New Zealand
DEFENCE
FORCE
Te Ope Kātua O Aotearoa

New Zealand Defence Doctrine Publication

COMMUNICATION AND INFORMATION SYSTEMS

NZDDP–6.0

New Zealand Government

COMMUNICATION AND INFORMATION SYSTEMS (NZDDP-6.0)

New Zealand Defence Doctrine Publication *Communications and Information Systems* (NZDDP-6.0) is issued for use by the New Zealand Defence Force and is effective forthwith for guidance in defence doctrine.

T.J. Keating
Lieutenant General
Chief of Defence Force
Headquarters New Zealand Defence Force
Wellington

October 2016

CONDITIONS OF RELEASE

AUTHORISATION

Headquarters New Zealand Defence Force is responsible for publishing doctrine and maintaining a hierarchy of such publications. Users wishing to quote New Zealand doctrinal publications as reference material in other work should confirm with the Deputy Director Doctrine whether the publication and amendment state remain extant. Comments on the factual accuracy or proposals for amendment should also be directed to the Deputy Director Doctrine at:

The Doctrine Cell
Directorate of Future Force Development
Headquarters New Zealand Defence Force
Freyberg House
2–12 Aitken Street
Wellington
New Zealand

DTelN:	349 7477
Telephone:	+64 4 496 0477
Facsimile:	+64 4 496 0699
Email:	nzdf.doctrine@nzdf.mil.nz
NZDF intranet:	http://www.nzdf.mil.nz

CUSTODIAN
Chief Communications and information Services
Headquarters New Zealand Defence Force

PREFACE

Scope

NZDDP-6.0 —*Communication and Information Systems* provides the philosophical basis for communicatons support to New Zealand Defence Force (NZDF) campaigns and operations. It also provides for sustainment of NZDF Communication and Information Systems and electromagnetic spectrum support for effective command and control of operational forces.

NZDDP-6.0 provides a framework for understanding the conduct of effective Communication and Information Systems and electromagnetic spectrum support to operations and for the management of information needed by commanders at all levels. It provides the necessary military guidance for the exercise of authority and the preparation of Communication and Information Systems related plans with consistent objectives and vision.

Purpose

The aim of NZDDP-6.0 is to present a consistent foundation for the planning, sustaininment, and in-service management and use of Communication and Information Systems infrastructure and related services by the NZDF, especially for the transfer and management of information by the NZDF.

This publication also provides the necessary linkages between the Defence Information Environment, NZDDP-D *New Zealand Defence Doctrine* (3rd Edition), and the other doctrine series. It introduces the subordinate application/procedural documents forming the subordinate 6 Series doctrines. The Defence Information Environment encompasses the computing and communications infrastructure of the NZDF, along with the people, skills, documentation, and management systems that deliver that infrastructure.

Application

NZDDP-6.0 applies across the mission spectrum from peace to war. It therefore is a guide to commanders and planners within the NZDF.

Structure

NZDDP-6.0 Communication and Information Systems comprises 3 chapters:

- Chapter 1: The Fundamentals
- Chapter 2: Information Exchange and Assurance
- Chapter 3: Planning, Engineering, and Technical Control

ACKNOWLEDGEMENTS

The New Zealand Defence Force acknowledges its intellectual debt in preparing this publication to the following military doctrinal publications:

- ADDP-6.0 *Communications and Information Systems* (2nd Edition), June 2012, Australian Department of Defence, Canberra, Australia
- JDP-6.00 *Communications and Information Systems Support to Joint Operations* (3rd Edition), January, 2008, Ministry of Defence, London, United Kingdom

CONTENTS

LIST OF ILLUSTRATIONS

Figure *Page*

EXECUTIVE SUMMARY

Chapter One: Fundamentals

Chapter One describes the strategic guidance for the New Zealand Defence Force's (NZDF) communication and information systems (CIS) philosophical and application doctrine. It outlines the basic principles of CIS support. Information is a critical resource for commanders at all levels. Its management and use in military operations are integral to success. The chapter further explains the functions of the Defence Information Environment (DIE). The DIE is a capability that consists of the data and information used by the NZDF for its business activities and military operations along with the means by which it is created, managed, manipulated, stored, and disseminated in and across all security domains. It includes all the NZDF's capabilities involved in the exchange of data, such as fixed, mobile, standalone, and deployable networks, and user devices and their support services. This includes NZDF services hosted on external servers. The NZDF's military capability depends on a commander's ability to seamlessly access intelligence, logistical, and personnel information to make strategic and tactical decisions. Effective information management provides a competitive advantage in determining an accurate situation understanding, rapid decision-making, and the precise application of force over adversaries. Defence's network planners at all levels of command and management need to take the principles of CIS support into consideration if they are to provide robust and flexible CIS support to the NZDF.

Chapter Two: Information Exchange and Assurance

Chapter Two introduces, in general terms, how information is exchanged and assured in the NZDF. The ways in which information is shared and protected play a vital part in ensuring that commanders have the information they need to maximise the effect of NZDF operations. Information exchange is concerned with how information circulates within the NZDF, and externally to our partners, allies, and other recipients of defence information. Information exchange is the formal or informal transmission of information from, to, or within an information environment. Information exchange can be conducted using electronic or physical means and in fixed or deployed environments spanning all security domains. Communications networks include strategic and tactical communications. Interoperability of CIS is very important in the context of joint and multinational operations. Information Assurance (IA) protects information and information systems and involves both active and passive measures. IA also includes monitoring CIS to maintain security, as well as measures required to respond to incidents.

Chapter Three: Planning, Engineering, and Technical Control

Chapter Three identifies the principles and responsibilities for CIS planning. It provides an overview of CIS design and engineering, including electromagnetic spectrum (EMS) management, and it identifies the principles and responsibilities for technical control and management of CIS assets. CIS must be carefully planned and managed to effectively support operational concepts. CIS technical control, which is based on the principles of centralised management and decentralised execution, has a fundamentally important relationship to command. CIS planning is a vital part of the appreciation process. Provision and engineering of CIS is often complex due to the kinf the equipment and systems involved. The radiofrequency (RF) spectrum is essential for the conduct of flexible, mobile military operations, and support activities. RF spectrum management is vital for effective use of the electromagnetic spectrum (EMS) by Defence.

CHAPTER 1: FUNDAMENTALS

CONTENTS

Figure 1-1: A communication system is defined as an assembly of equipment, methods, procedures, and personnel organised to accomplish information transfer functions.

Introduction

1.01 The availability of accurate and timely information is fundamental to the effective prosecution of military action. The New Zealand Defence Doctrine Publication (NZDDP) *New Zealand Defence Doctrine* notes "information enables the application of the three elements of national power; diplomatic, military, and economic". The dissemination of information, in accordance with a cross government information strategy, enables diplomatic, economic, and military influence to be exerted in an effective and comprehensive way. The right information needs to be delivered to the right place, at the right time and in the right form, as this enables the New Zealand Defence Force's (NZDF's) capabilities in the maritime, land, air, and space domains. The acquisition, operation, and support of information systems, and the recruitment, training, and retention of the skilled people who provide these capabilities, require effective management and coordination. The concept of 'information superiority' centres on the elements of the fighting force being interconnected at the tactical and operational levels, by a robust network of communication and information systems (CIS), that is capable of disseminating and presenting the data required by that force.

1.02 The NZDF depends on achieving decision superiority to provide a 'force multiplier' effect. The capacity of the NZDF's CIS to deliver a global network that enables commanders to execute effective command and control (C2) and provides an accurate situation picture to our commanders, seamlessly and securely across many platforms, contributes significantly to the successful achievement of the NZDF's mission. The provision of mobile, robust, and reliable C2 requires that communication systems and information systems – thystem systems components of the term CIS – are closely coordinated to transfer and present data to the users of those systems, which allows for rapid conversion of data into useful information.

Key Term

Communication and Information System

An assembly of equipment, procedures, and personnel organised to accomplish data transfer and information processing functions.

Benefits of Effective Command and Control

1.03 The terms 'command' and 'control' are closely related and are regularly used together. However, 'command' and 'control' are not one and the same.

1.04 **Command**. Command is the legal authority given to an individual to direct, coordinate, or control armed forces. It is the process of a commander imposing their will and intentions on subordinates to achieve assigned objectives. Command encompasses the authority and responsibility for deploying and assigning forces to fulfil their missions. Decision-making is a prime manifestation of command, as making major decisions is a commander's key duty.

1.05 **Control**. Control is inherent in command. To control is regulating forces and functions to execute the commander's intent. Control of forces and functions helps commanders and staff define requirements, allocate forces, and integrate efforts. Control allows commanders freedom to operate, delegate authority, and place themselves in the best position to observe, assess, and lead. It provides commanders means to effectively and efficiently employ joint forces to achieve objectives and attain desired end-states.

1.06 **Command and Control System**. The NZDF C2 System involves people, processes, technology, and information working for effective decision-making to maximise positive operational outcomes for the government of New Zealand. The C2 benefits chain is shown in Figure 1-2. Each step has its people, process, technology, and information component and each relies on the effectiveness of the step below it.

Command and Control Functions

1.07 Effective C2 relies on having people and technology to support the five functions, consisting of 20 processes, shown in Figure 1-3. Visualisation of C2 as a series of processes enables a systems vi what the overall process of commanding and controlling and the relationships between the functions and their processes.

1.08 The five C2 functions are detailed in the bullets below.

- **Conduct Joint Intelligence** – processes used to direct, collect, analyse, and disseminate information to facilitate assessments of operating environments.
- **Develop Situational Understanding** – processes used to help develop accurate interpretations of situations and the likely actions of groups and individuals within them.

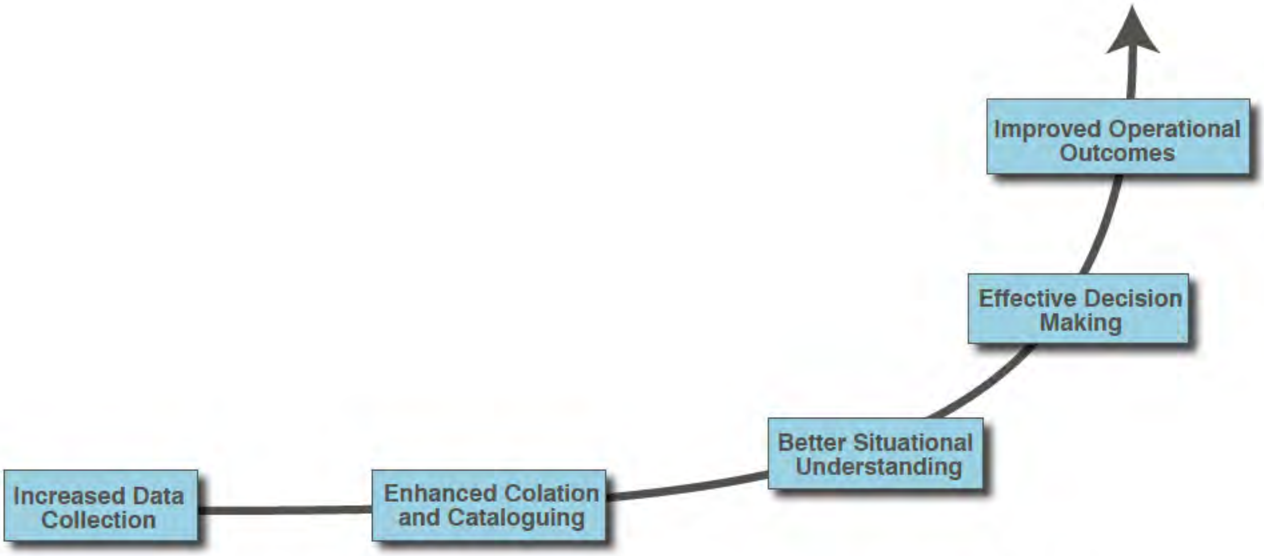

Increased Data Collection
Enhanced Colation and Cataloguing
Better Situational Understanding
Effective Decision Making
Improved Operational Outcomes

Figure 1-2: New Zealand Defence Force Command and Control Benefits Chain.

- **Conduct Joint Planning** – processes for developing options to combat adversaries courses of action and achieve mission objectives in operating environments.
- **Monitor Operations** – processes necessary for monitoring the conduct of operations and reporting operational outcomes.
- **Conduct Command and Control** – processes for executing effective C2 over assigned forces.

New Zealand Information and Communications Technology Environment

1.09 The NZDF is required to operate within New Zealand's Information and Communications Technology (ICT) environment. The NZDF has very little control of the national ICT environment so it must remain adaptable in order to maximise the opportunities that are available to execute its operations and activities.

1.10 New Zealand's ICT environment is overseen by the Government Chief Information Officer (GCIO). The GCIO is responsible for leading government ICT in order to improve services and service delivery, generate efficiencies across departments, develop expertise, and capability across the Public Service, and ensure business continuity.

1.11 The operating model that has been established by the GCIO is intended to provide a system-wide coordination of investment, resources, and capabilities. The operating model is also designed to develop business leaders across the system that can harness the full potential of technology and leverage information assets for transformative gains. The GCIO provides the ICT assurance function across government and is responsible for assurance oversight of ICT projects. The NZDF has taken an active role, observing and contributing to many of the initiatives that could be aligned to NZDF's mission. The NZDF factors evolving ICT initiatives into its Information Systems Strategic Plans (ISSPs).

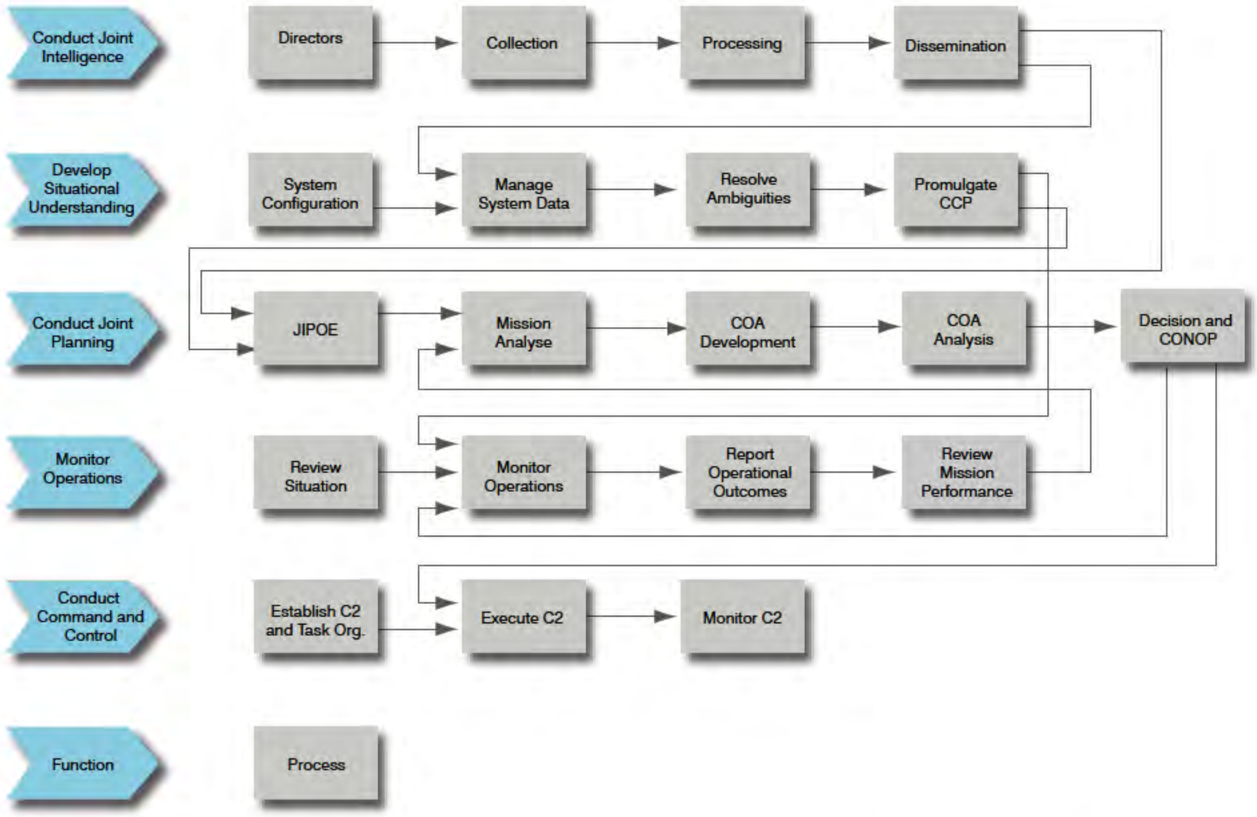


Figure 1-3: New Zealand Defence Force Command and Control Functions and Processes.

