commander's priority information requirements and, when integrated with the force intelligence cycle, these collection operations support the development of fused intelligence. This provides the commander with improved knowledge of the battlespace, ideally leading to decision superiority.[1]

[1] *Land Warfare Doctrine 2-0, Intelligence* [Chapter 1].

Situational awareness support

Situational awareness support includes the planning, management and operation of capabilities that support persistent intelligence, surveillance and reconnaissance, the delivery of meta-data and video in real time, the retention and mining of data, the integration of joint and coalition systems, and support to tactical mission systems. The signals capability also contributes to the development of situational awareness both through specialist electronic warfare inputs into the intelligence cycle and through such functions as electromagnetic spectrum control and electronic force protection.

The signals capability is responsible for enabling the timely and effective dissemination of intelligence, surveillance and reconnaissance data. This data must move horizontally between joint headquarters, coalition partners and, often, interagency organisations, and vertically between strategic, operational and tactical headquarters and the intelligence, surveillance and reconnaissance collection capabilities. Equally important is the ability to move, store and support the analysis of large quantities of data, as well as supporting the management of information exchange across a range of platforms and systems. The complexity of this function underlines the importance of signals input into intelligence, surveillance and reconnaissance planning and the development of specialist applications and networks.

Tactical mission systems such as the Battle Management System – Command and Control and the Battle Management System – Fires, as well as aviation, unmanned aerial systems and ground-based platform mission systems, play an important role in the situational awareness of the deployed force. These mission systems are typically low-bandwidth, stand-alone and mobile systems that are under significant threat. In this context situational awareness support ensures that these networks have sufficient redundancy and resilience, applying a priority of effort in line with the commander's requirements and the phase of the operation. Effective support also requires significant planning and technical effort to design and maintain technical and procedural methods of information exchange between these tactical systems and the broader force level information and communications technology systems.

Specialist electronic warfare capabilities contribute directly to the situational awareness of the force as a result of their role in the broader intelligence, surveillance and reconnaissance effort. Electronic support missions search for, intercept and identify, direction find, analyse and report on electromagnetic emissions. Such activities, when combined with other reporting, support the development of the broader intelligence picture and can, when required, provide tactical reporting. Specialist electronic warfare elements also enable access to joint, coalition and national assets, significantly enhancing the breadth and depth of collection assets available to the commander.

Counter command and control

Commanders and their command and control systems present an attractive target for exploitation, disruption, denial or destruction, and increased connectivity as well as the proliferation of personal communications systems has resulted in increased vulnerability. The counter command and control function aims to locate, exploit, disrupt, deny or destroy adversary networks. The function also reflects the contested nature of the electromagnetic system and cyberspace, and hence reflects efforts made to defend friendly command and control against adversary counter command and control activities.

Army's signals capability contributes to broader efforts to degrade adversary command and control through the provision of specialist electronic warfare capabilities and their integration into intelligence and targeting processes. Electronic warfare capabilities are able to employ electronic support to locate, exploit and, if necessary, analyse emissions to determine an adversary's command and control location and status, while electronic attack can be employed to disrupt or deny adversary command and control networks. Electronic warfare assets can also leverage national, joint and coalition capabilities to assist with countering adversary command and control networks. These actions must be tightly coupled with the commander's manoeuvre plan to ensure appropriate synchronisation and asset survivability.

The conduct of adversary command and control analysis and 'reverse' battlespace operating system planning also contributes to the development of counter command and control activities. This is conducted during the intelligence preparation of the battlespace phase of the planning process, as described in Chapter 3. Importantly, this analysis and subsequent wargaming allows for the development of high-value targets within adversary command and control systems, and the identification of adversary command and control vulnerabilities and likely adversary actions against friendly command and control.

It is accepted that any adversary will target friendly command and control. Signals planning should consider the employment of counter electronic warfare plans, electronic protection, the use of friendly monitoring systems, the redundancy and prioritisation of systems, and the procedural and technical protection of computer networks and mission systems. Signals staff must also be prepared to work with commanders, public affairs teams and security staff to develop effective and practical plans to manage the risks posed by the use of social media.

Electromagnetic spectrum management

This function includes the management of the electromagnetic spectrum through both battlespace spectrum management, and the dynamic monitoring, planning and directing of joint electromagnetic operations in support of the commander.

These activities provide spectrum awareness, thus enabling exploitation, attack and denial of the opponent's use of the spectrum while protecting our own.

The number of emitting platforms within the modern battlespace results in significant competition for spectrum; consequently, there are more opportunities for frequency conflict, and increasing difficulty in understanding and managing spectrum usage. Consequently, robust and active battlespace spectrum management is critical to mission success; this requires a collaborative and informed approach across a wide range of spectrum users, not just communicators. Effective usage of the electromagnetic spectrum in such an environment requires detailed planning, assignment, disciplined use and deconfliction of assigned spectrum. Army also has a responsibility to manage its assigned spectrum as part of the joint and/or coalition battlespace, as well as to contribute to joint/coalition force spectrum awareness, management processes and organisations.

Army's signals capability also has a role to ensure dynamic situational awareness of friendly, adversary and noncombatant use of the electromagnetic spectrum. This enables effective, prioritised and active exploitation of the electromagnetic spectrum by friendly forces, and seeks to support actions taken against adversary and noncombatant use of the electromagnetic spectrum. These actions seek to ensure control of the spectrum during critical phases.[2] The ability to conduct dynamic management and exploitation such as this relies on effective monitoring systems and an integrated joint spectrum planning and management process.

Information exploitation/management

This function recognises that information management is more than just the establishment of processes for document creation, storage and disposal; information must also be effectively disseminated and its value fully exploited. The Army's signals role within this function is to enable the sharing and use of information to achieve shared situational awareness, improved decision-making and the coordination of desired effects. It encompasses specialist advice and the management of capabilities to support information/data storage and management, content management, and staging.

These activities seek to exploit the value[3] of the information gathered, developed and stored by the force in support of command and control processes. Information management will continue to grow in importance given the significant increase in intelligence collection capabilities across the Australian Defence Force. Army's signals capability should expect to provide management and support to 'big data'[4] through the storage and provision of effective search and analytical functions. This

[2] These electromagnetic spectrum operations have been titled variously as electromagnetic battle management and joint electromagnetic spectrum management operations.

[3] Maximise the benefit of the information.

[4] 'Big data' refers to collections of data that require specialised applications for storage and management due to either to the size/amount of the data or its complexity.

implies the requirement for signals elements to work closely with commanders and staff to assist in the development of information management processes and to ensure that these processes are feasible given equipment and network capabilities.