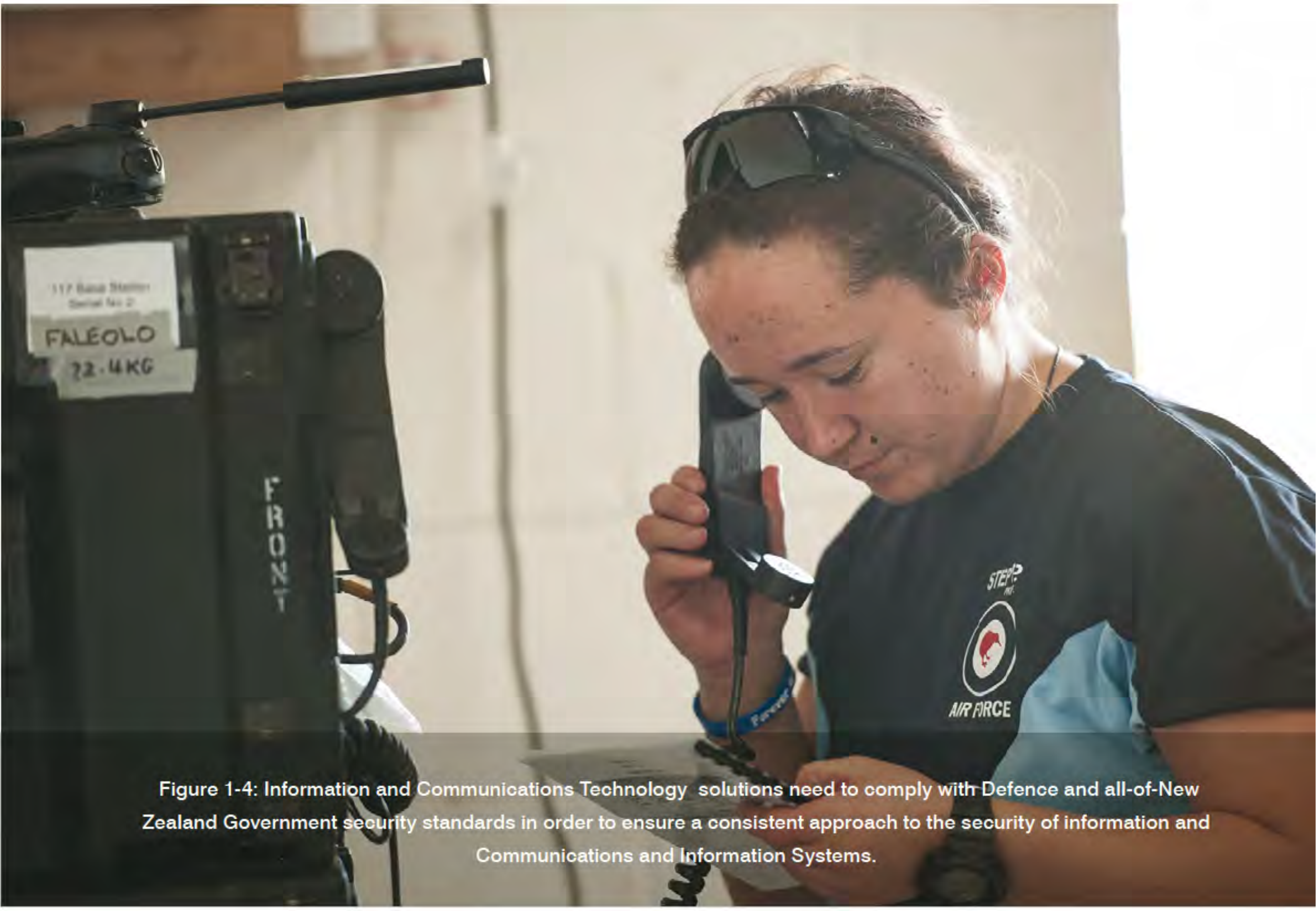


Figure 1-4: Information and Communications Technology solutions need to comply with Defence and all-of-New Zealand Government security standards in order to ensure a consistent approach to the security of information and Communications and Information Systems.

1.12 The NZDF aligns its ICT portfolio with appropriate GCIO driven initiatives and directives. This is under constant monitoring and reporting action. Engagement is through the NZDF Chief Communications and Information Services (CCIS). This single interface point ensures consistency and coherence across all GCIO directed initiatives. There may be exceptional occasions when the GCIO (as Chief Executive of the Department of Internal Affairs) communicates at a peer level with CDF.

Information and Communications Technology's Impact on Operations

1.13 The ongoing development of ICT capabilities is creating both opportunities and challenges for the NZDF. Improvements to the NZDF's ICT enhances decision-making and operational effectiveness. However, emerging and relatively inexpensive ICT capabilities of potential use to the NZDF will also be available to adversaries and the public. The NZDF continues to develop, deploy, and exploit advanced ICT to operate successfully in the operational environment. Defence leverages ICT capabilities to plan and implement the full spectrum of tasks assigned to it by government, connecting all-of-nation capabilities in an environment of increased uncertainty and reduced warning times. Defence continues to develop its holistic approach to ICT capability, integrating both military and business functions so that technology enables the information access and functionality needed to accomplish its mission. To support this, the NZDF continuously monitors and improves the quality of the Defence Information Environment (DIE) by using an efficient standard for ICT support to all functions. Through the continued development of an efficient and architectured DIE, Defence is better able to meet the demands of the strategic, operational, and tactical user.

Interoperability Trends

1.14 The ability to operate with other agencies, both domestically and internationall, is a key enabler of NZDF capability. Whether the NZDF is acting cooperatively with another New Zealand Government agency or operating as part of a multinational force, its ability to exchange information quickly and securely is essential. The NZDF continues to develop a coordinated and robust CIS architecture to support these interactions.

1.15 The NZDF is evolving an effective governance framework to enable interoperability that accommodates both government and NZDF interoperability priorities in support of Defence's requirements to interact domestically and internationally.

1.16 Improved information management and sharing enhances joint, multi-agency, and multinational interoperability. This reduces the disadvantages caused by regional factors and helps mitigate the risks associated with asymmetric threats.

1.17 The ability to lead and act decisively in New Zealand's primary area of strategic interest involves the continued development of a robust ICT capability by investing in critical infrastructure, such as satellite communication, along with sufficient spectrum and network bandwidth to meet demand.

1.18 ICT requirements need to be taken into account when introducing new capabilities (including sensor and weapon systems) and control systems into the environment. In addition, ICT solutions need to comply with Defence and all-of-Government (AoG) security standards. This ensures a consistent approach to information security and CIS, while supporting the business and enhancing Defence's information sharing capability.

1.19 The NZDF's joint forces conduct campaigns and operations by connecting to, and focussing on, globally dispersed systems and organisations. To do this, they draw upon shared capabilities, which have increased in number, influence, capacity, and degree of interaction, due to the rapid evolution of ICT.

The Defence Information Environment

1.20 The DIE interacts with the global information environment. It is a capability consisting of data and information used by the NZDF for business activities and military operations. The DIE also consists of the means by which data and information is created, managed, manipulated, stored, and disseminated in and across all security domains. It includes all the NZDF's capabilities involved in the exchange of data, such as fixed, mobile, standalone, and deployable networks, along with user devices and their support services, including NZDF services hosted on external servers.

Key Term

Information Environment

The aggregate of the individuals, organisations, and systems that collect, process, disseminate or act on information.

1.21 The DIE also encompasses the computing and communications infrastructure of the NZDF, along with the people and management systems that deliver that infrastructure. It includes the computing networks, business applications, and the data that they generate, as well as the standards and electromagnetic spectrum (EMS) required for deployable networks.

1.22 The DIE infrastructure is integral to the continuity of core NZDF functions. The DIE supports information domains such as command and control, intelligence, surveillance, reconnaissance, target acquisition, information activity, the planning and conduct of campaigns and operations, logistics, strategic policy, capability development and management, and resource management services involving personnel, finance, and asset acquisition, and onto through-life support or sustainment. As a capability, the acquisition, operation, and support of the systems that provide this information, require continuous, effective management, upgrading, and coordination.

1.23 Each information domain requires interoperability considerations at all interfaces to the DIE boundaries, information management, sensors, and other external entities. Some examples are allied, coalition, industry, and other government agencies (OGA) networks. This requires negotiated agreements of responsibilities, common standards, and DIE reviews (operational, system, and technical), which include information nodes and the data flows between them and to the external interfaces. The CCIS coordinates the development of the DIE through the Chief Technology Officer (CTO) in conjunction with the Services' Technical Regulatory Authorities.

Responsibilities

1.24 The Communications and Information Systems (CIS) Branch, Headquarters New Zealand Defence Force (HQNZDF) is responsible for the provision, sustainment, and governance of the NZDF's ICT. This includes the responsibility for the ongoing running and development of the DIE, controlling sustainment costs, and enabling the NZDF to take advantage of emerging technologies. However, many ICT- enabled capabilities that reside in the DIE rely on the raise, train, and sustain functions owned by the Services.

1.25 Under the current NZDF Operating Model, the Chief of Joint Defence Services (CJDS) has been delegated the overall responsibility for the delivery of NZDF's enabling functions, including CIS. The CCIS reports to the CJDS.

Principles

1.26 The following guiding principles below provide the intellectual framework within which the DIE is developed, operated, and managed.

- **National Alignment.** The NZDF aligns with the national approach to information management. The AoG approach to harnessing information is a key component of national power. Government agencies will understand evolving circumstances so that military actions are in concert with the national approach. Civil infrastructure is a vital national asset, providing additional capacity and flexibility. It features in all CIS planning. Technical solutions to enable coordination between elements of a comprehensive AoG approach are essential. To complement CIS activities within Defence, coordination is required across civil agencies, including telecommunications authorities and EMS management.

- **Multiple Security Domains**. The NZDF operates multiple security domains within the DIE (for example the Top Secret, Secret and Restricted domains). The CCIS, in consultation with the Chief of Defence Force (CDF), CJDS, Commander Joint Forces New Zealand (COMJFNZ), and Assistant Chief Capability (AC CAP), establishes the strategic direction, governance, and coordination arrangements for the development, operation, and management of the DIE. [1]

- **Information is Managed.** Timely and useful information is an important resource to the people in our maritime, land, air, and Special Forces. Managed information delivers the right information to the right people at the right time and in the right form. Useful, current information enables decision-makers to quickly increase awareness of the situation in order to maximise the chances of mission success. It permits greater organisational agility, increased operational tempo, and improved business precision in a secured information environment.

- **The Military is Supported**. Military operations are the NZDF's unique contribution to national security. The DIE is required to meet current operational requirements and continually develop to provide appropriate support to future military operations.

- **The Military is Supporting**. The NZDF provides specialised AoG ICT contributions. These include:
  - providing High Frequency (HF) communications coverage
  - hosting the National Maritime Coordination Centre (NMCC)
  - providing network services to New Zealand Government Agency staff deployed in NZDF platforms.

[1] A security domain is a system or collection of systems operating under a security policy that defines the classification and releasability of the information processed within the domain. It can be exhibited as a classification, a community of interest or reliability within a certain classification

Communication and Information Systems

1.27 CIS are assemblies of equipment, methods/procedures, and personnel organised so as to accomplish specific information conveyance and processing functions. In the operational environment of today, effective C2 and information management cannot be achieved without properly deployed and managed CIS. They are an essential part of military operations that provide commanders at all levels with the means to exercise C2 and disseminate vital information.

Development of Systems

1.28 The major purpose of CIS in a military context has always been the passage of information to inform and support C2. From the earliest times, when communications between a commander and their forces was by means of a messenger, through to the development of visual signalling, to the early forms of electronic signalling, to the current environment of computing systems connected by various communications means, the intent has been the same.

1.29 The NZDF's information flows have been stove-piped in the past, and remain so to some extent. That is, information flows up and down through lines of control with little cross-organisational or lateral flow. Stove-piping is a characteristic of organisations that have a strong hierarchical structure, such as the NZDF. In a network-enabled organisation, information is global and flows laterally as well as vertically and is available to all who need it. In a modern, network-enabled organisation information is available in real or near-real time but often the value, and even the security classification, of information is diminished by the time taken to promulgate it.

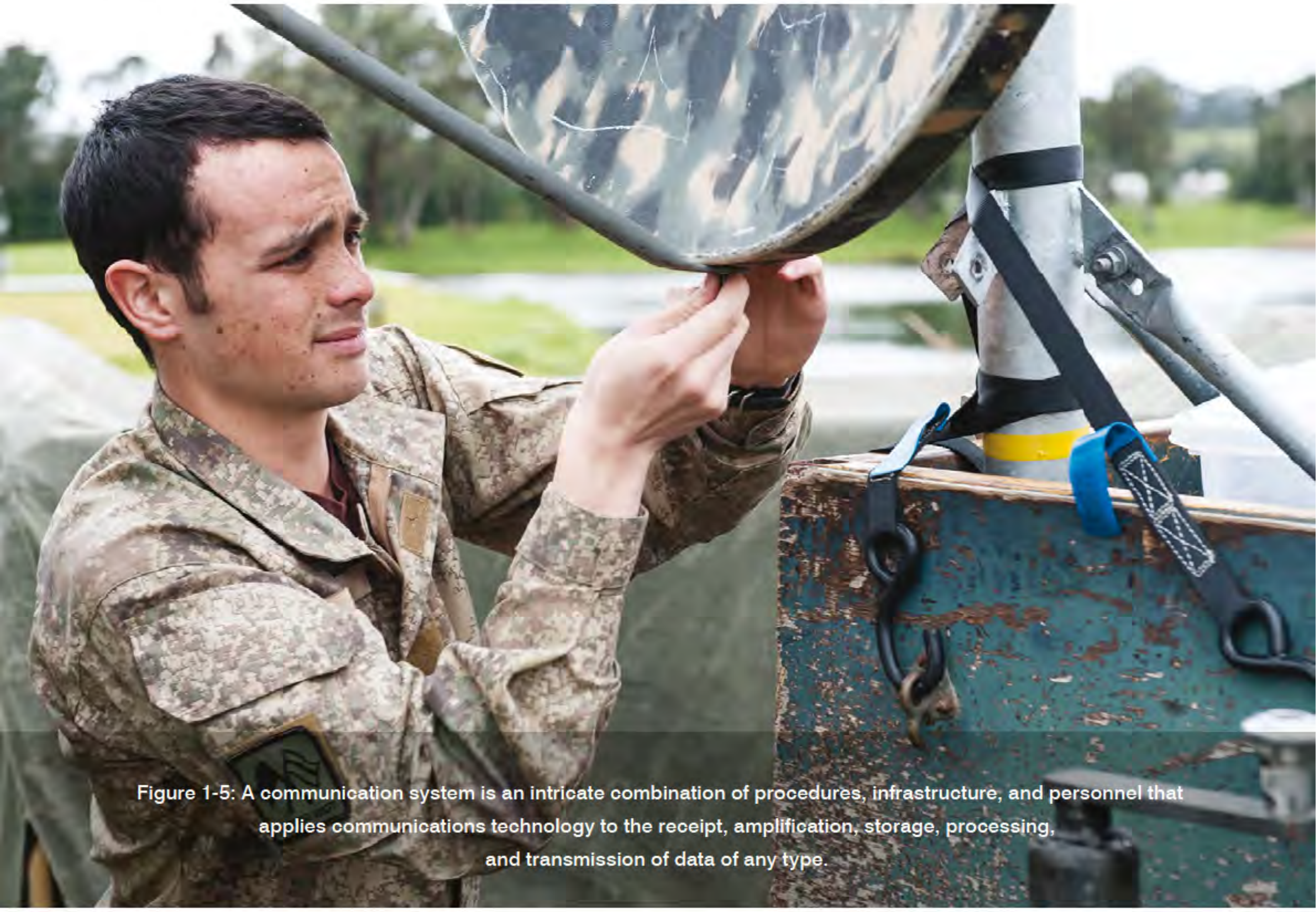


Figure 1-5: A communication system is an intricate combination of procedures, infrastructure, and personnel that applies communications technology to the receipt, amplification, storage, processing, and transmission of data of any type.

Communication Systems

1.30 A communication system is defined as "an assembly of equipment, methods, and procedures and, personnel organised to accomplish information transfer functions." A communication system is an intricate combination of procedures, infrastructure (for example, facilities, satellites, transmitters, receivers, antennas, power supplies, switches, cables, and data), and personnel (specialist operators and terminal users) applying communications technology to the receipt, amplification, storage, processing, and transmission of data of any type (analogue, digital, audio, video, image, and so on). A communication system provides communications between its sending and receiving users and embraces transmission systems, switching systems, and user terminal systems.

Key Term

Communications System

An assembly of equipment, methods, procedures, and personnel, organised to accomplish information transfer functions.

A communication system provides communication between its users and embraces transmission systems, switching systems and user systems.

1.31 Communications, as distinct from verbal communication within the normal range of human senses, requires a data transmitter and receiver, connecting network of links, common services, and data. This may not involve any human intervention or analysis, which differentiates a communication system from an information system. The NZDF's communication systems could include any of the following:

Figure 1-6: A communication system provides communications between its sending and receiving users and embraces transmission systems, switching systems, and user terminal systems.

- radiofrequency (RF) bearers providing radio-based tactical and strategic communications to and from deployed or mobile users enabling both voice and data communications providing data at multiple security classifications over multiple networks (national/allied/coalition) to and from NZDF units
- wide area and local copper or fibre optic cable systems providing a similar range of voice and data communications between fixed locations
- manual systems such as signals dispatch services and visual signalling using signal lamps, lasers, or flags.

Information Systems

1.32 An information system, just like a communications system, consists of personnel, procedures, software, and resources organised for the collection, processing, maintenance, transmission, and dissemination of information, whether automated or manual. It includes human and user terminal devices, as data can only be converted into information when it has been put into context. An information system can have one or more different purposes, some of which are outlined below.

- C2 arrangements require rapid, secure, and comprehensive distribution of the commander's intent and the prevention of network overload so that information can be delivered accurately, for example our own national rear link requirements for multinational activities.
- s. 6(a)
- Collaborative planning systems allow commanders and their staff to aggregate, manipulate, and present information in a clear, concise format to enable timely and informed decisions. Disadvantages of geographical separation of the chain of command must be overcome allowing the efficient use of relevant system planning, operation, mission rehearsal, simulation, modelling, and experimentation tools.
- Logistic support or materiel information management systems or applications allow for maintenance, repair and configuration control of equipment, ordering of supplies, tracking of supplies and equipment, movement management, training readiness, and other logistics processes.
- Administration systems or standard applications enable management of Defence business processes, administrative needs, and personnel.
- Interoperability and multinational information sharing systems facilitate automatic exchange of information between the military forces of New Zealand and those of other nations at all levels of command.
- Interagency information sharing systems provide entry into organisations with which Defence needs to interface to manage its business processes, campaigns, operations, exercises and other activities.

Information Management

1 33 Information is a strategic asset for defence. Therefore, the effective and efficient management of that information is the ability that will bring that asset properly to bear on the NZDF's business and in doing so, help to improve decision making. Information management within the NZDF is based on providing the right information, at the right time, to the right person, and in the right format to enable the right decision to be made. This depends on:

- a single source of truth (the right information)
- information governance (the right time)
- a culture of information sharing between those who need to know (the right person)
- according to agreed standards (the right format).

1 34 The NZDF's military capability depends on commanders' ability to seamlessly access intelligence, logistical, and personnel information in order to make strategic, operational, and tactical decisions. Effective information management provides a competitive advantage in determining accurate situational understanding, rapid decision-making, and precise application of force over adversaries. Effective information management also ensures costs associated

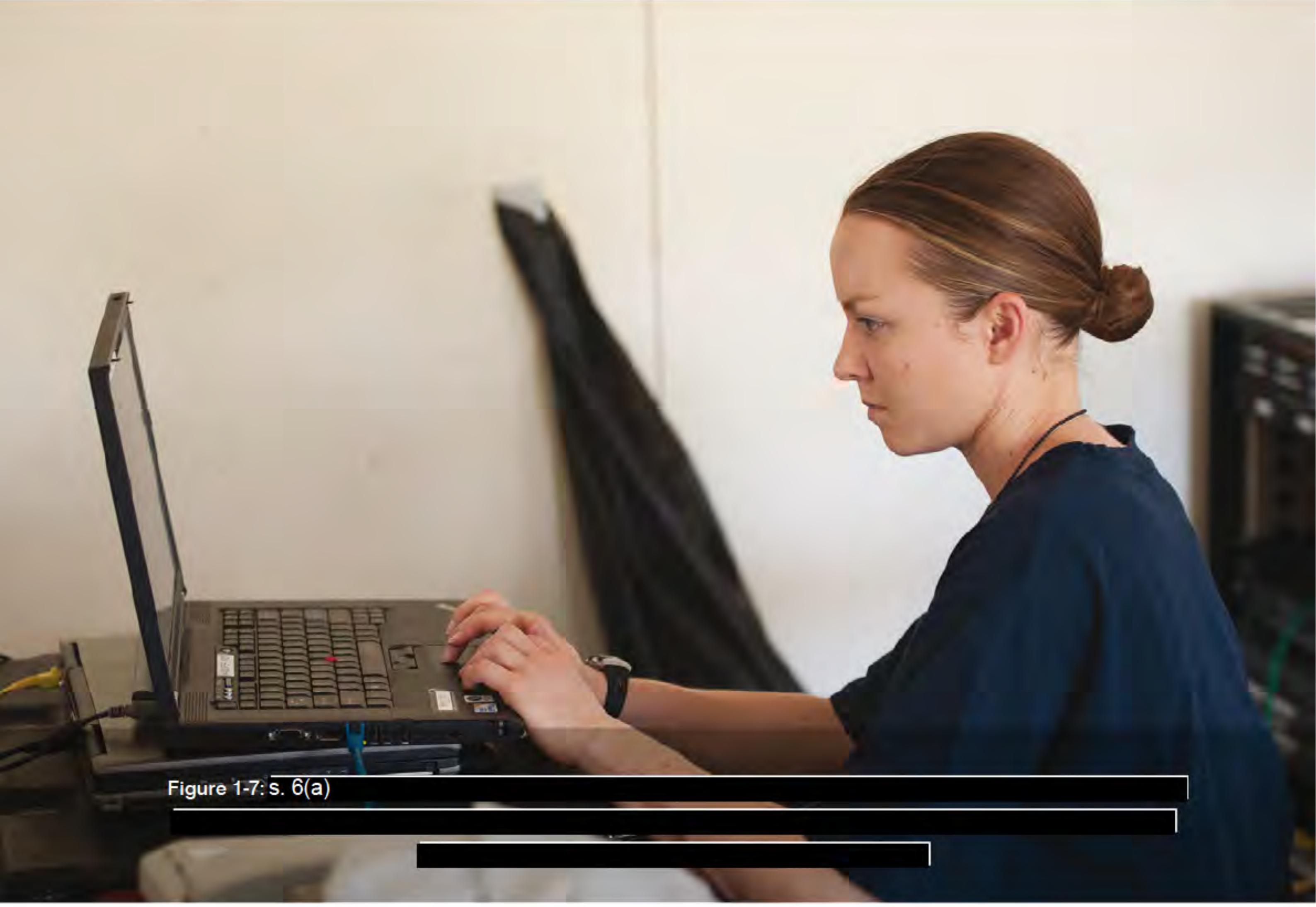


Figure 1-7: s. 6(a) [redacted]

with military capability are reduced by eliminating 'stovepiping' of information and that the principle of 'need-to-share' (within security constraints) is pervasive.

1.35 Information management is the processes required to achieve desired outcomes through effective and efficient stewardship of information. Integrated management of processes and services provides exploitable and timely information in the right place and format to maximise freedom of action.

1.36 The management of information encompasses:

- automated and manual processes
- systems and facilities involved in defining and developing the architecture (architecting) of business processes and systems that relate to the creation, manipulation, presentation, archiving, and destruction or deletion of information in any form, whether electronic or physical.

1.37 Information management is a joint enabling activity that is part of the foundation of effective information exploitation. It assists commanders and staffs to achieve common situational understanding of the problem or crisis with which they are dealing. Exploitation leads to situational understanding that, when combined with experience and culture, results in intuitive or reasoned risk assessment and decision-making.

Data Management

1.38 Information management should not be confused with data management. Data management relates to organisational and technical tasks concerning the planning, storage, and provision of data, both for computer personnel and end-users. Data is any

Figure 1-8: Information management within the New Zealand Defence Force is based on providing the right information, at the right time, to the right person, and in the right format, to enable the right decision to be made.

representation of facts, concepts, or instructions in a formalised manner suitable for communication, interpretation, and processing by humans or automatic means. Representations may be symbols, characters, or analogue quantities to which meaning can be assigned.

1.39 Data needs to be contextualised before it can be information. This generally requires data being placed into a predefined field along with metadata describing the data or field. Data is a general term used to denote facts, numbers, letters, and symbols refering to or describing an object, idea, condition, situation or other factor. It involves basic elements of information that can be processed or produced by a computer.

Principles of Communications and Information Systems Support

1.40 In order to provide robust and flexible CIS support to the NZDF, its network planners at all levels need to take the following principles of CIS support into consideration. As principles often conflict, balance is always the aim:

- **Support the Chain of Command**. To support the transfer of data amongst commanders, staff, and other users, CIS plans need to complement the commander's intent and concept of manoeuvre and also ensure that services are available where and when required to maintain continuity of command. CIS architecture should be designed to provide relevant functionality, quality performance, pervasivness, and use available resources to optimal effect. This requires adaptability to changing command structures through a technical control chain that ensures appropriate conformance with standard procedures and doctrine. To ensure the efficient allocation of limited resources planners need to understand that CIS is provided and technically controlled between headquarters and units from higer to lower, left to right, supporting to supported.

- **Integration.** The CIS technical control hierarchy must be integrated within the chain of command to ensure command priorities are met. Integrated networks reduce the need for data exchange points and system interfaces, all of which are potential points of failure. CIS standardisation and use of common equipment and processes maximise interoperability, effectiveness, and efficiency through seamless exchange of data, preferably from a single, trusted source, both internally and externally.

- **Reliability.** CIS must be reliable to maintain continuity of command. A reliable system, with a minimum of nodes and facilities, is usually preferable to complex systems providing superior facilities that are less reliable and more difficult to recover in confused environments. This is particularly important for tactical, deployed systems. Availability, survivability, and training all contribute to resilience and reliability.

- **Flexibility.** CIS architectures need to be adaptable to evolve with changing technology and responsive to changing demands through surge and rapid reconfiguration, as well as to challenges posed by uncertain environments. The same CIS equipment should be usable for as many military tasks and in as many climatic environments as possible.

- **Survivability.** Robust CIS networks ensure continuity of C2 and minimise the impact of adverse events and the time needed to recover from them. CIS equipment needs to be appropriately ruggedised to meet environmental demands. The data and information they pass need to be protected and preserved throughout their required life.

- **Mobility.** The mobility of CIS at all levels of command must be commensurate with that of the supported force, especially with its commander. They need to be designed for continuous portable use or rapidly closed down and re-established. Maximum support must be sustained when command is handed over after movement, relocation, or steping-up of headquarters and units.

- **Security.** Data and the CIS infrastructure both need to be assured and protected to ensure confidentiality, availability, and integrity. This information assuranace maximises protection of our highly valued people, equipment, and information. Unless adequate consideration is given to the security of information held on and transmitted by CIS equipment, operations can be compromised.

- **Simplicity.** Simple CIS plans are more likely to withstand the stresses of campiagns and all type of operations. A simple plan will be more readily understood and more easily implemented. CIS equipment should be easy (intuitive) to operate and simple to repair by modular replacement, so as to minimise training requirements.

- **Capacity.** To ensure that information is current when it reaches its destination, CIS must be able to cope with traffic peaks and troughs, and permit all data to be eventually transmitted, within a priority-based release methodology.

- **Quality.** The quality of CIS networks must be such that the integrity of the information is not questioned, meaning is not lost in transmission and data or systems remain appropriately responsive to the requirements of commanders and other decision makers. Accuracy at the point of data entry and identification of the primary source of that data are particularly important.

- **Economy.** CIS assets, including memory/storage space, spectrum and bandwidth, are finite resources and demands on networks should be kept to the essential minimum. Sole-user facilities will be restricted, usually to commanders and key staff positions. Information management is a key to ensuring the economic use of CIS resources.

- **Interoperability.** Information networks should support the uninterrupted flow of data between, joint task force headquarters, their force elements, any supporting government agencies, and the forces from multinational partners. It is important to remember that these systems may not be interoperable. Therefore, the CIS staff needs to plan for interoperability using procedures and liaison detachments to facilitate information transfer in an appropriate form.

- **Anticipation of requirements.** Some CIS require long lead times to ensure commercial support is provided or logistics pre-positioning can occur. This requires planning staff to anticipate requirements. Maintenance staff should also establish mechanisms to anticipate failures to prevent uncontrolled/ unplanned outages.

Overview of Communications and Information Systems in Defence

1.41 CIS is central to the conduct of all functions of the NZDF, whether operational or non-operational, and from the strategic to the tactical. For this reason and because of the requirement for consistency in the provision and acquisition of CIS across the NZDF, the CCIS is responsible for the planning, development, and operation of the DIE. Specifically this involves:

- developing NZDF ICT concepts, plans, doctrine, and policy
- providing leadership in the use of best practice in design, delivery, and operation of ICT systems
- advising all NZDF committees on ICT issues
- developing an architecture for the DIE for all NZDF ICT systems and setting ICT standards and product lists
- ensure requirements from business process owners are met through commercial and standardised solutions, and refer any requests for bespoke and customised solutions for NZDF and Government approvals
- consolidate the operation of the NZDF ICT systems based on standard commercial models
- establish priorities and engagement strategies for ICT interoperability with other New Zealand Government agencies, allies, and coalition partners
- establishing the governance mechanisms necessary for executing these responsibilities and accountabilities
- developing an agile solutions design capability that will work with business and ICT stakeholders to deliver pragmatic and practicable outcomes for the NZDF.

1.42 **Command and Control.** CDF commands the NZDF through the Service Chiefs. Command of the Services is exercised by the repective Chiefs of Service, except for operations. Headquarters Joint Forces New Zealand (HQJFNZ) is the operational level headquarters that plans, controls, and conducts campaigns, operations, joint exercises, and other activities on behalf of CDF. Although the Service Chiefs are the principal advisers to CDF for single-Service aspects of operations, COMJFNZ commands operations and the forces assigned to them on behalf of CDF.

1.43 A COL (E) military officer is the principal strategic adviser (Strategic J6) within CIS Branch to CDF and COMJFNZ on CIS and EMS matters. The Strategic J6 is the coordinating authority for the NZDF CIS support capability.

Historical Example

The Genesis of the Modern Networked Force

Throughout the history of military communications, the need for reliability, speed, accuracy, and security has been constant. Despite significant technological advances of recent times, reaching optimal levels of these attributes remains a challenge. Progress resulting in new weapons or communication systems has inevitably been followed by changes in military operational concepts and doctrine, a pattern that has continued in an increasingly complicated international political and cultural scene.

Communication systems until 1900 slowly progressed from local area, sound, and visual systems (drums, smoke, and flags) to extensive telegraph systems using fixed wire circuits. The British first used Morse's electric telegraph during the 1854 Crimean War; more extensive use occurred in the American Civil War. Its spread increasingly rapidly during the late 19th Century: the Prussian and French armies used mobile telegraph trains, and European and British powers formed specialised Engineer or Signals corps responsible for communications.

Less than a half-century later came a second revolution in military communications: development of wireless telegraphy and radio in the late 19th Century extended communications beyond line-of-sight and the reach of wired networks. The first real large-scale military testing of both wired and wireless communications came during World War I. Wartime needs and growing equipment procurement greatly accelerated the pace of radio's technical development. In 1914, when obsolete spark-gap wireless telegraphy was still widespread, vacuum tube based equipment was rare. The addition of voice capability to Morse meant that by 1918 its use was becoming standard.

During the interwar period, innovation continued in both commercial and military laboratories, which further aided military communications. Developments included radar, microwave transmission, improvements in long range short wave radiocommunications, and the development of Frequency Modulation (FM) radio. Electric cipher machines and teleprinter equipment, which were to play a significant part in the forthcoming conflict, were also developed. Further significant developments, not just in technical capabilities but also in the employment of military communications, occurred during World War II.

The ability to use communication systems to pass information in a timely manner and to protect that information played a significant part in military success. By the end of the war, virtually every Allied military vehicle and aircraft carried a transceiver. Walkie-talkies allowed the infantry to stay in constant communication with their headquarters, one of the first demonstrations of small-scale, mobile communications in wartime.

The period since World War II has seen military communications develop at an even increasing pace, concurrent with advances in civilian communications and technology generally. Communications have become real-time, automatic, digitised, netlike, multilevel, multiservice, and dependent on commercial information and communications technology innovations. The developments in packet switching and satellite communications have allowed for development of networks able to share information more quickly and easily to provide improved awareness of the operational environment.

CHAPTER 2:

INFORMATION EXCHANGE AND ASSURANCE

CONTENTS

Introduction

2.01 New Zealand Defence Force (NZDF) Communications and Information Systems (CIS) includes systems used for command and control (C2) as well as those for acquisition, storage, display, analysis, protection, processing, and transfer of information within the NZDF. It also includes those systems that provide interoperability with other New Zealand government departments, non-government agencies, allied militaries, coalition partners, and regional organisations. Information exchange involves the systems, applications, and procedures related to both fixed and mobile CIS elements with specific focus on command support and information operations. It also involves the systems available for the exchange of information between allied, coalition, and regional partners. Activities undertaken to defend and protect information and CIS are known as information assurance, which is a key component of information superiority. Information assurance integrates people, operational techniques, and technology to protect, detect, and react to intrusions or attacks and restore information services as quickly as possible.

2.02 The purpose of this chapter is to introduce in general terms how information is exchanged and assured in the NZDF. Procedural aspects of information exchange can be found in the Australian Defence Force Publication (ADFP) 6.0.2— *Communication and Information Systems Support to Operations*. The key Information Security policies for the NZDF are the *Protective Security Requirements* (PSR) issued by the New Zealand Security Intelligence Service (NZSIS) and the *New Zealand Information Security Manual* (NZISM) issued by Government Communications Security Bureau (GCSB). Information contained in these manuals is elaborated in various Defence Force Orders (DFO).

Information Exchange

2.03 Information exchange is the formal or informal transmission of information from, to, or within an information environment. Information exchange can be conducted using electronic or physical means in fixed or deployed environments spanning all security domains[2]. Such information can be text, graphics, or other forms. Informal communication is used for information when non-repudiation and authentication are not imperative.

2.04 Development of new technologies, including social networks, has changed the nature of both the Internet and military communications. Faster, more interactive, and less formal means of communications are now commonplace and are becoming accepted in the NZDF environment. The NZDF is committed to continually adapting to new ways of working. This means that the NZDF often needs to add features to common applications, such as chat, to make them fit for C2 purposes. This usually means increasing the application's security functionality, for example introducing non-repudiation and automatic archiving of messages.

2.05 Formal messaging is used in the NZDF when the originator considers the text of the message must be conveyed with guaranteed security and reliability, and when the addressee is expected to take action without repudiation and with minimum delay. Transmission of Standard Military Text Format messages is an example of a formal messaging.

Key Terms

Infomation Exchange:

the formal or informal transmission of information from, to, or within an information environment.

Security Domain:

A system or collection of systems operating under a security policy that defines the classiification and releasability of the information processed within the domain. It can be exhibited as a classification, a community of interest, or reliability within a certain classification

[2] A security domain is defined in the NZISM as 'a system or collection of systems operating under a security policy that defines the classification and releasability of the information processed within the domain. It can be exhibited as a classification, a community of interest or reliability within a certain classification. This term is not synonymous with *Trust Zone*.'