Network operations

Network operations refers to the planning, engineering installing, operating, maintaining, controlling and defending of strategic, operational and tactical command and control networks. It includes the day-to-day management and proactive planning for, and dynamic response to, the network degradation caused by technical issues or adversary action. Network operations require the ongoing monitoring of communications networks and the ability to reconfigure networks in response to changing operational circumstances. This function also requires the ongoing monitoring and configuration of information repositories and dissemination processes to ensure that information is available at the right place at the right time. Network operations also manage the network assurance, systems, processes and procedures that ensure the confidentiality, integrity and availability of information.

The coordination of signals elements across the battlespace and awareness of the command and control network status is enhanced through effective network operations. Effective coordination and network situational awareness increases the agility of command and control support, assists in the orchestration of joint signals effects and supports effective signals planning.

Fundamentally, this function recognises that the operation of signals networks requires an active, informed and responsive management philosophy, enabled by effective tools that provide network awareness and management functionality.

Signals support

The signals capability also enables the broader control and sustainment of the force, which includes:

- support to specialist logistic and administrative information and communications technology systems, such as deployed warehouse, maintenance and catering systems
- support to specialist health systems such as casualty regulation and general health management systems
- installation and rigging capabilities that support fixed infrastructure in deployed and specified domestic locations
- the development, testing and management of specific communication and information systems in support of the force

- linking strategic and deployed information and communications technology environments.

One of the major signals support activities for a number of Royal Australian Corps of Signals units is the provision of first-line logistic and life support for combat brigades and deployable joint force headquarters. This includes the administrative and logistic support and security required to support the headquarters on operations. These Signals Corps units are intimately involved in the planning, layout and occupation of headquarters sites, ensuring effective communications and the adequate sustainment and security of the headquarters. Within combat brigades and the deployable joint force headquarters, the organic Signals Corps units are responsible for the coordination of local security efforts, including command of assigned security assets.

Cyberspace operations and information-related capabilities

Information-related capabilities are the capabilities, techniques or activities that use information to create a physical, functional, temporal or psychological effect upon targets or target audiences and/or protect friendly use of information.[5] This function includes such activities as cyberspace operations, electronic warfare, signature management[6] and information assurance activities. It also recognises the role that these capabilities play in support of operations security and deception.

Cyberspace, by its nature, cuts across the traditional warfighting domains and functional groupings such as battlespace operating systems. Consequently, cyberspace operations require a high level of synchronisation in order to achieve effects in the information domain[7]. The concept of cyberspace and electromagnetic activities[8] provides a useful model to guide the coordination of electronic warfare, electromagnetic spectrum control and cyberspace operations. Cyberspace and electromagnetic activities seek to:

- seize, retain and exploit an advantage over adversaries in both cyberspace and the electromagnetic spectrum

[5] *Australian Defence Doctrine Publication 3.13, Information Activities* [Chapter 1].

[6] Signature is defined as the characteristic radiated electromagnetic energy or sonic pattern of the target displayed by detection classification and identification.

[7] Information domain is defined as the aggregate of individual, organisations and systems that collect, process, disseminate, or act on information.

[8] United States Army, *Field Manual 3-38, Cyber Electromagnetic Activities* defines cyberspace and electromagnetic activities as activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. Cyberspace and electromagnetic activities consist of cyberspace operations, electronic warfare and spectrum management operations.

- simultaneously deny and degrade adversary use of cyberspace and the electromagnetic spectrum
- protect mission command systems.

Cyberspace and electromagnetic activities recognise the convergence of cyberspace and electromagnetic operations and seek to ensure orchestration of these activities. They provide a simple model to support planning and to understand the integrated and converged nature of this function.

Information assurance, as another information-related capability, plays an important role in ensuring the protection of friendly information through both procedural and technical activities. These activities aim to protect friendly information while detecting and reacting to challenges to the integrity of information systems, and include:

- controlling access to information and ensuring a consistent approach to the physical protection of information
- the planning, use and management of cryptographic systems (equipment and material)
- identity and certificate management – the use of automated systems to verify an individual’s clearance and authorisation to access information on friendly information and communications technology networks
- the control and allocation of radio waveforms.

Effective emission control and signature management also enhance the protection of friendly force information. Uncontrolled emissions and poor signature management allow adversary intelligence, surveillance and reconnaissance assets to determine friendly locations, orders of battle, patterns of life and indicators of future intentions. The significant number of emitters in a modern networked force results in a requirement for well-considered and well-monitored emission control and signature management plans. These plans must be able to dynamically change in response to operational phases or a changing threat.

While responsibility for emission control and signature management rests with the commander, signals elements provide expert advice to the planning process, and assist with the implementation and monitoring of both plans. These activities support effective operations security, and when tightly coupled with the operational plan can contribute to a commander’s deception plan.

The commander’s deception plan is enhanced through activities such as the simulation of command and control radio nets, the manipulation of traffic loads, the spoofing of adversary command and control links through deceptive imitation, the employment of cyberspace operations effects and social media deception. Some of these activities are signals led; in others signals assets play an enabling or advisory role. In each case they require close orchestration with the commander’s deception plan and any physical deception activities.

Electronic force protection

This function seeks to improve force protection through activities in the electromagnetic spectrum. This includes electronic protection actions, assisting in the defeat of improvised explosive device threats, analysing threat use of the electromagnetic spectrum and the management of electronic countermeasure capabilities.

Electronic protection is an important part of both counter command and control and electronic force protection. Electronic protection includes passive and active measures to protect personnel, facilities and equipment against electromagnetic spectrum threats. While electronic protection is a responsibility of all communications users, the Signals Corps provides a range of capabilities to enhance the electronic protection of the force, such as analysis of adversary electronic warfare capabilities and techniques, situational awareness of the electromagnetic spectrum, and the monitoring of friendly force communications. Effective spectrum management also contributes to the electronic protection effect, minimising the chances of electronic fratricide in a congested environment. The rapid passage of information from a range of threat warning sensors such as radars is also crucial to effective electronic protection.

Force protection electronic countermeasures aim to protect platforms and personnel using sensors and countermeasures to detect, identify, destroy or evade specific threats. Responsibility for the effective planning and use of force protection electronic countermeasures systems lies with both specialist signals personnel and all-corps users. This shared responsibility will increase with the expected increase in the number of platforms with integrated force protection electronic countermeasures systems. The signals capability has the responsibility for the training and management of standalone systems, as well as the ongoing development of threat databases that support both standalone and platform systems.

Training and education

Reaping the full benefits of a technology-enabled force requires the intellectual capacity to blend technical knowledge with operational and tactical acumen. Development of this intellectual capacity requires comprehensive and contemporary training for specialist signallers and across the force. It will also require an increased investment in both intellectual and practical training in contested electromagnetic spectrum environments.

The Army signals capability is responsible for ensuring the provision of quality, contemporary and challenging individual signals training through:

- managing a coordinated approach to all-corps signals training and consistent quality control of all signals training

- continued engagement with industry, ensuring that Army maintains contemporary training and develops personnel who can take advantage of emerging evolutionary, revolutionary and possibly disruptive technologies
- the development and maintenance of effective learning loops that inform individual training, and leveraging the uneven levels of modernisation between elements of the force to rapidly modernise training.

Army must make maximum use of the existing skills in the part-time cyberspace and information and communications technology workforce to reduce the cost of training, harness specialised skills and ensure that Army keeps pace with technology.

In the collective training environment the signals capability must support efforts to provide realistic contested electromagnetic spectrum and cyberspace environments. This requires effective contributions to exercise scenario design and control, and active participation by specialist elements capable of creating a contested environment.

Alignment with combat functions

Land Warfare Doctrine 3-0-3, Formation Tactics identifies six combat functions. These functions describe the range of effects that a force conducting land operations must be able to undertake to plan, conduct and consolidate operations. When integrated, these combat functions aid commanders in orchestrating and directing operations.[9] The Army signals functions contribute directly to the conduct and integration of the combat functions across the force. Table 2–1 demonstrates the alignment between the Army signals and combat functions.

[9] *Land Warfare Doctrine 3-0-3, Formation Tactics*, p.10.

Table 2–1: Alignment of Army signals functions with Army combat functions

Army combat functions	*Signals functions*
Know The capacity to detect, recognise, assess and understand the strengths, vulnerabilities and opportunities available within the operational environment.	Command and control support Situational awareness support Electromagnetic spectrum management Counter command and control support Information exploitation Signals support Cyber- and information-related activities Electronic force protection Training and education
Shape Actions that delay an adversary's response, lead them into inadequate or inappropriate responses, or prompt them to respond in a manner we want.	Command and control support Electromagnetic spectrum management Counter command and control support Cyber- and information-related activities Training and education
Strike Apply precise discriminate, physical or non-physical force, both lethal and nonlethal, in a timely fashion to achieve specific outcomes while minimising unintended consequences.	Command and control support Counter command and control support Information exploitation Cyber- and information-related activities Electronic force protection

Army combat functions	*Signals functions*
Shield Protect friendly forces, infrastructure, local population and other noncombatants where required. Shielding is achieved by measures that include avoiding detection and protecting against physical or non-physical attack.	Command and control support Situational awareness support Electromagnetic spectrum management Counter command and control Network operations Signals support Cyber- and information-related activities Electronic force protection
Adapt To respond effectively to a change in situation or task.	Command and control support Situational awareness support Electromagnetic spectrum management Counter command and control support Network operations Information exploitation Network operations Cyber- and information-related activities Training and education
Sustain Provide appropriate and timely support to all forces from deployment, through the completion of assigned missions, to redeployment.	Command and control support Electromagnetic spectrum management Information exploitation Network operations Signals support Training and education

Chapter 3

Signals planning

Signals and the staff planning process

Planning is the art and science of envisioning a desired future and laying out effective ways of achieving it. It is a command-driven function, and the planning process places detail around the commander's guidance and concept for the operation. Army's approved planning process is the military appreciation process, as detailed in *Land Warfare Doctrine 5-1-4, The Military Appreciation Process*.

The military appreciation process is a continual process that bridges both current and future operations. It may be a deliberate detailed activity or an abbreviated planning response to current events. The process, including the joint military appreciation process, is applicable to the planning staff within strategic and operational headquarters, small tactical headquarters and individuals. In each environment, the military appreciation process provides a method for effective integration of the different battlespace operating systems. This supports the commander's requirements for the synchronisation of forces and the orchestration of effects.

The continuous integration of signals planning staff into the commander's planning process is critical for effective support to manoeuvre, particularly mission command and orchestration. Support to the planning process is a key signals function (command and control support) that requires active, informed and tactically astute input from signals commanders and staff.

Effective signals advice is the result of concurrent and synchronised signals planning which feeds into and is guided by the staff planning process, as represented in Figure 3–1.

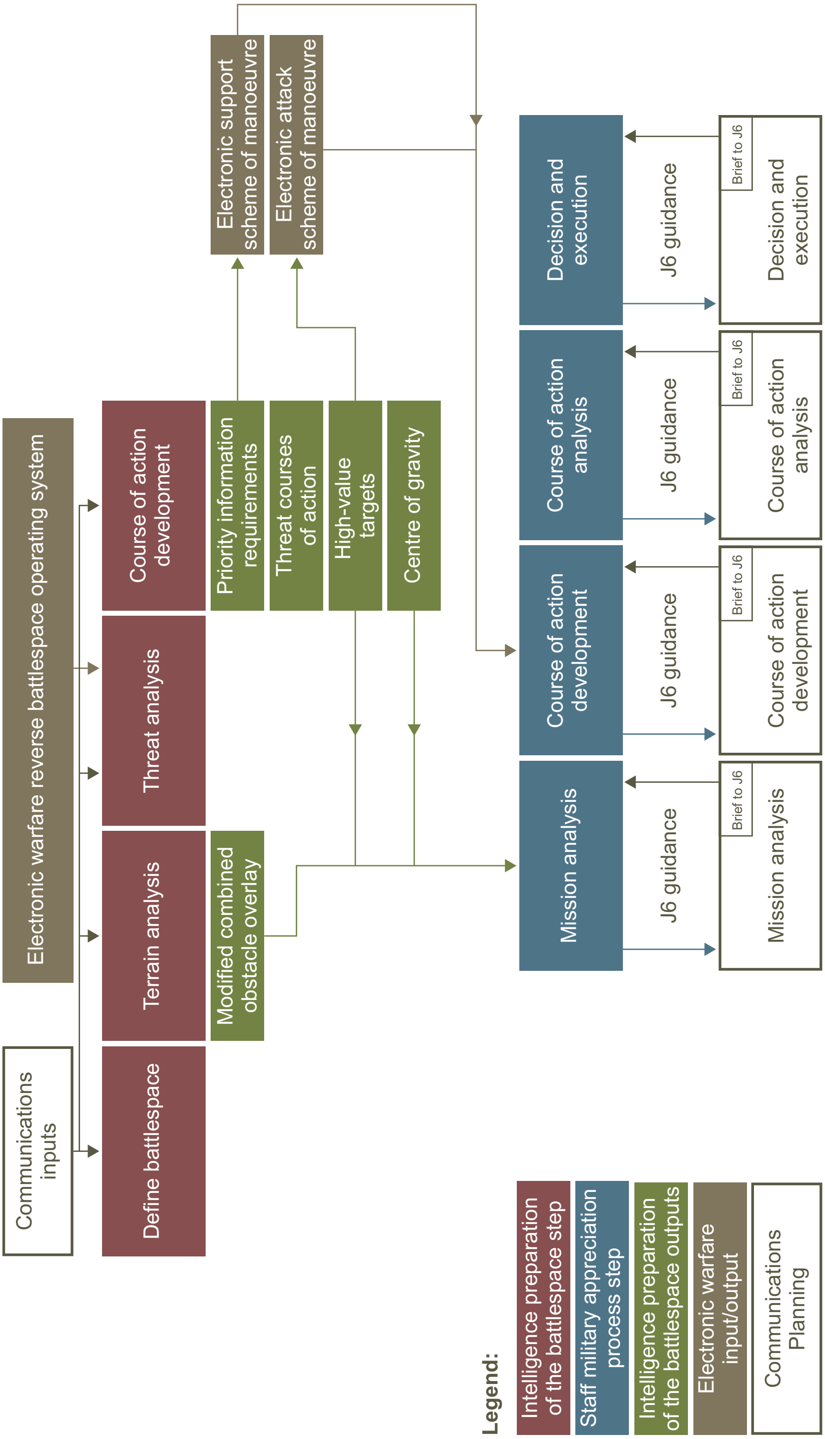
Communications inputs
Electronic warfare reverse battlespace operating system
Define battlespace
Terrain analysis
Threat analysis
Course of action development
Modified combined obstacle overlay
Priority information requirements
Threat courses of action
High-value targets
Centre of gravity
Electronic support scheme of manoeuvre
Electronic attack scheme of manoeuvre
Mission analysis
Course of action development
Course of action analysis
Decision and execution
J6 guidance
J6 guidance
J6 guidance
J6 guidance
Brief to J6
Brief to J6
Brief to J6
Brief to J6
Mission analysis
Course of action development
Course of action analysis
Decision and execution
Legend:
Intelligence preparation of the battlespace step
Staff military appreciation process step
Intelligence preparation of the battlespace outputs
Electronic warfare input/output
Communications Planning