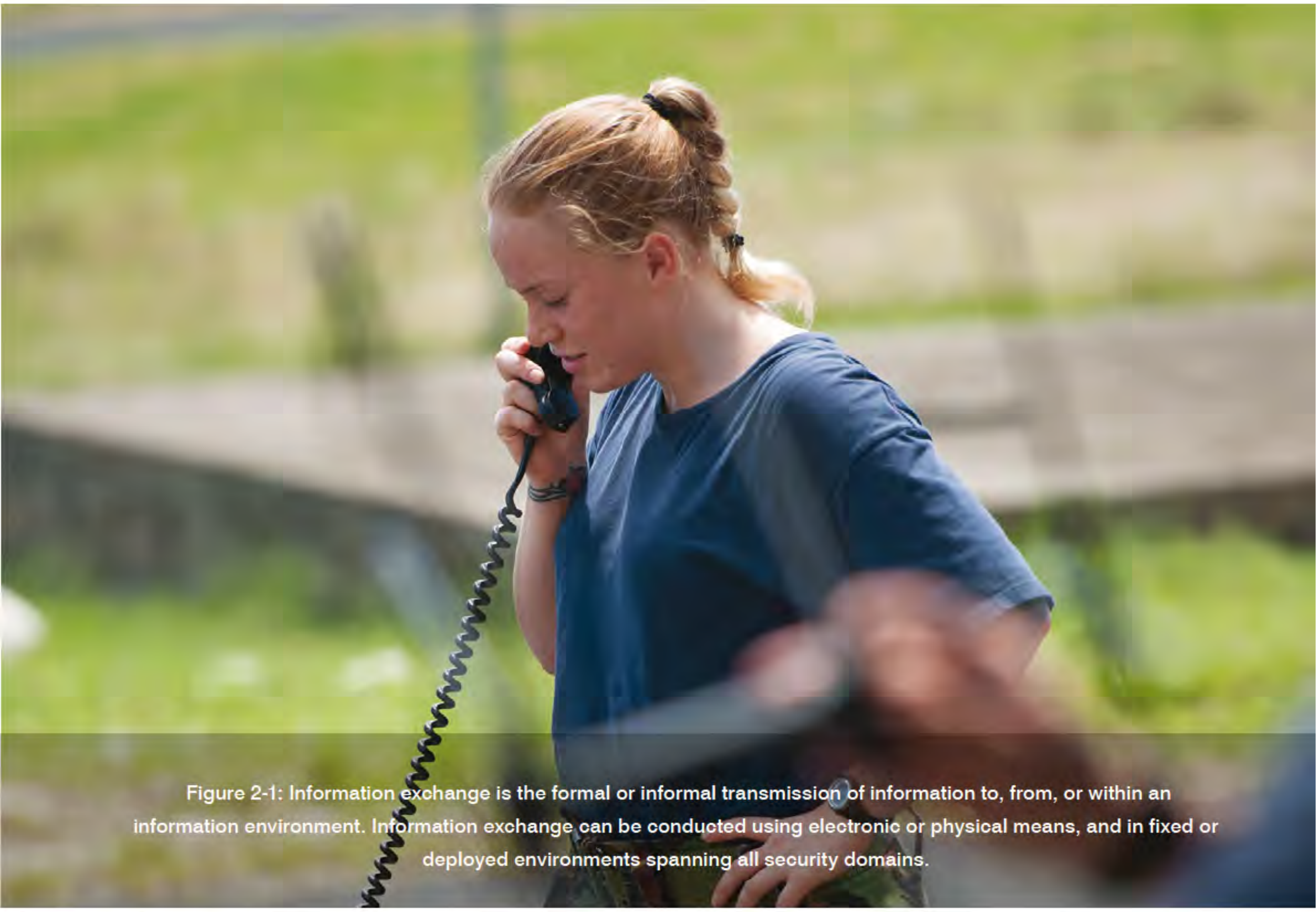


Figure 2-1: Information exchange is the formal or informal transmission of information to, from, or within an information environment. Information exchange can be conducted using electronic or physical means, and in fixed or deployed environments spanning all security domains.

Services and Systems

2.06 Information availablity is integral for commanders to make decisions that maximise the ability to achieve mission success on NZDF campaigns and operations. Timely and safe passage of information requires secure connectivity between the commanders and their assets; operational level headquarters and joint task force headquarters, whether deployed or garrisoned; and allied, coalition, and regional nations, and other government departments and non-government organisations. CIS services available to the NZDF at the strategic (including in garrisons), operational, and tactical levels include:

- networks that support data and information exchange
- voice communications
- secure and non-secure facsimile (fax)
- formal military messaging
- video conferencing
- electronic information exchange (EIE) supporting emails with attachments, web services, data storage and recovery, collaborative planning, stand alone and enterprise applications, situational awareness, and common operating picture tools and management applications
- hand messaging services in conjunction with signals dispatch services interfacing with logistics and corporate safehand courier systems.

Communication Networks

2.07 Communications networks consist of one or more communications links and are classified as either tactical or strategic networks (however, some systems, depending on the information exchanged, can be both). These communications networks are defined as follows:

- **Strategic Communications Networks**. Strategic communications networks connect fixed sites, camps, and bases. They are established for use by the NZDF's staff and organisations. They include satellite services, terrestrial bearer links, and High Frequency (HF) bearers that can be connected to deployed units and headquarters at home or overseas.
- **Tactical Communications Networks**. Tactical communications networks are communications systems deployed to provide CIS for C2 of land, air, and sea forces. They are used either to communicate with other forces in the deployed environment or reach back into the NZDF's strategic communications networks.

2.08 **Tactical Communications Networks**. A tactical communications network can be interfaced into a strategic communications network and its supported systems. Although it should be considered as a single logical network, for practical deployment reasons, a tactical communications network is categorised by its major architectural component (referred to as subsystem). It consists of the following networks.

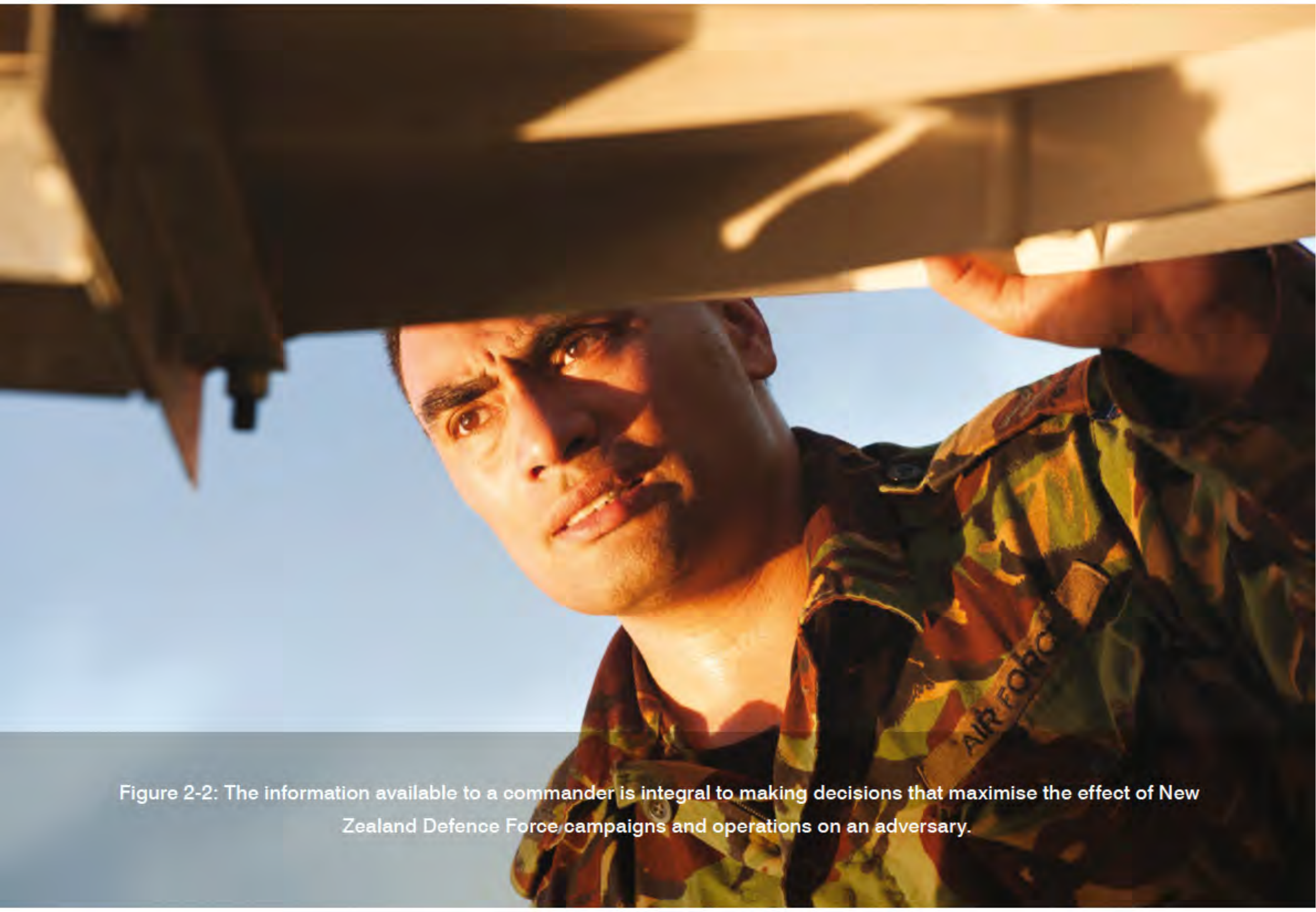


Figure 2-2: The information available to a commander is integral to making decisions that maximise the effect of New Zealand Defence Force campaigns and operations on an adversary.

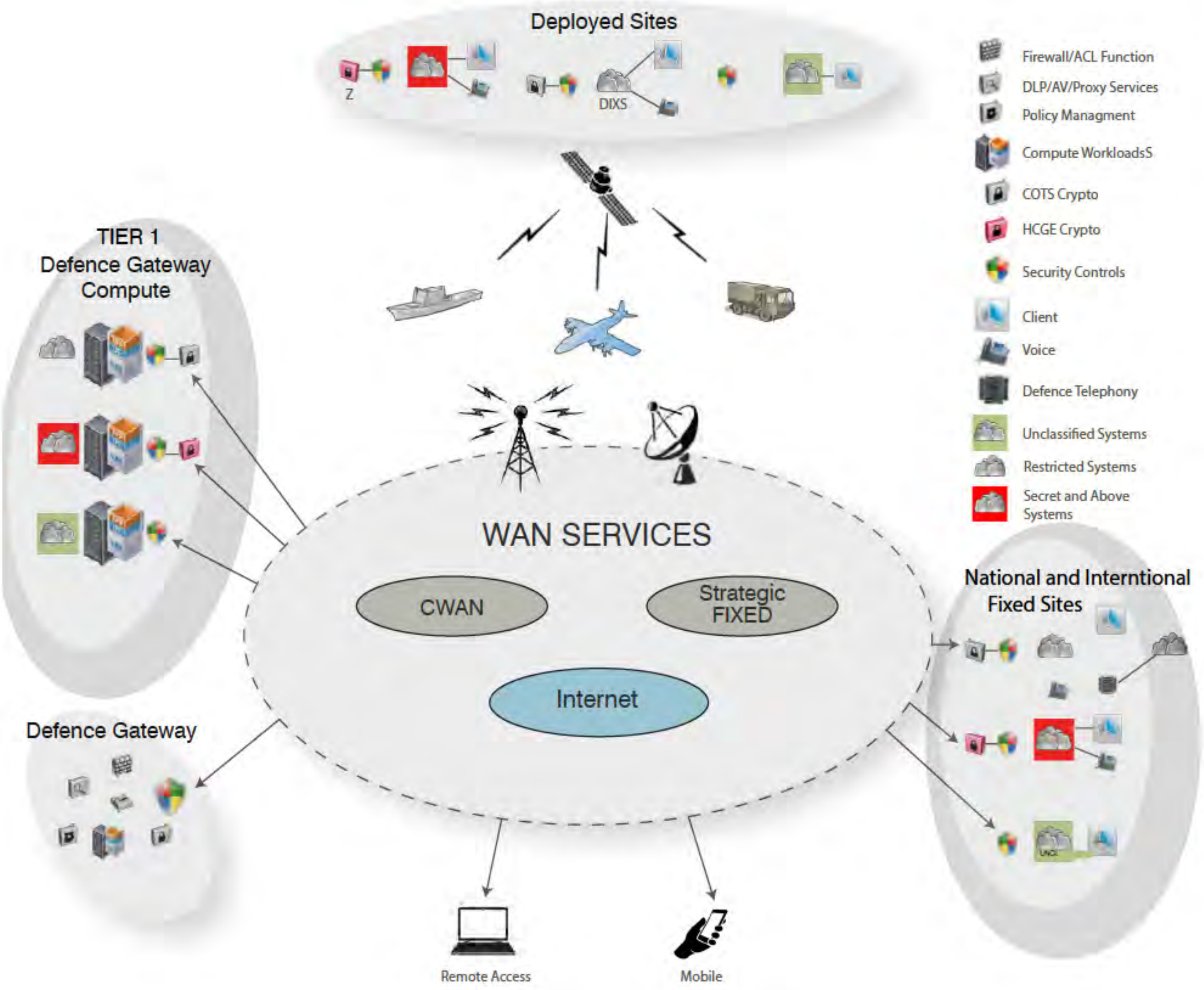


Figure 2-3: Defence Information Environment

- **Local Radio Networks**. Local radio networks include radios providing voice and data communications to support force elements' C2.
- **Trunk Networks.** Trunk networks are the high capacity infrastructure used to support voice and data communications between communications nodes (for example a radio relay or satellite terminal).

2.09 Local radio or trunk networks may not have sufficient range to extend high capacity communications over the distances required to support dispersed operations. Extending the range of these systems may be achieved by employing combat net radio (CNR) retransmission and radio relay sites, satellite trunk systems, and airborne retransmission systems.

2.10 **Strategic Communications Network.** The strategic network provides the following services:

- the Defence Wide Area Network (DEFWAN) is a network capable of passing operational voice, video, and data traffic. It comprises telecommunications carrier-grade routers and switches provide the NZDF and Ministry of Defence (MOD) with a core network capable of high assurance and reliability under normal operating conditions. Routers and switches are either owned and operated by the NZDF or provided as a managed service via designated contracts with telecommunications carriers. Delivery, maintenance, and support of the DEFWAN is managed by CIS Branch, Headquarters New Zealand Defence Force (HQNZDF). The following networks are normally operated as virtual private networks of the DIE:

- the Top Secret Information Environment (TSIE)
- the Secret Information Environment (SIE)
- the Defence Information Exchange System (DIXS)
- the Defence Telephone Network (DTelN)
- Defence Secure Videoconferencing Environments
- unclassified solutions include but are not limited to:
  - simulation
  - internet to the desktop (ITD)
  - bespoke services across the organisation
  - bespoke networks for discrete low-threat missions
- Gateway services include but are not limited to:
  - interface to satellites
  - High frequency (HF) communications, including the tactical interface
  - PEGASUS international services
  - access to other Government agencies
- Defence's satellite and high frequency network services, including tactical interface sites
- support to international information services
- NZDF's Internet gateways.

Communications Services

2.11 Tactical and strategic communications networks do not exist in isolation. They exist to provide services and support to joint and multinational systems, such as command elements, sensors, weapon platforms, command support systems, information services such as video-conferencing and information management, and network management systems. As information and communications technology (ICT) becomes more accessible and secure, commanders' expectations increase, and CIS managers are required to configure communications networks to deliver a broader range of CIS services.

2.12 The CIS services that a commander could expect include the following:

- voice services (telecommunications and internet protocol (IP))
- connection of two or more electronic systems in order to share information:
  - data file transfer and email
  - command support systems
  - administrative and logistics support systems
  - surveillance and sensor systems.
  - data links
- formal messaging
- videoconferencing services.

2.13 The following systems provide commanders with information support in the enterprise and operations domains of the information environment.

- **Enterprise Resource Programme Systems.** Enterprise Resource Programme (ERP) systems are enterprise-wide. They include financial, logistics, personnel management, and health management systems. The policy, standards, architecture, and operation of ERP are managed by the Chief Communications and Information Services (CCIS) on behalf of the NZDF.
- **Command Support Systems.** Command Support Systems (CSS) includes the Defence Command and Control System (DC2S), plus others. Strategic J6's role is to advise the Chief of Defence Force (CDF) on C2 and electromagnetic spectrum issues for the NZDF. The Strategic J6 also provides CIS planning advice to the staff Branches in HQNZDF, single Service headquarters, Headquarters Joint Forces New Zealand (HQJFNZ), and units and formations of the NZDF. However, it is the CCIS who is responsible to the CDF for infrastructure and operation of the DIE. Capability Owners (as defined in Capability Management Plans) are responsible for the Through-Life Support (TLS) as an integral part of wider Through-Life Capability Management. Within that overarching responsibility, other TLS groups across the NZDF organisation have

significant roles in providing and managing discrete TLS areas (for example, Defence Logistic Command – maintenance and supply support; Defence Human Resources – personnel; New Zealand Defence College and Service training establishments – training; Computing Information Systems Branch – computer support). The Assistant Chief Capability (AC CAP) is responsible for the design and delivery of TLS solutions integral to all projects in conjunction with the MOD (Acquisition). AC CAP also oversees related capability development where interoperability of CSS is a key consideration.

- **Network Requirements Determination and Interface Systems.** Although operational and tactical level military and commercial satellite communications are managed by CIS Branch, operational requirements and priorities are determined by HQJFNZ. This includes prioritisation of relevant tactical to strategic interface station anchor requirements.
- **Tactical Level Systems.** CIS staffs at each headquarters are responsible for liaising with CIS Branch and HQJFNZ on Service- or unit-specific connectivity requirements.

Safehand Services

2.14 The NZDF has in place corporate safehand services to support its daily activities. As part of NZDF's normal planning processes the provision of tactical and operational hand carriages services are a planning consideration.

Standards and Interoperability

2.15 Interoperability is the degree to which organisations, groups, or individuals are able to operate together to achieve common goals. Communications interoperability is achieved when data or services can be directly exchanged between systems and their users. The ease and level of interoperability between the NZDF, other militaries, and other government agencies (OGA) directly contributes a Joint Task Force (JTF) meeting its mission objectives. Interoperability cannot be considered solely at an equipment or systems level; it must also include common standards in doctrine, people, procedures, and training.