Figure 3–1: Synchronisation of staff and signals planning processes

Signal staff inputs to each step of the military appreciation process include:

- *Intelligence preparation of the battlespace.* Inputs to the intelligence preparation of the battlespace include advice on adversary command and control systems, likely adversary courses of action and critical vulnerabilities (commonly known as reverse battlespace operating system planning); assessments of noncombatant and third-party signals threats (including cyberspace threats); and analysis of the battlespace environment (including the electromagnetic spectrum and cyberspace). This phase requires a clear articulation of information gaps pertaining to signals planning. Electronic warfare staff will also provide advice on the priority information requirements they are able to collect against as part of the broader intelligence collection plan.
- *Mission analysis.* Signals staff inputs to the mission analysis phase include advice on available signals capabilities, limitations and opportunities, and higher headquarters technical control plans and directions. Signallers should advise on critical friendly signals vulnerabilities and the ability to surge or prioritise services.
- *Course of action development.* Signals planners contribute to the development of courses of action through analysis of decisive events and proposed schemes of manoeuvre, command and control arrangements and information flows. This includes identification of the nonlethal options available to support decisive events. Signals planners should also provide input into force protection (both physical and electronic) and deception planning.
- *Course of action analysis.* Signals planners contribute to the analysis of courses of action through participation in the staff wargaming process. Considerations for each course of action include network capacity, security, mobility and protection. While signals considerations should not limit the commander's plan, planners should not shy from identifying risks to effective command and control resulting from a proposed course of action.
- *Decision and execution.* Signals planners contribute to the development of the selected courses of action into an operational order or plan. This includes support to the preparation of warning orders, support to preparation of operational documents, and participation in rehearsals and orders groups. In the execution phase signals commanders and planners must ensure appropriate execution of the signals plan, synchronise refinements to the signals plan as the operation unfolds, enact branches and sequels as required, and exploit any opportunities to improve levels of support. Signals planners also support immediate operations planning in response to changes in the environment, technical issues or adversary actions.

Immediate planning

Plans will change in response to adversary actions, interplay with local populations, changes in own force capabilities and higher headquarters direction. In many cases this will require an immediate planning response. Army's process for immediate planning is the combat military appreciation process, which provides a combat decision-making tool drawing on pre-H-hour planning, existing knowledge of the battlespace, judgement and tactical experience. The combat military appreciation process is an abbreviated four-step process as described in *Land Warfare Doctrine 5-1-4, The Military Appreciation Process*. Signals staff must provide up-to-date and timely specialist input to this process, based on a high level of awareness of the status of the signals capability as well as the current electromagnetic spectrum and cyberspace threat. Signals staff must also ensure that they remain aware of current manoeuvre operations in order to anticipate requirements and prepare for immediate planning cycles.

Signals planning

Active engagement with the staff or commander's planning process allows signals assets to anticipate demands and ensure that the technical signals plan supports the manoeuvre plan. Signals planning must not be seen as a separate process from the operational plan; rather it is complementary and enables both effective signals input into the staff planning process and the development of an integrated signals plan focused on the commander's intent. The commander's intent must be foremost in the development of signals plans, not the achievement of an elegant technical solution.

Australian Defence Force Publication 6.0.1, Communication and Information Systems Planning provides a detailed description of the joint signals planning process, while *Australian Defence Doctrine Publication 3.5, Electronic Warfare* identifies joint electronic warfare planning considerations. *Land Warfare Doctrine 6-1, The Employment of Signals* also details Army processes for signals planning. Broadly, however, the signals planning process supports several outcomes:

- It supports signals input into the commander's planning process by conducting a concurrent and detailed signals appreciation. The outcome of this signals analysis underpins the advice taken forward into the commander's planning process.
- It ensures the integration of the commander's intent into signals plans (communications and electronic warfare plans), orders and control procedures. This includes guidance for users on issues such as information processes, radio nets, network use and emission control.
- It allows for the development of supporting technical plans, collection and analysis plans, directives, databases and control systems.

These outcomes rely upon a sound understanding of the commander’s plan, plus the technical acumen to link manoeuvre requirements with network design and management.

Specific electronic warfare considerations

Specialist electronic warfare planning is usually separate from the communications planning process. This reflects both the different focus of their core tasks – supporting the intelligence function (conduct collection to answer priority information requirements, enhance force protection, and develop high-value targets); and joint fires (disruption, denial, destruction) – and the different process for joint electronic warfare tasking and management. That said, the close linkages between the two mission sets demand a mutually supporting and collaborative approach to ensure a holistic signals effect.

Electronic warfare representation within the staff planning process is critically important, given the specialist nature of many of the electronic warfare effects and the linkages to joint and coalition electronic warfare capabilities. As well as providing input to the staff planning process, electronic warfare participation in the military appreciation process allows for the cueing of long lead-time electronic warfare assets, early deployment of electronic warfare collection assets in support of the commander’s priority information requirements, and improved synchronisation of electronic warfare effects with the commander’s plan.

Joint/coalition considerations

Operating within a joint force or as part of a coalition provides a significant increase in the scale of capabilities that can be brought to bear in support of the commander’s manoeuvre plan. For signals planners there are significant opportunities to increase reach, capacity, redundancy, flexibility and the range of effects. Realising these opportunities, however, requires a sound appreciation of the differing priorities, policy constraints and capabilities of each party. Within a coalition consideration must also be given to the impact of national interests upon the collaborative effort.

Signals planning, particularly within a coalition environment, can be further complicated by different technical standards, different build states of common applications, and differing security compliance requirements. These issues are exacerbated when the coalition is built from nations that are outside the standard alliance framework. Such issues can largely be overcome through early and collaborative planning, and the establishment of joint/coalition signals planning and operations teams. In some cases, there may be a requirement for mission-specific systems and processes to be developed in order to overcome both technical and policy constraints.

Operating within a joint and coalition environment will usually see a greater requirement for centralised control and management of signals operations. This is necessary to ensure that local decisions and actions do not impact across a joint or coalition network, and in the worst case lead to a loss of connectivity or access to joint or coalition capabilities and information. The loss in local freedom of action and sense of priority from a centralised approach will usually be offset by access to capabilities, and the resultant information far greater than that available locally.

Planning considerations

Some planning considerations will apply in almost all circumstances. These include:

- *Threat focus.* Signals planners at all levels must remain threat focused. The operating environment requires dynamic management of signals in the face of adaptive opposition and multiple means of communication and disruption. This requires a thorough analysis of the threats presented by the adversary as well as by noncombatant and third-party elements. Such an analysis allows for the adoption of an appropriate defensive posture and the development of proactive actions and effective response plans. A threat focus also ensures the effective integration of an adversary's command and control vulnerabilities into ongoing manoeuvre planning.
- *Technical control.* A range of technical constraints, imposed through the separate signals and electronic warfare technical control chains, will impact on signals planning. These constraints result from domestic and international laws and agreements (such as satellite landing rights or information release restrictions), national interests and alliance considerations, as well as the requirements of higher headquarters. Chapter 4 discusses the issue of technical control in greater detail.
- *Time.* The time line for the staff planning process and development of the operational plan defines the time available for specialist planning. There will usually be limited time for signals-specific planning. Planning under tight time constraints requires a simple and well-practised process and a high level of situational awareness.
- *Equipment constraints.* Austerity will remain a characteristic of deployed signals support, particularly in the early phases of an operation or in a highly mobile activity. The demand for services will often outstrip the capacity, capabilities and/or quantity of equipment. In some cases, the equipment available may not be suitable for the proposed task. A thorough understanding of equipment capabilities and network capacity is critical.
- *Signals principles.* Planners should not slavishly apply the signals principles detailed in Chapter 1. That said, the principles represent the collected experience of generations of signallers and lessons drawn from operations. As such they provide a useful reference for planners, particularly when developing and analysing signals courses of action.
- *Compliance requirements.* Signals planning will occur within several compliance frameworks. These may be legislative (such as information management or electrical safety standards), technical (such as cryptographic or electronic warfare technical compliance) or due to the

expectations of coalition partners. Planning and operating within these compliance regimes is part of a professional approach to signalling. They support effective security and interoperability and, in many cases, enable access to sensitive capabilities. Complying with recognised standards is also fundamental to enabling information exchange between joint and coalition partners.

Chapter 4

Signals staff relations and technical control

The commander

A strong relationship between the senior signals leader and the supported commander is fundamental to the success of the signals mission. It ensures that the commander has confidence both in the assigned signals capability and that these capabilities will be focused upon supporting and enhancing their manoeuvre plan. Such a relationship also improves the signals staff's understanding of the commander's intent and their ability to anticipate requirements. The development of an effective relationship requires senior signals staff to demonstrate both technical and tactical competence and add value to the key headquarters processes.

The signals and staff relationship

The synchronisation and effective conduct of the signal functions also require an effective working relationship with headquarters staff. Signals staff should work actively to develop a trusted and valued relationship with the headquarters staff. This enables effective information flows and leads to improved levels of support. It increases the ability to anticipate changes and enables a more proactive approach to resolving issues.

Operations and plans staff

The relationship between signals staff and headquarters operations and plans staff must support a two-way flow of information. Active participation by signals staff in the headquarters battle rhythm ensures these information flows and supports effective integration.

The signals staff's responsibilities to headquarters operations and plans staff include:

- input to immediate and deliberate planning, including time-sensitive planning
- the provision of signals instructions in operational tasking documents
- an agile, active response to communications outages and technical issues
- advice on emission control and operations security

- assistance with the development of effective information exploitation/management processes
- advice on the employment of signals services and any specialist assets
- advice and planning regarding the movement and defence of the headquarters
- advice regarding cyberspace operations consideration in both current and future operations.

The key responsibilities of operations and plans staff include:

- early advice on changes to plans or operational requirements and impending moves of the headquarters
- advice on the priority of services within the headquarters during establishment, moves and outages
- support in the development and enforcement of information processes, emission control and operations security plans
- support for signals staff involvement in staff planning processes
- provision of a release authority for technical control directions
- advice on changes to operational control measures as they relate to remote detachments.

Intelligence staff

The relationship with intelligence staff reflects the mutual support required between signals and intelligence assets as well as the direct contribution to the intelligence function provided by specialist electronic warfare assets. Added importance is placed on the relationship by the reliance on specialist networks and applications by the intelligence staff.

The signals staff's responsibilities to the intelligence staff include:

- support to intelligence information exchange and dissemination requirements, including security and compliance assurance
- support to and, where appropriate, integration of specialist networks and applications, including analytical applications
- the provision of data storage, search and retrieval capabilities to enhance intelligence analytical capabilities
- support to the communications infrastructure for surveillance and reconnaissance assets
- the inclusion of adversary command and control and electronic warfare (reverse battle operating system) analysis in intelligence planning
- the provision of electronic warfare staff to support all-source intelligence development

- the provision of specialist electronic warfare collection assets to answer priority information requirements and threat warnings
- the development of electromagnetic spectrum-based target sets.