2.16 Achieving interoperability of ICT and CIS is one of the most significant challenges to conducting joint operations. Determining how various systems are coordinated to accomplish joint missions must be addressed by the NZDF's Communications Planners and its Architecture Developers. When provisioning CIS infrastructure and systems needed for competent levels of joint mission C2 and ICT as well as intelligence, surveillenace and recoconnainse (ISR), interoperability must be considered by the single Services when upgrading or introducing Service specific CIS capabilities. Understanding the specific nature and the level of interoperability required is a key consideration for information architecture.

2.17 Required levels of CIS interoperability will vary through differing joint, combined, and coalition operational levels. Determination and compliance of appropriate communication standards and data formats is essential for effective interoperability. Common technology standards, processes, and procedures provide the NZDF references for practical cooperation. They also enable the NZDF to make the most efficient use of its research, development, and production resources. Interoperability must involve inter-organisational or national agreements to broadly adopt the use of common and compatible:

- doctrine and operational, administrative, and logistic procedures
- technical procedures and criteria
- and interchangeable supplies, components, or equipment.

2.18 The NZDF is a member of several different organisations that specifically focus on facilitating interoperability between it and the armed forces of Australia, Canada, the United Kingdom,and the United States:

- CCEB – Combined Communications and Electronics Board
- AUSCANZUKUS – Maritime Information Warfare Organisation
- ABCANZ – American, British, Canadian, Australian, New Zealand Armies Program
- ASIC – Air and Space Interoperability Council
- M2I2 – Maritime Multi-National Information Systems Interoperability Board.
- QCJWC – Quinquiparate Combined Joint Warfare Conference
- TTCP – The Technical Cooperation Programme.

2.19 The CCEB produces specifications for protocols that provision military collaboration between the five nations. These specifications are published in Allied Communications Publications (ACPs), which are specifically issued for guidance and implementation of the member nations.

2.20 Membership of these fora obligates New Zealand to consider interoperability with allies when upgrading or introducing new communication capabilities. Adhering to the protocols and standards issued by these organisations must be prioritised when planning and introducing to service ICT and CIS.

2.21 The interdependent nature of Command, Control, Communications and Computers (C4) requires AC CAP to understand all related C4 activities, programmes, projects, and operations to ensure the Defence Force is able both to operate independently if necessary and be interoperable with our allies. To ensure better collaboration and synchronisation across the C4 capability portfolio, AC CAP leads overall management of the full capability lifecycle for all C4 related capabilities from Capability Definition, introduction into service (IIS), through to removal and retirement from service. The Ministry of Defence is responsible for the acquisition of major capabilities.

Relationship between Information Operations and Communication Information Systems

2.22 Information operations rely on resilient, robust, and secure CIS networks to exercise effective C2 of operations in the information environment and to transport information to aid in understanding and decision-making. A resilient and secure CIS network is also needed for delivering information effects against target systems and target audiences. CIS rely on a number of information related capabilities (IRC) to create favourable conditions for successfully operating in the information environment:

- Information Assurance provides the framework to operate CIS securely and reliably
- Cyberspace Operations provide defensive measures and information about the environment
- Electronic Warfare and Operational Security guard against physical destruction and degradation.

Key Terms

Information Operation

The coordination of information effects to influence the decision making and actions of a target audience and to protect and enhance our own decision making and actions in support of national interests.

Information Related Capabilities

A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions.

Information Assurance

2.23 Information Assurance, a key component of information operations, is defined as ‘measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities. Information assurance comprises the activities undertaken to defend and protect information and information systems not only from direct attack but also from natural disaster and human error. Information assurance integrates people, operational techniques, and technology to protect information services, detect and react to intrusions or attacks, and restore information services as quickly as possible. This multi-layered approach, known as defence-in-depth of information assurance, is an NZDF-wide responsibility. Security requirements for NZDF employees are detailed in Defence Force Order (DFO 51(4)) *Security - Information Systems Security* and exercised through guidance from the Government Communications Security Bureau (GCSB) and CIS Branch. It must be remembered that:

- information is always at risk whether from natural, accidental, or deliberate actions
- it is not possible to ensure absolute protection of information, so risk profiles are developed and treatments assigned accordingly.

2.24 Information assurance aims to ensure the following objectives outlined below.

- **Integrity.** Protection against unauthorised or unintended modification or destruction of data.
- **Availability.** Timely and reliable access to data by authorised users.
- **Confidentiality.** Assurance that information is not disclosed to an unauthorised persons or people.

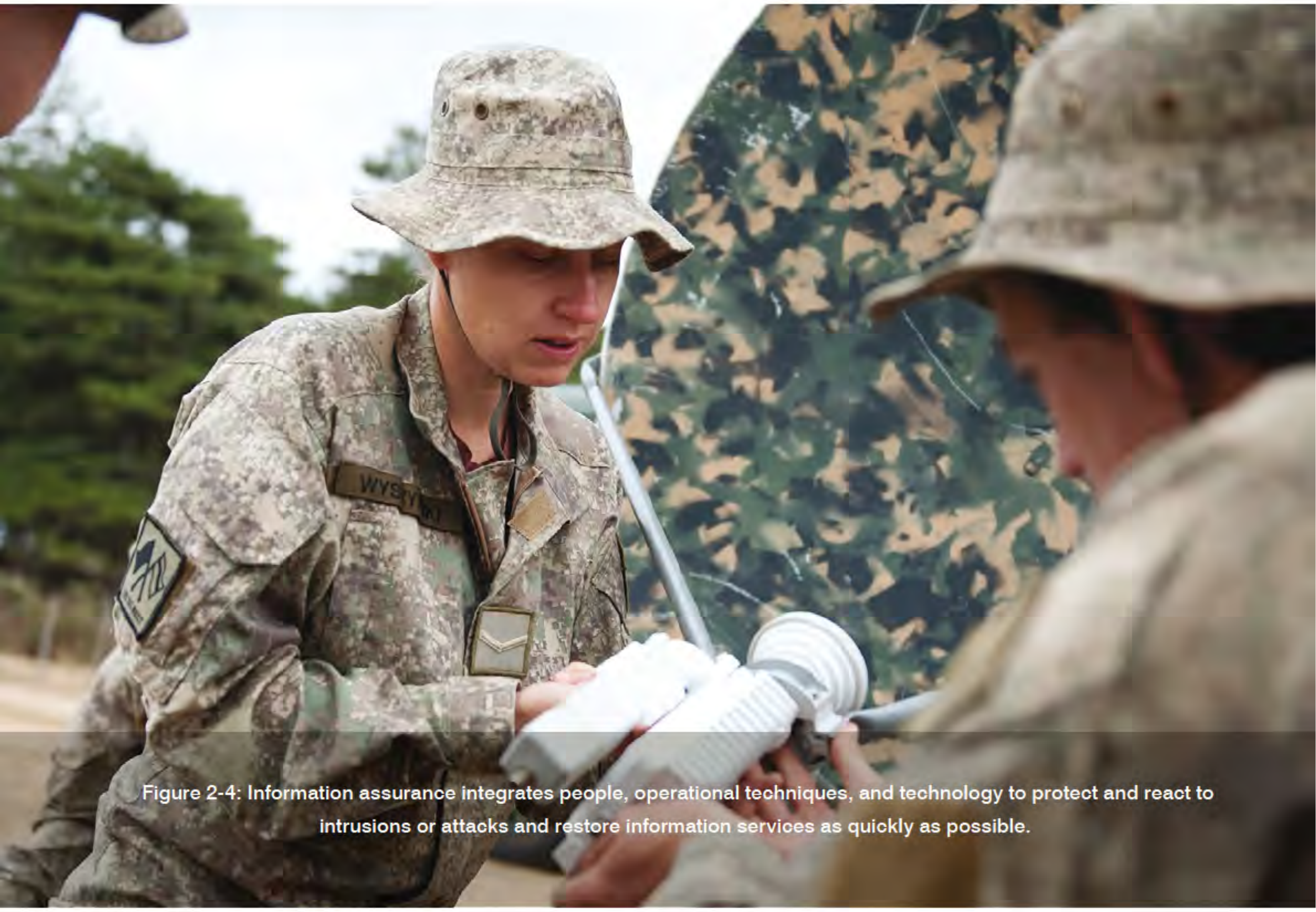


Figure 2-4: Information assurance integrates people, operational techniques, and technology to protect and react to intrusions or attacks and restore information services as quickly as possible.

- **Authenticity**. The combination of unique identification and authentication so the system recognises an entity. These may be security measures designed to establish the validity of a transmission, message, or originator; or means to distinguish between information that verifies, with some degree of assurance, an individual's authorisation to receive specific categories of information.
- **Non-repudiation.** Assurance that data is sent with proof of delivery and the recipient receives proof of the sender's identity so that neither can later deny having processed the data.

Key Term

Information Assurance

The measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Components of Information Assurance

2.25 The philosophy of defence-in-depth underpins the provision of information assurance. It embeds defence mechanisms at all layers of the information system, including people, operational techniques, and technology. Information systems use physical, procedural, and technical measures to provide security. These are not only passive, but also include preventative, detective, and incident response measures.

2.26 **Preventative Measures.** Actions taken to ensure operational security (OPSEC) and information security (INFOSEC), including the elements shown in Figure 2-5.

2.27 **Detective Measures.** A range of measures used to identify threats, intrusions, and attacks directed towards an information system. These include auditing, network sniffing, communications security (COMSEC) monitoring, and network monitoring.

2.28 **Incident Response Measures.** These are the equipment, processes, and procedures maintained for a rapid and thorough response mechanism to effectively manage, investigate, and contain incidents. Some measures implemented in response to incidents will be the same or similar to those implemented to protect CIS. What will differ is their scope or intensity.

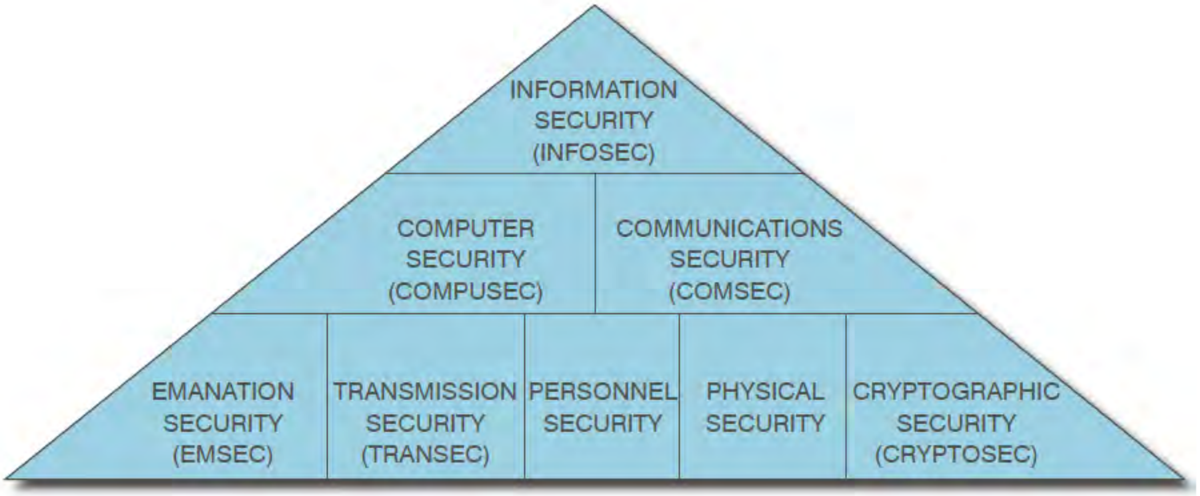

INFORMATION SECURITY (INFOSEC)
COMPUTER SECURITY (COMPUSEC)
COMMUNICATIONS SECURITY (COMSEC)
EMANATION SECURITY (EMSEC)
TRANSMISSION SECURITY (TRANSEC)
PERSONNEL SECURITY
PHYSICAL SECURITY
CRYPTOGRAPHIC SECURITY (CRYPTOSEC)

Figure 2-5: Information Security Components.

Preventative Measures

2.29 The NZDF collects, receives, develops, and transmits information to fulfil its operational and business functions. Information assurance provides the policy and doctrine to maximise the protection and availability of information to the users who need it. This protection is referred to as INFOSEC, which comprises a number of inter-related elements as shown in Figure 2-5.

2.30 The term 'information' in the context of information assurance encompasses documents, electronic data, software, systems, and networks on which information is stored, processed, and communicated. Information is knowledge acquired by individuals and physical items from which information regarding design, components, and use could be derived.

Key Term

Information

The knowledge acquired by individuals and the physical items from which information regarding design, components or use could be derived.

2.31 While all official information has utility, some is especially valuable to the NZDF because it is critical for the Defence Force in performing its functions and because the consequences of compromise or misuse of information could adversely affect New Zealand, the Government, community, or the individual to whom it relates. For these reasons, the NZDF is required to identify and classify such information through sound risk assessment and ensure it is protected from compromise and misuse.

Communications Security

2.32 Whenever transmissions are made over a communications circuit, it must be assumed that an adversary can intercept and record them to gain information. Every possible precaution must be taken to ensure transmissions are protected against interception and exploitation, such as by direction finding. COMSEC is a component of information assurance. It deals with measures and controls taken to prevent unauthorised persons derviving information from telecommunications and ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material[3].

2.33 The GCSB is the National Authority responsible for advising all government agencies on all aspects of INFOSEC, including COMSEC. COMSEC information may be released by GCSB to appropriately security cleared commercial companies to support their involvement in New Zealand Government projects and assist them in the design and development of equipment for government use. Responsibility for COMSEC in the NZDF is as follows.

- **Governance**. The CCIS is the NZDF's Departmental COMSEC Officer (DCO). The COMSEC Governance Group (CGG) provides subject matter expertise in cryptography and provides a platform from which guidance and direction can be given to all communities involved in the planning, use, and TLS of COMSEC systems . To obtain relevant wider decision making information, it engages with the DLC Integrated Logistic Support Centre of Expertise and other TLS constituent groups/service providers across the NZDF. Policy Advisor COMSEC (PACOMSEC) has day to day responsibility for COMSEC within the DIE.

- **Single Services, Headquarters Joint Forces New Zealand**. Service Chiefs and COMJFNZ in liaison with the DCO appoint single Service and HQJFNZ COMSEC officers.

- **Defence Information Environment, Joint and Coalition**. As part of normal COMSEC planning, routine COMSEC key requirements are processed through the New Zealand Defence Force Distribution Authority (NZDFDA). For new COMSEC equipment or keying matrial, requests come to PA COMSEC. Distribution is through the NZDFDA.

[3] As defined in Committee on National Security Systems Instructions (CNSSI) No. 4009 *National Information Assurance – Glossary*

Cryptographic Security

2.34 Cryptographic Security (CRYPTOSEC) is a component of COMSEC focussed on provision of technically sound cryptographic systems and their proper use.[4]

2.35 CRYPTOSEC protection protects NZDF information in transit and at rest. These cryptographic systems include

- **Technical**. Network and removable storage media based systems, which perform the processes of encryption and decryption automatically and simultaneously
- **Manual.** Low-grade tactical codes used to protect transmission of short-term classified tactical information normally transmitted via non-secure radio nets or circuits.

Emanations Security and TEMPEST

2.36 All electronic systems produce unwanted electromagnetic emanations, which can be related to any information being processed. These emanations can cause interference with nearby equipment or may be intercepted and used to extract the information being processed. Emanation Security (EMSEC) are protective measures taken to prevent unauthorised individuals deriving information from interception and analysis of compromising emissions from crypto-equipment or an information system. TEMPEST refers to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.[5] These investigations are conducted in support of EMSEC.

2.37 Compromising emanations can come from all electronic devices, including computer keyboards and visual display units. The majority of modern consumer grade devices have been designed to limit emanations in order to avoid interference with wireless networks and other devices. However, when electronic equipment is used to process classified information in high risk environments, expert advice should be sought at the earliest possible stage of planning, particularly in relation to equipment selection and acquisition. Doing so ensures the maintenance of security standards within the NZDF and economic implementation of TEMPEST reduction techniques.

2.38 The New Zealand Information Secuirty Manual (NZISM) is the paramount policy for information security matters, including TEMPEST and EMSEC. The GCSB, the national authority, provides specific standards relating to TEMPEST and EMSEC policy. These are generally classified publications; copies are held by the NZDF Radiation Hazard (Radhaz) and TEMPEST Unit, HMNZS PHILOMEL, Auckland. Advice on current standards used for contract deliverables and platform, facility, and equipment compliance is obtainable from the NZDF Radhaz and TEMPEST Unit.

Emission Control

2.39 Emission control (EMCON) is the effective management of all electromagnetic emissions or emanations from a friendly force. Effective EMCON reduces the risk of disclosing the presence, location and composition of friendly forces to the enemy, while still operating sufficient equipment to maintain command and control, and to provide adequate warning of a threat. If it is to effectively support strategic and operational aims, the EMCON intent of a commander must be integrated into the CIS plan and be coordinated with other friendly users of the electromagnetic spectrum.

2.40 EMCON plans aim to exploit any limitation of an enemy's electromagnetic activities by permitting only the use of emitters that have a low probability of interception. An EMCON plan may impose a variety of radiation status indicators upon frequency bands or specific emitters, designating conditions they use. In addition to supporting a commander's aim, EMCON plans need to be sufficiently flexible to cope with changes to the operational or tactical situation.

[4] As defined in *Committee on National Security Systems Instructions* (CNSSI) No. 4009

[5] As defined in CNSSI No. 4009

2.41 **Responsibilities**. The basis for developing an EMCON plan should be determined during the CIS and EMS planning process. As an operational planning process, this is achieved through the HQJFNZ's Joint Communications Planning Group's deliberations. Guidance that allows deployed commanders to formulate their own EMCON plan is normally included in the relevant CIS Support Plan or Communications-Electronics Operating Instructions.