The intelligence staff's responsibilities to the signals staff include:

- support for the development of an understanding of the electromagnetic spectrum and cyberspace environment and threats
- the provision of clear intelligence collection priorities to support electronic warfare planning
- well-defined user requirements for specialist intelligence systems, including analytical tools and data storage
- well-defined user requirements for information exploitation/management planning and assistance in developing effective information exchange architectures
- intelligence support to the force protection of signals assets
- intelligence inputs into the development of emission control and electronic force protection planning.

Joint fires cell

The signals staff contribute to joint fires operations through:

- support to joint fires networks through electromagnetic spectrum control, the provision of network redundancy, situational awareness support, and the establishment, operation and management of joint fires networks by regimental signallers and mission system operators
- the provision of specialist capabilities, including the identification and selection of targets through electronic support and electronic protection and strike-through electronic attack, noting that electronic attack within a manoeuvre formation is coordinated by the joint fires and effects coordination centre with specialist advice from electronic warfare staff.

At the same time, the joint fires network represents a significant communications asset, particularly in the tactical battlespace. The scale of the network presents opportunities for improved communications redundancy as well as mutual support and the efficient use of scarce communications assets. A collaborative approach to realising these opportunities requires appropriate signals input into the joint fires planning process.

Other staff cells

Army aviation. Army aviation represents both a significant collection capability and a significant user of information. Many Army aviation communications systems are bespoke, and hence effective information exchange requires close planning between signals and aviation staff. A collaborative approach is also vital when planning ground-to-air, airspace coordination and air casualty evacuation communications. A sound relationship also allows the identification of opportunities for aviation to support signals reconnaissance and the placement, resupply and evacuation of remote detachments.

Combat service support staff. The combat service support capability is heavily reliant on data. Combat service support elements will typically rely on bespoke systems and applications, often designed to support in-barracks logistics, maintenance, medical and civilian contractor requirements. Combat service support information exchange requires early and detailed planning supported by an active relationship between the signals and combat service support staff. This relationship is of added importance given the substantial increase in tactical communications systems within combat service support units as well as the increase in onboard vehicle diagnostic systems.

Joint and coalition elements. The development of effective information flows across disparate joint or national networks and/or applications requires early, effective and collaborative planning between respective staff. Access to joint and coalition assets requires a sound understanding of the relative capabilities and an awareness of their availability. Planning and situational awareness requires a trusted relationship between joint and coalition signals staff. The effective employment of technical control across a joint or coalition force also requires effective relationships between signals and command staff.

Signals support

The signals support function is enhanced as a result of effective relationships between the supported headquarters staff and the supporting signals unit. This is particularly the case with the provision of first-line logistics to the headquarters and movement and defence of the headquarters. An effective relationship ensures:

- early advice of planned moves
- a clear understanding of the priority of services (including opening and closing times for communications)
- a collaborative approach to the development of the headquarters battle rhythm, logistic procedures and security plan.

The provision of signals

The widespread adoption of digitisation and information-enabled platforms across Army sees a greater mix of specialists and non-specialists within the overall Army signals capability. Lines of responsibility are less well defined and the boundaries between strategic and deployed systems are increasingly blurred. As such the provision of specialist signals capabilities is based on a balance between the task requirements and the availability and organisation of equipment and personnel.

Communications

The Royal Australian Corps of Signals generally provides communications support from joint task force headquarters or formation headquarters down to unit headquarters. Internal-to-unit communications is generally the responsibility of unit personnel. Unit personnel include Signals Corps members on unit establishment, regimental signallers and/or mission system operators. In some units, additional Signals Corps support is provided for the establishment and maintenance of internal Battle Management System – Command and Control networks.

Within Special Operations Command, Signals Corps elements provide support from the operational level down to the tactical level, usually as part of task-organised teams.

Electronic warfare

Specialist electronic warfare units provide force-level capabilities responsible for answering priority information requirements or supporting force-level joint fires outcomes. Electronic warfare assets may be assigned to subordinate units as a way of integrating them into the manoeuvre plan, but will not necessarily be tasked to provide any support to the assigned unit. Often intimate support will be provided to the unit as a by-product of co-location. The command and tasking authorities must be clearly understood in these circumstances.

All-corps units retain the responsibility for the conduct of electronic protection and, where required, the conduct and local management of force protection electronic countermeasures.

Command authorities

To effect command and control across a force it is common for a commander to assign signals elements to subordinates. The command status used to assign the elements reflects the commander’s intent to maintain technical control or the tasking authority. Usually conventional signals elements are assigned in a manner that retains command and the tasking authority with the senior commander but recognises the requirement for local tactical direction (such as operational control). A command authority (such as tactical command) may be used if the commander has assigned the signals element to a subordinate commander for intimate support to the subordinate’s mission.[1]

Command arrangements for assigned signals elements will also normally include the direction ‘for local administration less specialist repair’. This implies that the supported unit is responsible for the provision of rations, water, ammunition, fuel and the repair of common items, but not for the repair of specialist signals

[1] Operational control is the authority delegated to a commander to direct forces assigned to them in order to accomplish specific missions or tasks that are usually limited by function, time or location. Tactical command allows a commander the freedom to task forces to achieve an assigned mission and to group and regroup forces as required within the assigned force structure. Command authorities are explained in detail in *Australian Defence Doctrine Publication 00.1, Command and Control*.

equipment. It is also possible that commanders will have a local administration responsibility for a signals asset in their location that, while part of the force commander's command and control network or electronic warfare capability, provides them with no local service.

Technical control

Technical control is not a command authority. It is defined as an administrative authority that allows for the provision of specialist and technical advice for the management and operation of forces. In a signals context, it allows for the senior headquarters to effectively manage and maintain the signals capability across the operational theatre. In the contemporary environment it also enables the detailed control of compliance and assurance for information and communications technology systems, software-programmable radios, and cyberspace and electronic warfare operations. It is normal for the commander to delegate technical control of the signals capability to the senior signals commander in the force. As such, technical control is exercised on behalf of the commander, and must reflect both the commander's intent and established policy.

Signals technical control supports the principle of centralised control and decentralised execution. The centralised control model allows for the necessary degree of configuration management, technical guidance, compliance and control across a theatre or area of operations. It supports the senior commander's command and control of the force. Centralised control is particularly important in a heavily connected and technology-enabled joint and/or coalition force operating in a contested and congested environment.

Decentralised execution allows for the local, direct management of assigned signals assets in accordance with the superior commander's intent. This allows freedom of action at lower levels and can increase agility. Decentralised execution relies on a clear understanding of the varying levels of responsibility and authority at the differing levels of command, and strong feedback loops through the signals reporting chain.

Signals technical control operates within an existing framework, as outlined in *Australian Defence Doctrine Publication 6.0, Communication and Information Systems* and *Australian Defence Doctrine Publication 3.5, Electronic Warfare*. Both documents provide significant detail regarding the joint technical control process for communications and electronic warfare. Figure 4–1 and Figure 4–2 detail the indicative technical control for both mission sets.

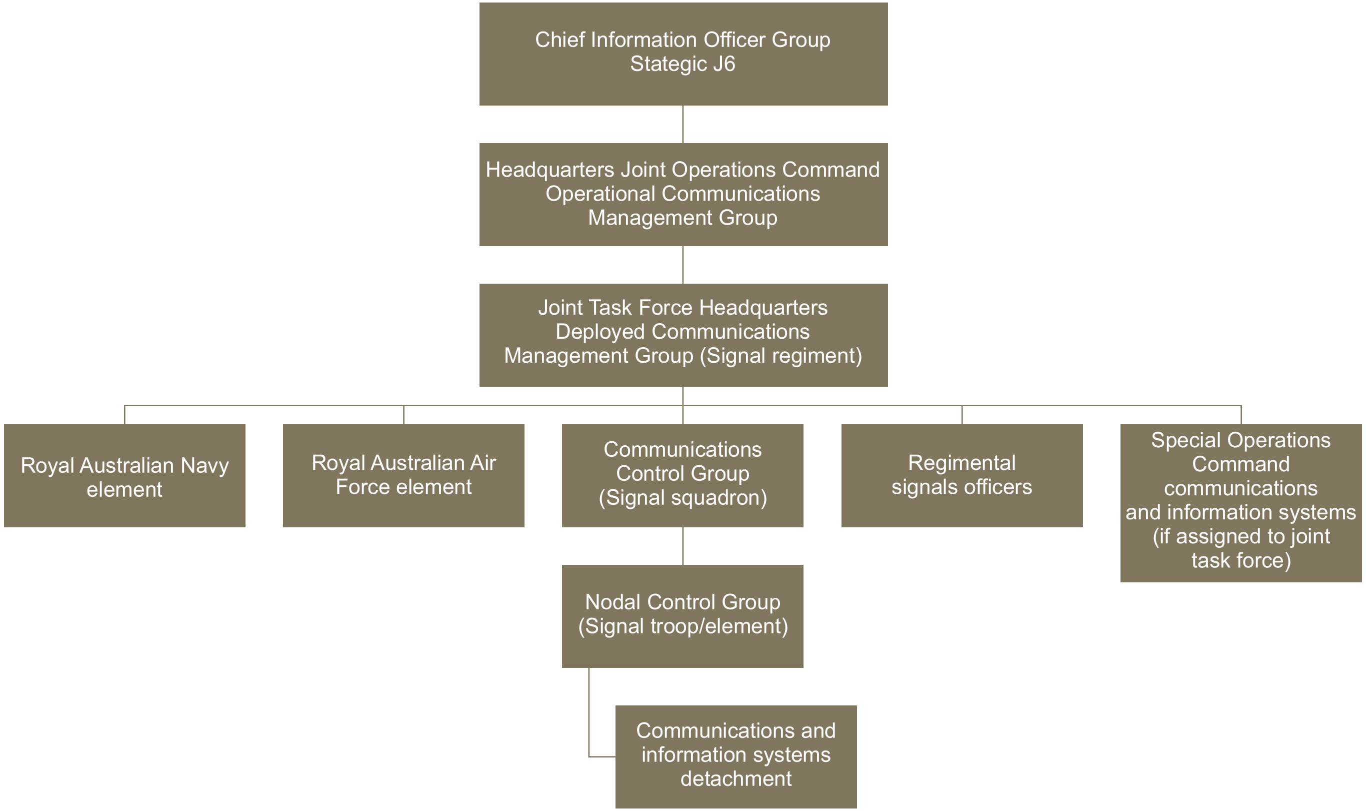
Chief Information Officer Group Stategic J6
Headquarters Joint Operations Command Operational Communications Management Group
Joint Task Force Headquarters Deployed Communications Management Group (Signal regiment)
Royal Australian Navy element
Royal Australian Air Force element
Communications Control Group (Signal squadron)
Regimental signals officers
Special Operations Command communications and information systems (if assigned to joint task force)
Nodal Control Group (Signal troop/element)
Communications and information systems detachment

Figure 4–1: Indicative technical control for communications

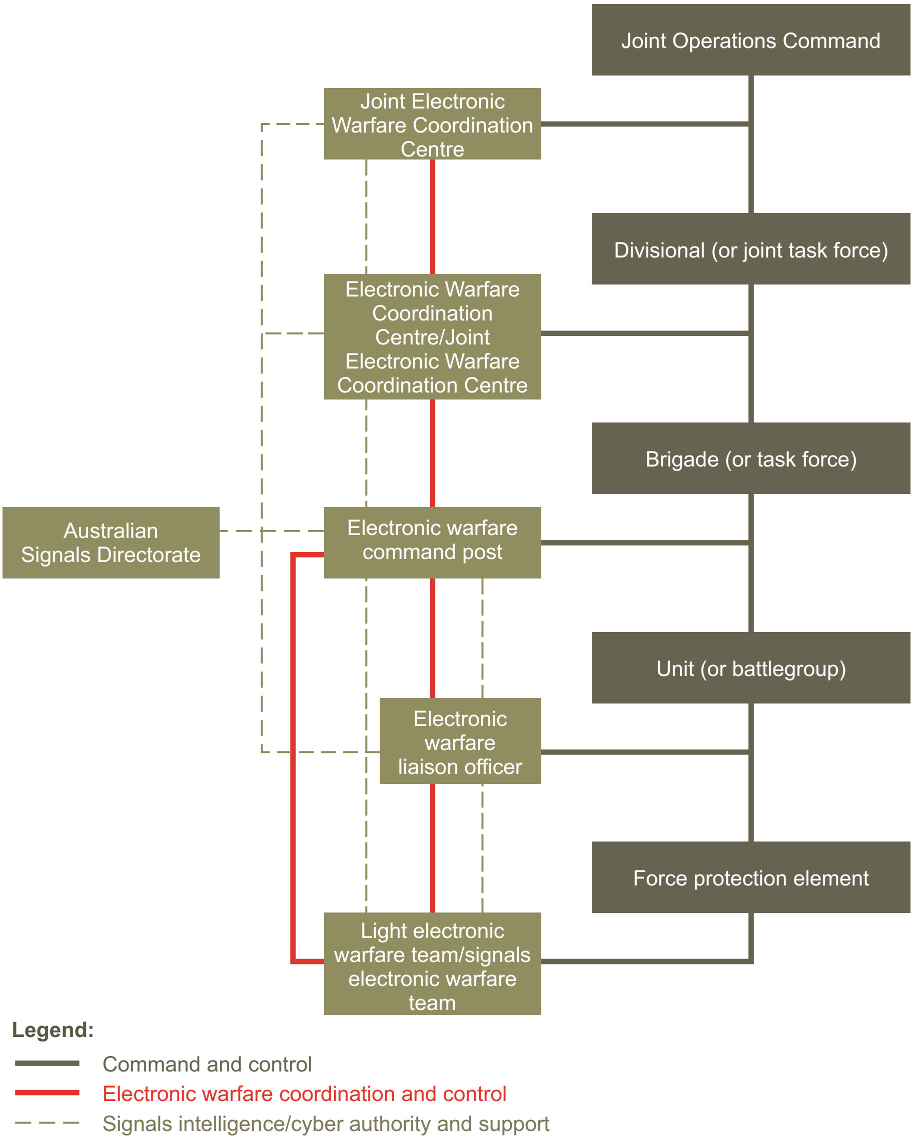
Joint Operations Command
Joint Electronic Warfare Coordination Centre
Divisional (or joint task force)
Electronic Warfare Coordination Centre/Joint Electronic Warfare Coordination Centre
Brigade (or task force)
Australian Signals Directorate
Electronic warfare command post
Unit (or battlegroup)
Electronic warfare liaison officer
Force protection element
Light electronic warfare team/signals electronic warfare team
Legend:
Command and control
Electronic warfare coordination and control
Signals intelligence/cyber authority and support