2.42 **Planning.** Achievement of the joint commander's intent for EMCON is to be planned at the highest appropriate level. The joint commander needs to be fully briefed and aware of the ramifications of the EMCON plan being implemented, prior to approving the plan's activation. The Commander retains the right to impose, amend, or lift the EMCON plan to suit the situation. EMCON plans should follow the conventions as detailed in the NZDF approved ACP-190 *Guide to Electromagnetic Spectrum Management in Military Operations,* particularly in respect to risk management.

2.43 **Security Risk Assessment**. Security measures are generally aimed at reducing the level of risk. It is impossible to operate in a risk-free environment but it is possible, although sometimes expensive, to reduce the risk level. The security measures, as determined through a vulnerability and/or threat and risk assessments, require implementation commensurate with the classification and/or sensitivity levels of the information being handled, stored, processed, or transmitted, and the system assets, to ensure that confidentiality, integrity, availability, and accountability concerns are adequately addressed.

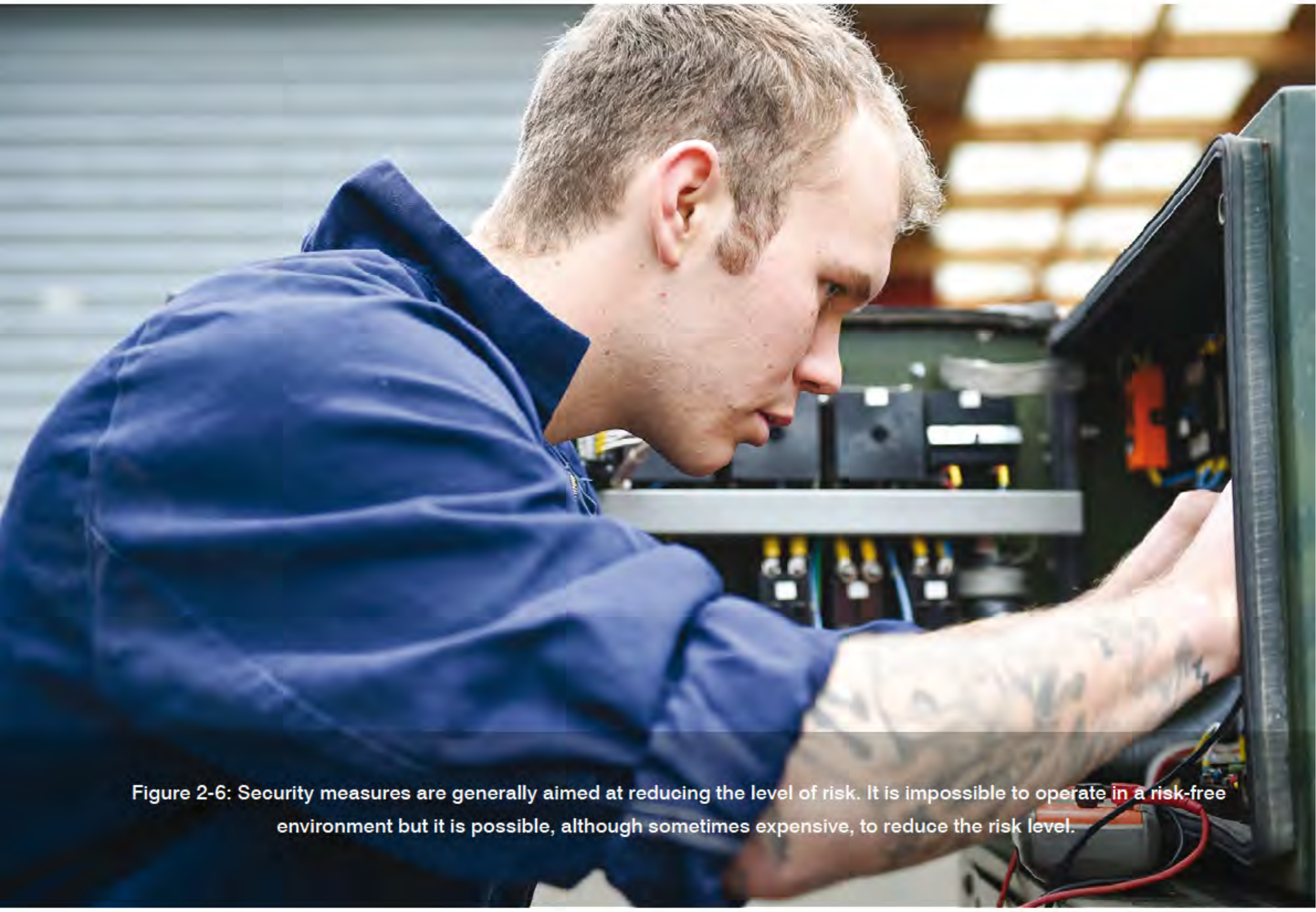


Figure 2-6: Security measures are generally aimed at reducing the level of risk. It is impossible to operate in a risk-free environment but it is possible, although sometimes expensive, to reduce the risk level.

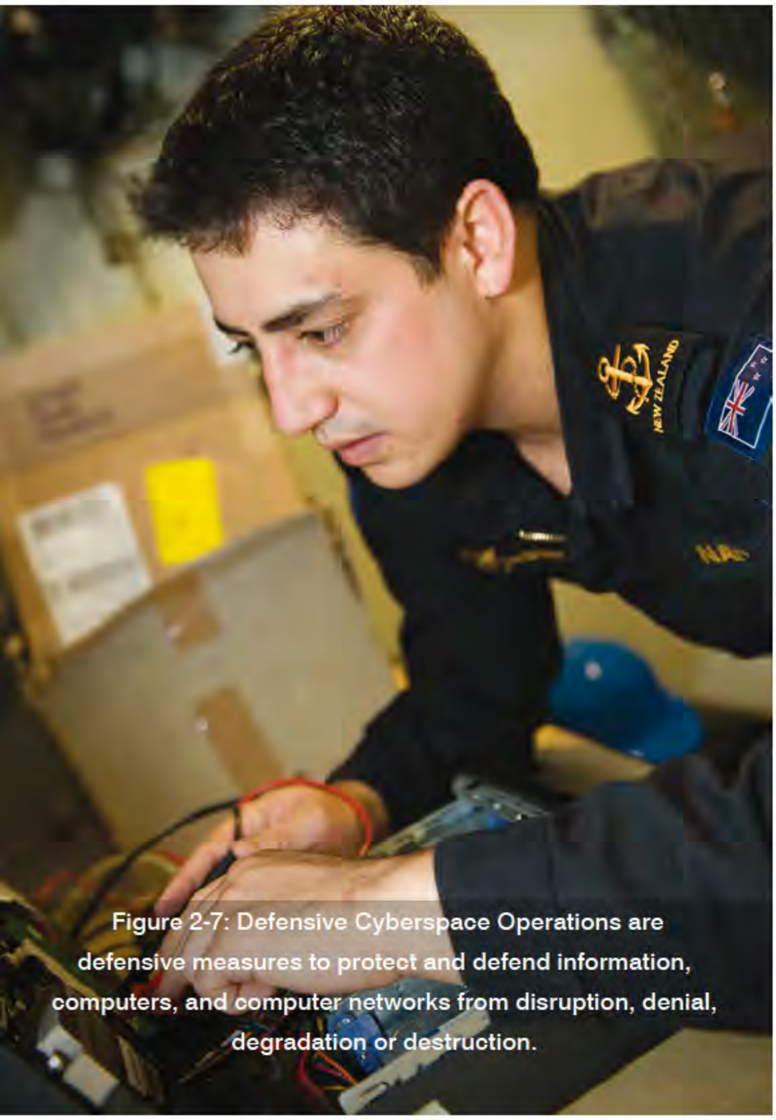


Figure 2-7: Defensive Cyberspace Operations are defensive measures to protect and defend information, computers, and computer networks from disruption, denial, degradation or destruction.

2.44 CIS risk mitigation is achieved in the NZDF through sound physical, personnel, and technical protection mechanisms, including Defensive Cyberspace Operations (DCO), computer network defence (CND), and COMSEC equipment. Overarching these mechanisms is the accreditation process that serves to ensure that the physical and electronic protection of information and related processes meet the required security standards.

Defensive Cyberspace Operations

2.45 DCO are defensive measures to protect and defend information, computers, and computer networks from disruption, denial, degradation, and destruction. They provide coordinated and dynamic defence of the NZDF's CIS networks against adversaries efforts to attack or exploit those networks.

2.46 Attempting to achieve information superiority over adversaries requires the NZDF places more dependence on its CIS. It also demands increased interconnection of its own networks and interconnection with allies, partners, and industry. This increases the susceptibility of the NZDF's networks to attacks in cyberspace.

2.47 The NZDF must preserve and protect its CIS networks from penetration and attack to maintain its ability to conduct operations. Because of the NZDF's increasing reliance on commercial off-the-shelf products, whose vulnerabilities are often identified and exploited, it must be able to detect, react, and recover from attacks dynamically to ensure operational continuity.

2.48 The defence of CIS is therefore achieved by having a combination of:

- the relevant processes, organisation, and an effective command structure that carry out cyber defence across, and on behalf of, the NZDF
- a minimum set of gateways that monitor and control the flow of traffic between internal and external security domains
- a set of intrusion detection sensors and tools on the best commercial and government off-the-shelf capability at all inter-domain gateways and key points
- monitoring and reporting systems, both electronic and procedural, to control the deployment and use of these sensors and tools
- technical security procedures that identify vulnerabilities and check the effectiveness of cyber defence
- rules of engagement, which permit the cyber defence organisation to conduct the defence of the CIS networks within the legal framework
- a set of supporting information assurance measures.

Key Term

Defensive Cyberspace Operations

Passive and active cyberspace operations intended to preserve the ability to utilise friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.

Detective Measures

2.49 Detective measures address management of the people, components and networks.

2.50 **Compliance Auditing**. Standard operating procedures provide a framework of accountability and processes that guide information system security officers and operators in administering the system and correcting non-compliances. The procedures cover normal operating processes and known exception and emergency activities.

2.51 **Intrusion Detection**. Intrusion detection involves recognising unauthorised and malicious entry into the NZDF's network. This includes monitoring for suspicious packet traffic, tracking intruders, and identifying security holes. It also involves detecting misuse inside the network, whether intentional, malicious, or accidental.

2.52 **Monitoring Communications.** COMSEC monitoring is searching for, listening to, and recording of one's own transmissions and, when specifically agreed (for example on combined operations orexercises), those of friendly forces. This is done for analysis and reporting to improve security, training, and standard operating procedures. It involves monitoring friendly CIS by friendly COMSEC monitoring units to provide commanders with insight into what the enemy can obtain by monitoring, deduction, and analysis of our transmissions. COMSEC monitoring is an important aspect of both training and operations and it allows commanders to assess transmission security within their respective commands. This allows commanders to take positive steps to pinpoint and correct insecure areas, thereby making the enemy's interception, analysis, and imitative deception much more difficult.

2.53 **Vulnerability Analysis.** Vulnerability analysis uses automated tools and techniques to scan equipment and software for known security vulnerabilities. Vulnerability analysis activities should be conducted at frequent intervals as new vulnerabilities in commercial software and equipment are regularly discovered. The goal of vulnerability analysis is to reduce the time that CIS is vulnerable to attack.

2.54 **Network Monitoring.** NZDF network operations centres manage threat responses to their respective networks. Threats include viruses, worms, macro viruses, logic bombs, and Trojan horses. Countermeasures used include commercial products that prevent and remove malicious code, electronic security (access constraint countermeasures), trapdoor access constraints, network security, connection and password sniffing, and physical security.

Incident Response Measures

2.55 Incident response measures include computer emergency responses, such as restoration of services, withdrawal of access privileges, and procedures for investigating loss of information or damage to the information system and for determining its effects. An effective incident response process is critical to confirm quickly and concisely if a system has been compromised.

Real-life example

Cryptography

Codes and ciphers have been used by military organisations for centuries to protect their information. By World War I the major powers had significant cryptological organisations, but it was during World War II that cryptography developed to such an extent that it made a vital contribution to Alied vicotory. The Enigma cipher was invented in 1918 to secure banking communications. The German military soon saw its potential and began to use it for military communications. Enigma was such a great advance on previous cryptographic machines, the Germans thought it was unbreakable. However, the Poles had broken Enigma before the War and in 1939 passed their knowledge to the British and French. Not only had the Poles cracked Enigma, they had managed to reconstruct an Enigma machine: this proved crucial to British efforts. At Bletchley Park, near London, teams worked to break Enigma. By exploiting Enigma's inability to encrypt a letter as itself and errors by German operators, the Enigma code was broken in January 1940. Wireless stations around Britain intercepted German communications and forwarded the messages to Bletchley, where they were decoded and analysed. To speed up the code breaking process, the brilliant mathematician Alan Turing developed an idea originally proposed by Polish cryptanalysts, which eventually resulted in the Bombe: an electro-mechanical machine that greatly reduced the odds and time required to break the daily-changing Enigma keys.

CHAPTER 3:

PLANNING, ENGINEERING, AND TECHNICAL CONTROL

CONTENTS

Introduction

3.01 This chapter identifies the principles and responsibilities for communications and information systems (CIS) planning, provides an overview of CIS design and engineering, including electromagnetic spectrum (EMS) management, and identifies the principles and responsibilities for technical control and management of CIS assets.

3.02 Employment and control of CIS assets need to be carefully considered in the CIS planning. Commanders at all levels must be supplied with system capability and connectivity, so that aggregation, manipulation, and presentation of information is achieved in a clear and concise format. This enables timely and informed decision making.

3.03 CIS personnel are required to manage the New Zealand Defence Force's (NZDF's) systems and networks for a variety of roles. Principles need to be considered, balanced, and incorporated into management techniques that best meet commanders' requirements. It is important that CIS planners, particularly at the strategic and operational levels, understand current in-service CIS capabilities, systems, and networks that are available to support the NZDF's campaigns, operations, and activities. This ensures maximal use of these capabilities to commanders' intent.

Employment and Control

Decentralised Execution

3.04 Decentralised execution allows flexibility and redundancy to be incorporated into operational and tactical CIS support plans. Evolving technologies lead to development of new capabilities, and the NZDF seeks to use technology to maximise the impact of its force and provide enhanced capabilities to achieve more effectively its overall mission. The NZDF avoids

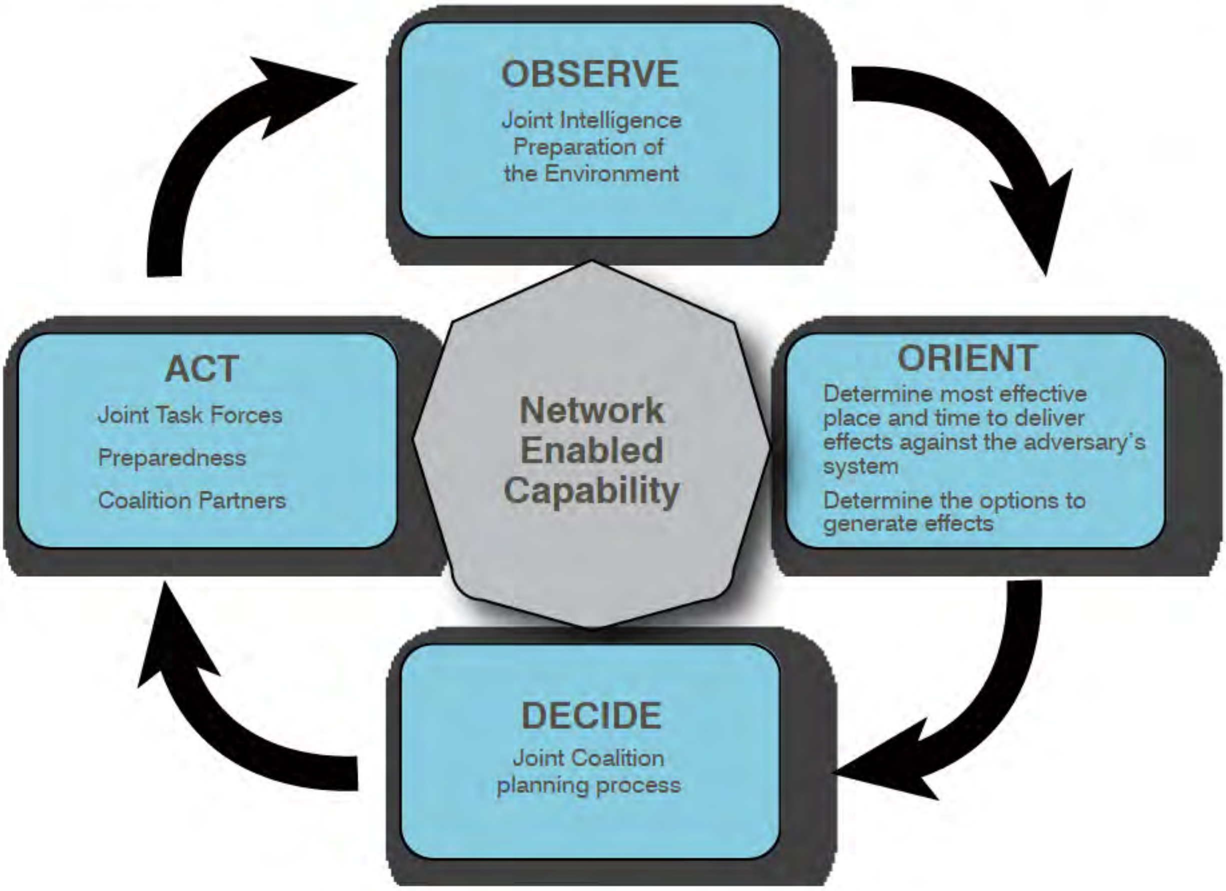

OBSERVE
Joint Intelligence Preparation of the Environment
ORIENT
Determine most effective place and time to deliver effects against the adversary's system
Determine the options to generate effects
DECIDE
Joint Coalition planning process
ACT
Joint Task Forces
Preparedness
Coalition Partners
Network Enabled Capability

Figure 3-1: Observe, Orient, Decide, and Act Loop.

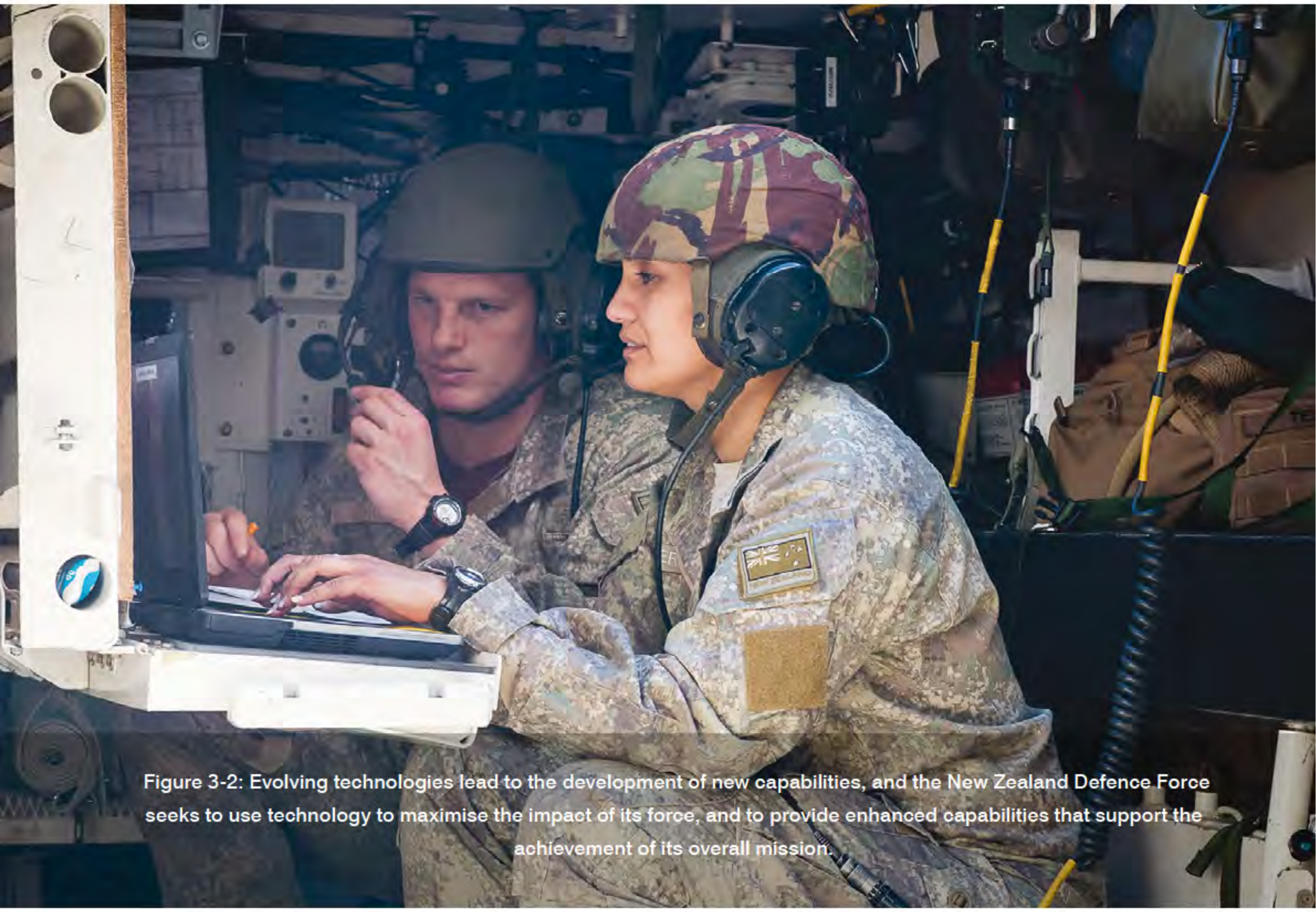


Figure 3-2: Evolving technologies lead to the development of new capabilities, and the New Zealand Defence Force seeks to use technology to maximise the impact of its force, and to provide enhanced capabilities that support the achievement of its overall mission.

the resource-intensive inefficiency of 'attrition warfare'. It aims instead to use manoeuvre concepts to minimise casualties and collateral damage, along with achieving desired outcomes as quickly as possible. It is therefore important that CIS capabilities keep pace with the improvements in other capabilities.

3.05 Planning for the use of national power[6] involves taking an all-of-government (AoG) and comprehensive approach to security, communications, and industry support. These often conflicting aspects require an appropriate balance to achieve designated national objectives. Diplomatic, military, and economic considerations need to be considered when developing an appropriate strategy. These are in turn. All of these are in turn enabled by information. Other factors including environment, culture, society, and religion must also be taken into account.

3.06 Commanders and planners seek to apply strength against weakness more quickly and decisively. Maximising surprise and deception requires the ability to act quickly, reach out to the critical place at the right time, and create simultaneous problems that adversaries cannot resolve. For the NZDF to fight this way, it needs to be deployed quickly and be sustainable both at home and overseas. Relevant and protected information, with concomitant skills to plan and control forces, are essential for our people to fight and win.

[6] NZDDP–D *New Zealand Defence Doctrine* (3rd Edition)

3.07 Unpredictable enemy forces and manoeuvre actions by friendly forces continually change the situational picture. Planners and commanders need to progress constantly through the Observe, Orient, Decide, and Act Loop, a decision-action cycle shown at Figure 3-1. The process is unified by one purpose: achieving the Commander's intent.

Establishing the Integrated Network

3.08 Establishing the network and the integration and exchange of information across it are fundamental to the NZDF's ability to plan and execute campaigns and joint operations. The integrated network essentially consists of a collection of nodes (computers, communication devices, and infrastructure) linked to network components allowing users to enact mission processes by accessing, creating, and sharing information, applications, and interfaces with internal and external systems.

3.09 However, networks are required to connect a vast and diverse array of joint, interagency, and multinational systems, all of which will be required to operate seamlessly in all environments and security domains, as well over a disparate array of communications means and linkages. A range of NZDF-level common services, including governance and compliance mechanisms, is also needed to support information integration and exchange within and between environments and domains, and with allies, coalition partners, and other government agencies operating outside the Defence Information Environment (DIE).

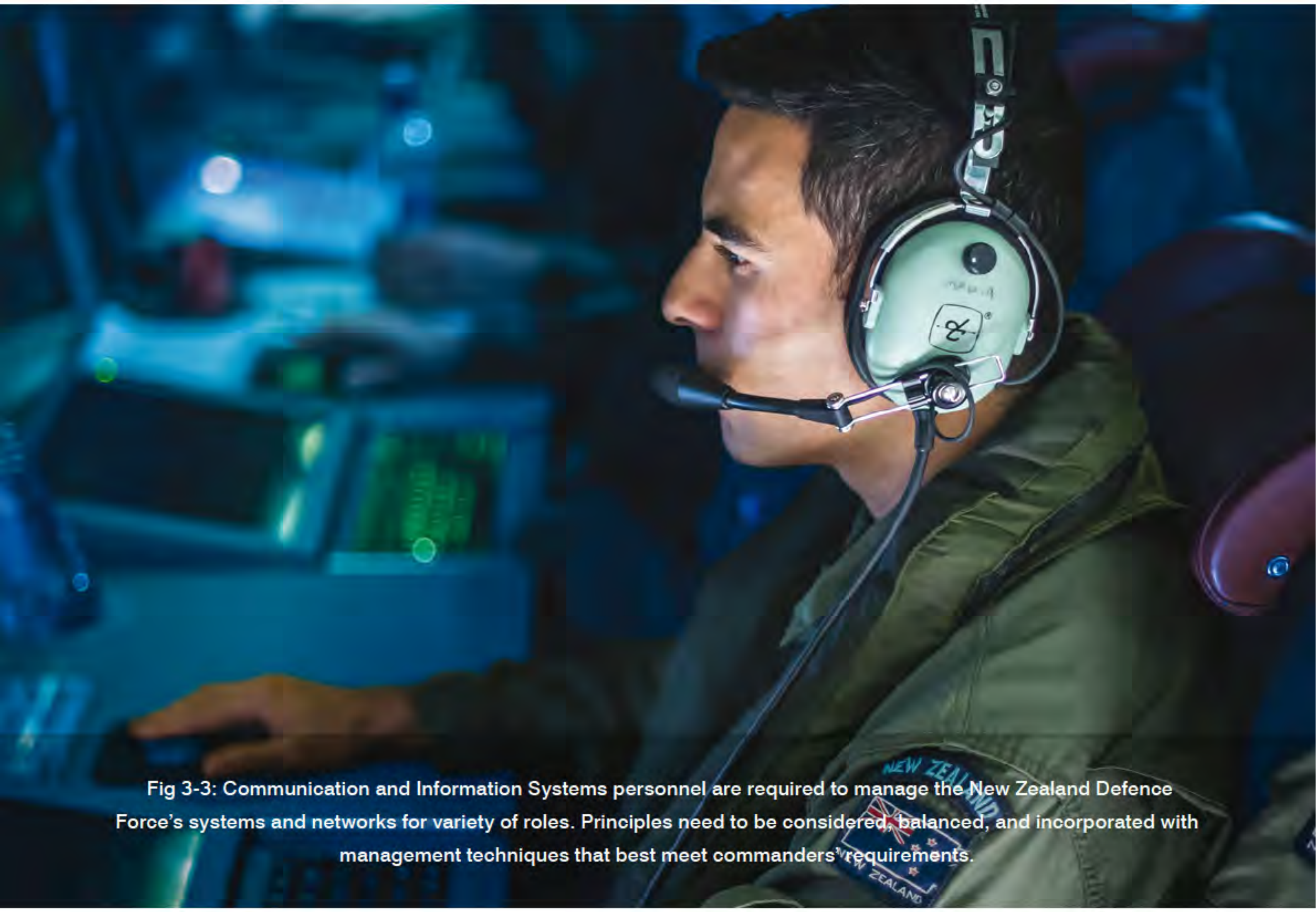


Fig 3-3: Communication and Information Systems personnel are required to manage the New Zealand Defence Force's systems and networks for variety of roles. Principles need to be considered, balanced, and incorporated with management techniques that best meet commanders' requirements.

3.10 The integrated network is also required to pass various forms of information and data at various transmission rates and security levels. Information is then processed through a combination of machine and human interfaces. In addition to meeting these operational requirements, the network must also meet high requirements for security, robustness, capacity, and congestion management.

Technical Control

3.11 CIS technical control has a fundamental relationship to command[7]. Exercise of technical control may require or force a technical imperative to influence a command decision; for example, the appointment of a Mission Joint CIS (J6) as the lead technical authority within a theatre of operations is a critical requirement. The Mission J6 is able to advise the joint commander where emitters such as radar heads should be placed, but can also order that emitter to be turned off should it becomes apparent that it has become a target or a threat to the security of the force elements within the Joint Task Force (JTF).

3.12 CIS technical control is based on principles of centralised management and decentralised execution. Centralised management allows for the necessary degree of guidance and control required for integration of CIS at the strategic level. Decentralised execution allows for flexibility and redundancy to be incorporated into CIS operational and tactical support plans.

3.13 There are a number of key individuals and groups who exercise CIS technical control within the NZDF.

3.14 **Chief, Communications and Information Services**. The Chief Communications and Information Services (CCIS), on behalf of the Chief of the Defence Force (CDF), is responsible for the governance, coordination, development, through life support and management and security of the DIE. The CCIS is the Enterprise Prime System Integrator (EPSI) for the DIE. This is exercised through a number of committees and working groups within the NZDF. The Chief Technology Officer (CTO) within the CIS Branch is responsible for the DIE architecture and technical standards and certification.

3.15 **Strategic J6**. The Strategic J6 is a COL (E) military officer who is the primary military advisor to the CDF on CIS and EMS matters. The Strategic J6 is responsible for the efficient operation of the DIE and provision of CIS advice. The Strategic J6's staff provides CIS advice to the J6 staff at Headquarters Joint Forces New Zealand (HQJFNZ), with which it works closely to manage the information capability and the provision of CIS support to operations.

3.16 **Commander Joint Forces New Zealand**. The Commander Joint Forces New Zealand (COMJFNZ) commands HQJFNZ and exercises command over assigned force elements and joint task forces when raised. HQJFNZ plans, controls, and conducts campaigns, operations, joint exercises, and other activities on behalf of the CDF. The HQJFNZ J6 is responsible to COMJFNZ for day-to-day management of theatre CIS, technical coordination, and control measures to support current theatre activities and the control and prioritisation of theatre CIS assets.

Key Term

Technical Control

The specialised or professional guidance and direction exercised by an authority in technical (professional) matters.

3.17 The following groups bring together the various command level communications officers and system controllers responsible for technical control for each particular theatre, joint force or other area of operations (AO), node, or specific equipment. Technical control is not an operational authority. It is specialised or professional guidance and direction, exercised by technical authorites on behalf of commanders in accordance their command priorities. Technical control ensures system elements are managed as part of a total capability. The relationships between these technical control elements of NZDF CIS management is outlined below.

[7] See NZDDP 00.1 – *Command and Control* (2nd Edition)

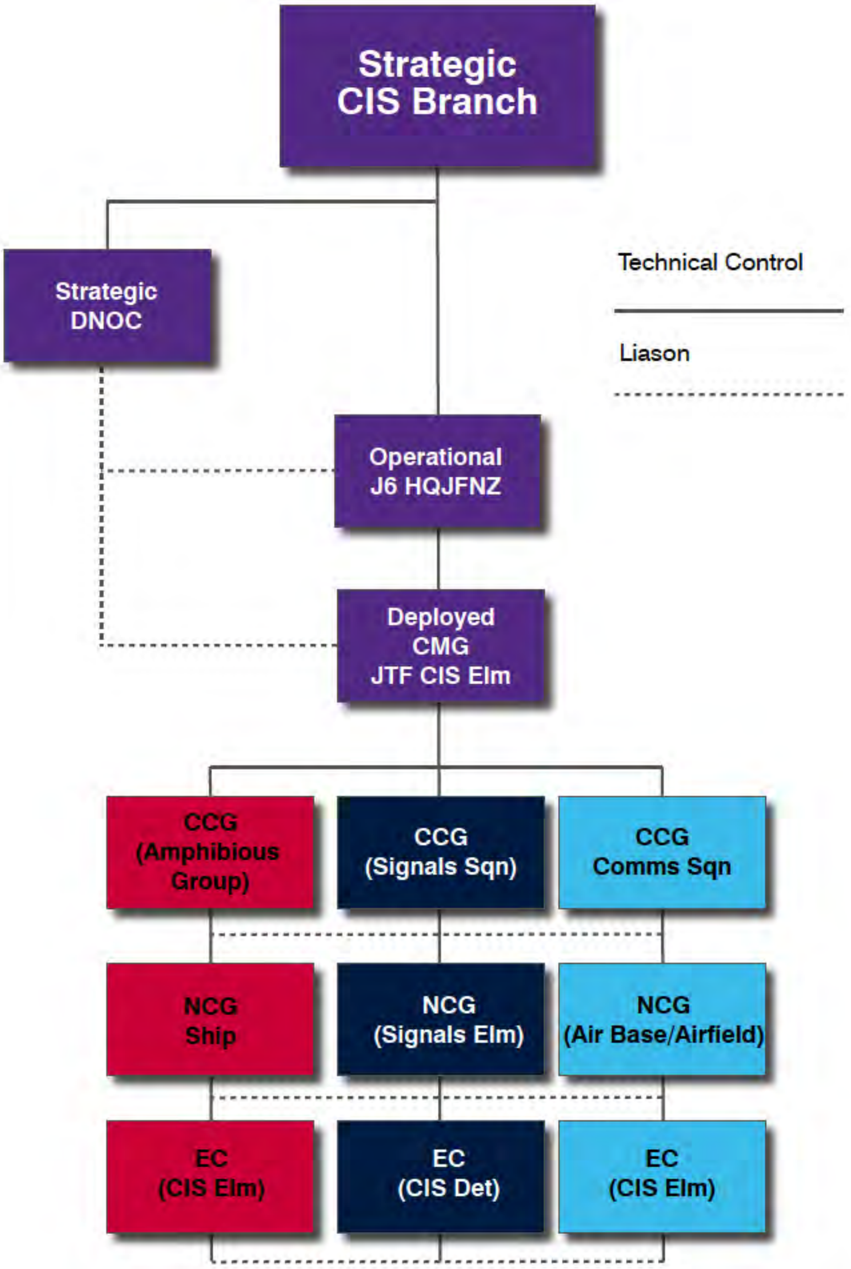


Figure 3-4: Indicitive Communications and Information Systems Technical Control Chain.

- The Strategic J6 exercises end-to-end technical control of all NZDF military communications. Advice is given by the Communications Information Systems Command and Control Coordiating Group (C4G), of which the Strategic J6 is chair.
- The Defence Network Operations Centre (DNOC) is the first response agency for all incident and fault reporting as well as control for the DIE.
- The J6 Staff at HQJFNZ is responsible for overall control and management of deployed CIS assets.
- For each operation a Deployed Communications Management Group (CMG) is normally formed by the senior deployed headquarters and commanded by the senior CIS officer, for example the JTF J6. CMGs may be single Service, joint, combined, or coalition. They are responsible for overall control and management of deployed CIS assets within their allocated AO.