Figure 4–2: Indicative technical control for electronic warfare

Characteristics of signals technical control

Reporting requirement. Effective signals technical control relies on sound situational awareness of:

- the network status and configuration
- anticipated changes to operational plans
- the status and location of capability bricks
- early advice of future reinforcement requirements.

This implies a reporting process that provides a consolidated operating picture at each level of responsibility. Reporting is a key responsibility of network operations and the electronic warfare command elements.

Theatre-wide management. The purpose of technical control is to ensure the most effective, efficient and secure use of capabilities across a theatre and within an area of operations in support of the senior commander's manoeuvre plan. Signallers should expect that the technical control chain will impose theatre-wide standards and configuration management processes. These may not best suit local circumstances; however, disregarding these directions may have theatre- or enterprise-wide implications. While signals personnel should ensure that the implications are understood by local commanders, dispensation may only be granted through the higher headquarters.

Planning constraints/opportunities. Centralised control places constraints on the employment of signals capabilities. These require clear articulation during the planning process. At the same time, a centralised control model allows the senior headquarters to reinforce the main effort, apply reserves and additional capabilities to resolve issues, and coordinate joint and coalition support. This may provide additional freedoms of action to subordinate signals elements.

Command tension. It is common for tension to be experienced between technical control directions and the local commander's intentions. In the worst case, the centralised management model may place limitations upon the local commander's plan. Signals staff must be able to provide clear and accurate reasons for technical control decisions, articulate the risk of disregarding the directions, and confirm the requirement to seek dispensation through the higher headquarters. The tension between local intentions and the constraints and limitations imposed by higher headquarters is one reason why close integration of technical control with the command chain is vital. For best effect all technical control directions should be released through the common headquarters tasking process.

Conclusion

While the nature of warfare is enduring, its character evolves, often in response to developments in society and advances in technology. Contemporary warfare demonstrates increased complexity within the operational environment, including in cyberspace and the electromagnetic spectrum. This requires an Army signals capability that has both a sound understanding of the foundation signals concepts and the cognitive agility and foresight to take advantage of the opportunities presented by technological advances. At the same time, the environment demands a threat focus, anticipating a continual contest for access, control and dominance across cyberspace and the electromagnetic spectrum.

It is recognised that Army's operations will be conducted within a joint setting as the norm, often with coalition and/or interagency partners. An effective information exchange between joint organisations and mission partners is crucial for the synchronisation of joint effects. This requirement impacts on almost all aspects of the Army signals capability, from capability development, planning, technical control and each of the signals functions.

The 10 enduring signals functions capture the output required of the Army signals capability, regardless of where on the spectrum of conflict an operation may occur. The functions provide a holistic view of individual activities and capability bricks which, when brought together, achieve the required effects. The functions are mutually supporting, and the emphasis upon a particular function will be dependent on the type and phase of the operation. The effective harnessing of the signals functions in support of the commander's intent requires sound collaborative planning between headquarters staff and signals leaders, advisers and specialist staff.

This collaborative approach is built on sound relationships between signals practitioners and the supported commander and staff. Such relationships are based on the technical and tactical competence of signals leaders and specialist staff. Equally important is effective technical control, an authority exercised on behalf of the commander, in order to ensure effective management, compliance and maintenance of communications and electronic warfare assets.

Fundamentally, effective signals operations in support of the commander's intent require a collaborative approach between digitally literate commanders and staff and dynamic signals practitioners who are technically and tactically astute. *Land Warfare Doctrine 6-0, Signals*, positions Army to achieve such a collaborative and integrated approach through the provision of a common understanding of the Army signals capability, in particular the underpinning concepts, principles and higher level processes. Importantly, it also explains how the Army signals capability is guided by Army's manoeuvrist philosophy and how that philosophy contributes to Army's combat functions.

While many of the concepts and principles are founded upon lessons drawn from both historical and contemporary operations, the document looks forward to address the opportunities and threats presented by advances in technology. It recognises the new information-related capabilities that will enter the Australian Defence Force across the next decade, and seeks to position Army to best realise the opportunities while guarding against the threats. It allows Army to debate the future of the signals contribution while maintaining a strong intellectual foundation for the Army signals capability.

References

Army Headquarters, *Future Land Warfare Report*

Army Headquarters, *Land Cyberspace Operations Strategy*

Australian Defence Doctrine Publication 00.1, Command and Control

Australian Defence Doctrine Publication 3.5, Electronic Warfare

Australian Defence Doctrine Publication 3.13, Information Activities

Australian Defence Doctrine Publication 6.0, Communication and Information Systems

Australian Defence Force Publication 6.0.1, Communication and Information Systems Planning

Cohen EA and Gooch J 2011, *Military Misfortunes: The Anatomy of Failure in War*, 2nd revised edition, The Free Press, New York

Land Warfare Doctrine 1, The Fundamentals of Land Power

Land Warfare Doctrine 2-0, Intelligence

Land Warfare Doctrine 3-0-3, Formation Tactics

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

Land Warfare Doctrine 6-1, The Employment of Signals

United States Army, *Field Manual 3-38, Cyber Electromagnetic Activities*

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

Tables