- The Communications Control Group (CCG) for each formation controls a number of subordinate CIS elements, which are specified by their CMG, deployed into the CCG's designated area.
- The Nodal Control Group (NCG) for each node of a communications network is responsible for exercising technical control over all CIS equipment in that node. An NCG is normally established when the complexity or diversity of CIS facilities warrants central CIS management within a particular location.
- An equipment controller (EC) is responsible for engineering, maintenance, and operation of allocated CIS equipment in accordance with unit and system standard operating procedures or technical control handbooks.

3.18 Figure 3-4 shows how joint headquarters and their allocated CIS units may be organised hierarchically to exercise technical control to meet particular operational requirements. The colours indicate the Service from which the control elements would be allocated to a JTF, as opposed to when operating along single Service lines[8].

Planning

3.19 Joint CIS planning and control occur in two dimensions across all levels of command and types of operation across the full range of potential security events:

- **Functional.** Functional planning is integration of the aims and intentions of the commander into CIS plans, orders, and control procedures.
- **Technical.** Technical planning is integration of functional CIS plans, orders, and control procedures into supporting technical plans, directives, databases, and control systems.

3.20 The coupling between the functional and technical planning dimensions must be closely synchronised. Like all organisational constructs, they tend to merge under certain conditions and within certain organisations. This is certainly the case when considered within the context of the DIE (detailed in Chapter 1). The functional dimension of CIS planning and control spans both the business and operations information domains. The technical dimension is weighted towards management of NZDF information infrastructure elements: data, applications, services, user devices, systems hardware, networks, datalinks, bearers, and more.

3.21 CIS planning is a vital part of any appreciation process and it sometimes limits joint commanders' plans. However, such limitations are only likely to occur if planning personnel do not anticipate requirements quickly enough. Planning and operations staffs must be aware CIS assets are finite resources, which require skilled personnel, capable equipment, bandwidth, and spectrum. Redundancy is required for survivability and continuity of operations. Compromises may be necessary when balancing operational requirements with CIS resource availability, mobility, and acquisition timeframes.

3.22 CIS planning must begin simultaneously with the start of operational planning and in conjunction with the planning activities for EMS use by non-CIS devices, logistics, electronic warfare, and information operations. This will require a sound understanding of the Joint Military Appreciation Process (JMAP).

Command Structure

3.23 NZDF command has a three-level structure: strategic, operational, and tactical[9]. CIS requirements for each of these levels changes to meet the needs of operational phases and planning processes. The ability of modern communications to reach across all three levels of command is an issue that needs to be considered in all phases of CIS planning.

3.24 There are also strategic, operational, and tactical interfaces to allies, coalition partners, non-government organisations, and other government

[8] For details of technical control for tactical interfaces and formal messaging, see Defence Force Order (DFO) 106 *Communications, Standing Orders, and Plans*.

[9] Detailed in NZDDP 00.1—*Command and Control* (2nd Edition) Chapter 2

departments that need to be taken into consideration by CIS planners. The technical and procedural interoperability between all of these elements needs to be determined and prioritised if commanders and communications staffs are to deploy and manage the information requirements of commanders and support organisations to achieve the mission. A contextual overview of these interfaces is shown at Figure 3-5.

Operational Planning

3.25 For The campaign and operations planning the NZDF employs the Joint Military Appreciation Process (JMAP) process. This process is detailed in New Zealand Defence Doctrine Publication (NZDDP) 5.0—*Joint Operations Planning* and NZDF approved Australian Defence Force Publication (ADFP) 5.0.1—*Joint Military Appreciation Process* (2nd Edition). CIS planning aspects are detailed in ADFP 6.0.1—*Communication and Information Systems Planning*.

- A campaign is a set of military operations planned and conducted to achieve a strategic objective within a given time and geographical area, which normally involves maritime, land, and air forces.
- An operation is a series of tactical actions, such as battles and engagements, conducted by

Key Terms

Campaign

A campaign is a series of related operations aimed at achieving strategic and operational objectives within a given time and space.

Operation

An operation is series of military actions or the carrying out of a strategic, tactical, Service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defence, and manoeuvres needed to gain the objectives of any battle or campaign.

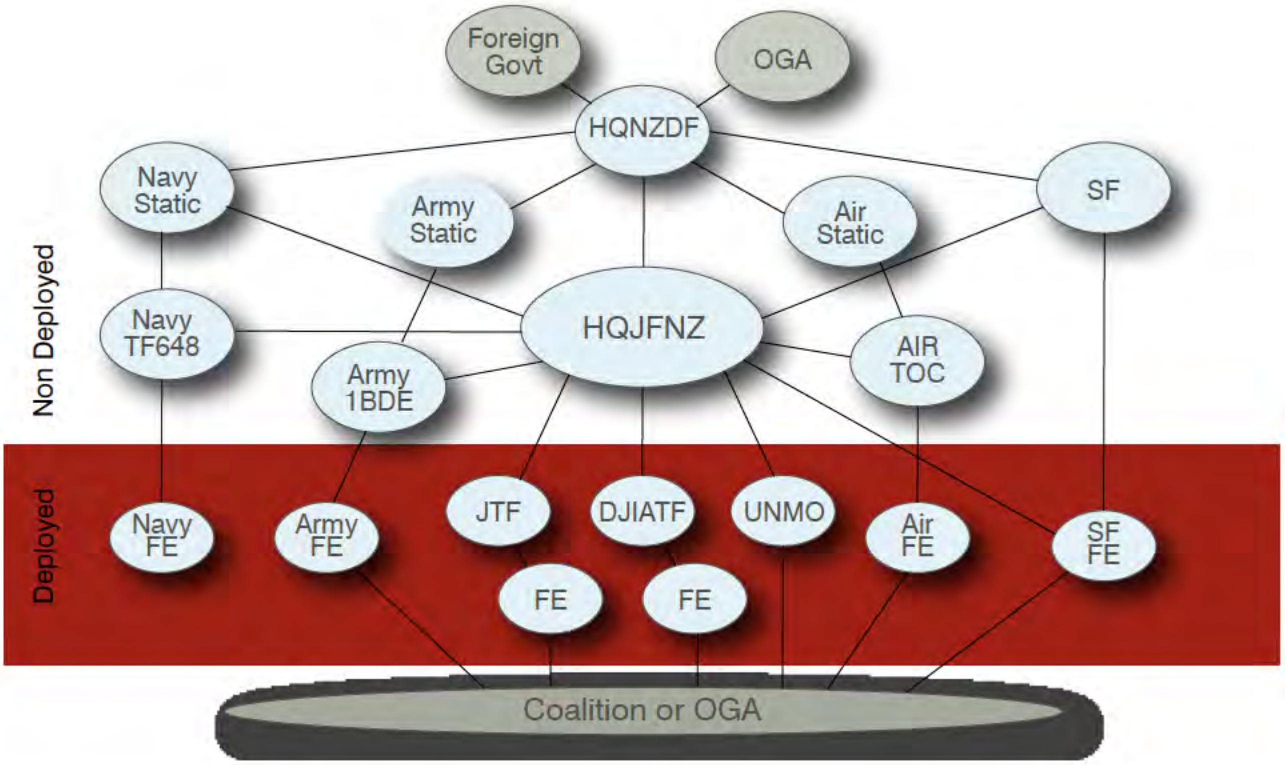


Figure 3-5: Context of New Zealand Defence Force Interfaces.

the elements of one or more Service, needed to achieve the objectives in the operational area. An operation may be a phase within a campaign or it may stand alone as a single event. The duration is generally measured in days and weeks.

3.26 **Types of Planning**. There are two types of planning:

- **Deliberate.** Deliberate planning is normally undertaken without undue time constraints or the need for immediate action. This allows for wide consultation, detailed analysis of information, and a more detailed product. Because of the time involved in deliberate planning, it is usually done in anticipation of a known or likely event. This is known as contingency planning, which also may be done in reaction to an event when there has been sufficient prior knowledge or warning, such as when reviewing or updating existing commitments.
- **Immediate**. Immediate planning creates military options to meet an actual, developing crisis. It takes place within a constricted time scale to meet short-term and usually unexpected security challenges or crises.

3.27 Campaign or operations planning is conducted at strategic and operational levels using either the deliberate or immediate processes. It aims at orchestrating tactical means in operational ways to achieve strategic ends, which is informed by the Government's strategic guidance. Determining needs for sequels, branches, and prioritisation of assets are all part of campaign and operations planning.

Predeployment and Deployment Considerations

3.28 **Predeployment Activities.** the JTF Commander (JTF Comd) is designated and forces

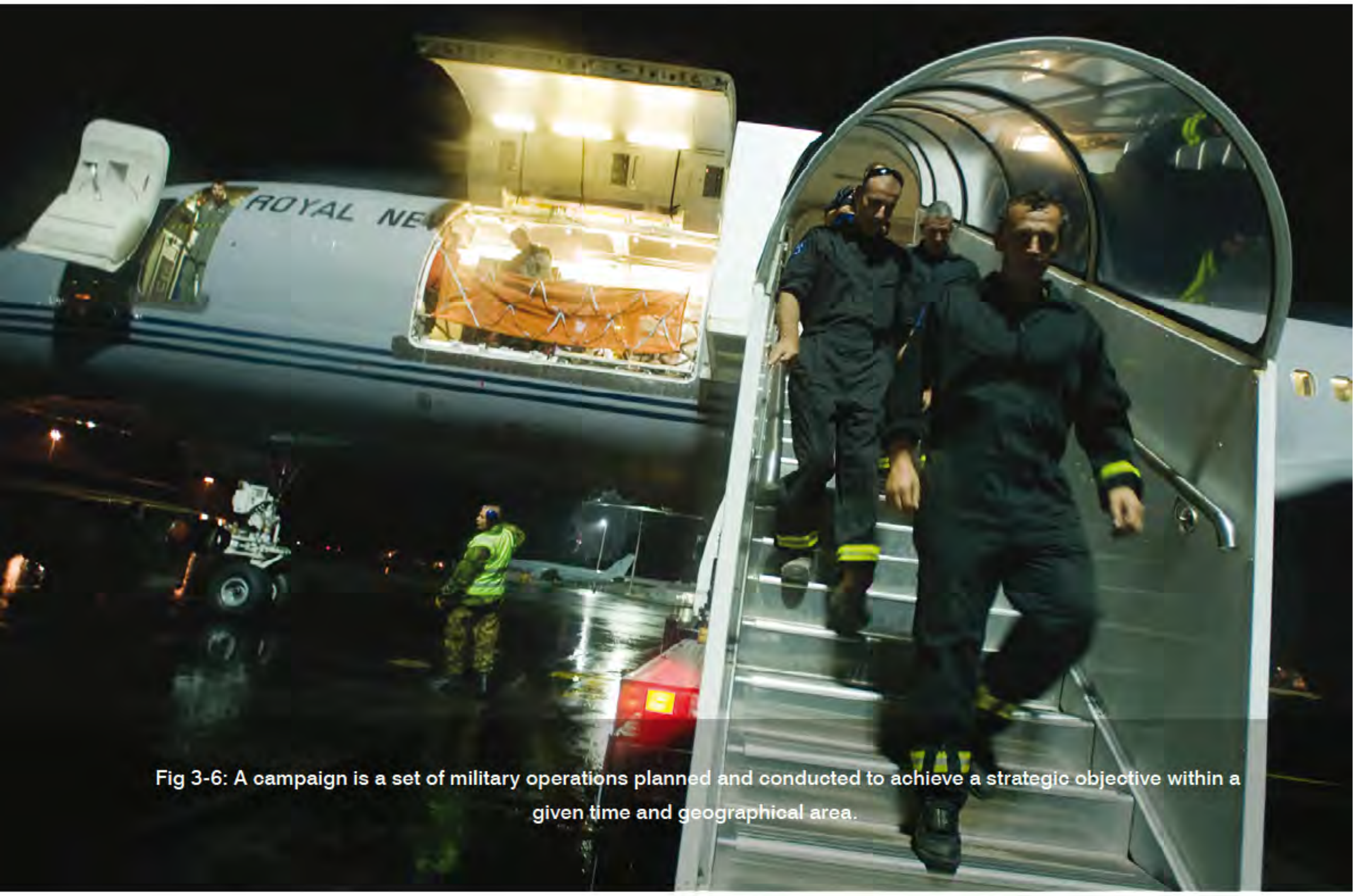


Fig 3-6: A campaign is a set of military operations planned and conducted to achieve a strategic objective within a given time and geographical area.

are assigned. The COMJFNZ's initiating directive provides the JTF Comd with guidance to initiate planning. The JTF Comd issues a mission statement and commander's intent, after which the CONOPS is developed. Predeployment activities produce a CIS plan to support the commander's intent, mission, and CONOPS. CIS deployment packages are prepared to provide initial operating capability to support the campaign or operations plan (OPORD). Planning of embedded communications to support initial tactical entry may also be required.

3.29 The J6 staff uses the planning methodology previously discussed to develop a plan to support the commander's course of action (COA). To begin mission analysis and initial planning, the J6 staff must clearly understand the command authorities and relationships of the deploying joint force.

3.30 This phase of the operation normally will rely exclusively on the existing commercial, strategic, and tactical communications infrastructure.

3.31 **Deployment Activities**. As the OPORD is completed and published, CIS are expanded to provide improved information flow between the JTF Comd and any component commanders. As the system deploys, CIS assets are extended into the Joint Force Area of Operations (JFAO). These assets deploy incrementally in support of the build-up in the operational area.

3.32 The objective of deployment activities is continuous flow of information between commanders during the initial phases of the operation and establishment of CIS infrastructure to support follow-on operations. The primary focus of initial CIS is to support the on-scene commander.

3.33 Available lift assets deploy the initial CIS capability. The initial deployment package provides connectivity as well as the foundation on which to build the remainder of the network. CIS support must include reliable, redundant capabilities that ensure the commander is always able to maintain command and control (C2) of component and supporting forces.

Campaign Transition

3.34 **Changes to Force Structure**. As the balance between warfighting, stabilisation, and peace support activities changes, civil engagement increases. This may necessitate changes in force structure and tasks and affect the JTF Comd's information needs. Drawdown of forces associated with an improving security environment may offer the opportunity to commercialise and contractorise military CIS capability.

3.35 **Rotation of Forces.** Rotation of forces may entail changes to the CIS requirement. These can be initiated by the JTF Comd, HQJFNZ J6, or the JTF J6. This may require CIS planning to:

- capture new information exchange requirements (IER)
- redesign CIS solutions
- issue new directives, such as a revised joint communications-electronic operating instruction (JCEOI)
- manage changeover of personnel.

3.36 Rotation may provide the opportunity to increase contractorisation and commercialisation to release military CIS assets and provide an enduring solution. Continuity of CIS capability is enhanced by engaging incoming CIS staff officers as soon as practicable in the planning process, which develops their appreciation of how extant CIS contributes to the overall mission.

3.37 **Handover of Responsibility.** The JTF Comd may need to hand over to a host nation force or multinational follow-on force at the end of the campaign. Careful planning with the incoming nation of CIS staff ensures CIS capability is sustained during the transition.

3.38 **Recovery.** The recovery of forces from theatre involves significant logistic effort, changes to CIS capability, potential contractorisation or commercialisation, and drawdown or cessation of services. To ensure that CIS capability is maintained at the appropriate level throughout this process, The JTF J6 staff requires early and close engagement with the Joint Logistics (J4) staff fo gain full appreciation of the JTF Comd's recovery plan.

Multinational Force

3.39 Multinational forces (MNF) are classified as either coalition or combined[10]. The lead national force, as the framework nation, will appoint the Coalition Commander in coordination with respective national authorities of participating forces. The Coalition Commander is responsible for MNF operation at the strategic level and issues national strategic guidance to the Commander of the MNF. The Coalition Commander is responsible to the Lead National Authority for planning and directing operations at the operational level of command, and more specifically for:

- preparation of CIS policy, guidance, and requirements for the MNF Commander to operate within the CIS infrastructure deployed
- coordination of CIS releasability issues
- coordination of MNF activities with component forces
- liaising with Troop Contributing Countries and other organisations to initiate resolution of CIS interoperability issues
- providing connectivity to the MNF.

3.40 Participating nations' strategic-level military commanders are responsible for military coordination and providing support to the Coalition Commander and MNF Commander. The respective Chiefs of the MNF's contributing militaries are the national military points of contact for coordinating their military forces and support. This may involve arranging non-military support from their nations. They are responsible for:

- indicating CIS personnel, assets, and capabilities available to support the MNF
- providing CIS support requirements to the lead nation
- supporting CIS activities of the MNF with other national and component forces, and other appropriate entities
- preparing national CIS policy and guidance to enable subordinate forces to effectively operate within a multinational force CIS structure.

3.41 The lead nation for an operation needs to have the will, capability, competence, and influences to provide the essential elements of political consultation and military leadership to coordinate the planning, mounting, and execution of a multinational military operation. It provides unity of effort and acts as the single channel of strategic direction to military forces within the multinational effort based on collaboration and agreements with participating nations. For more information on MNF operations see the NZDF approved ADFP-00.3 *Multinational Operations* (2nd Edition) and its New Zealand Supplement.

Design and Engineering

3.42 CIS staffs are required to manage the NZDF's systems and networks for a variety of roles. Principles need to be considered, balanced, and incorporated into management techniques meeting commanders' requirements. It is important that CIS planners, particularly at the strategic and operational levels, understand current in-service CIS capabilities, systems, and networks available to support the NZDF's campaigns, operations, and activities. This ensures the most effective use of these capabilities in meeting the joint commander's intent.

3.43 Provision of CIS in operational and tactical environments is complex. Commonly recognised procedures for establishing, maintaining, and managing CIS in support of the NZDF's campaigns, operations, and activities are necessary to ensure effective provision of network and systems management and associated CIS services. The NZDF currently uses industry best practice methodologies to support its design and engineering efforts.

[10] NZDDP-3.0 *Campaigns and Operations* (2nd Edition)

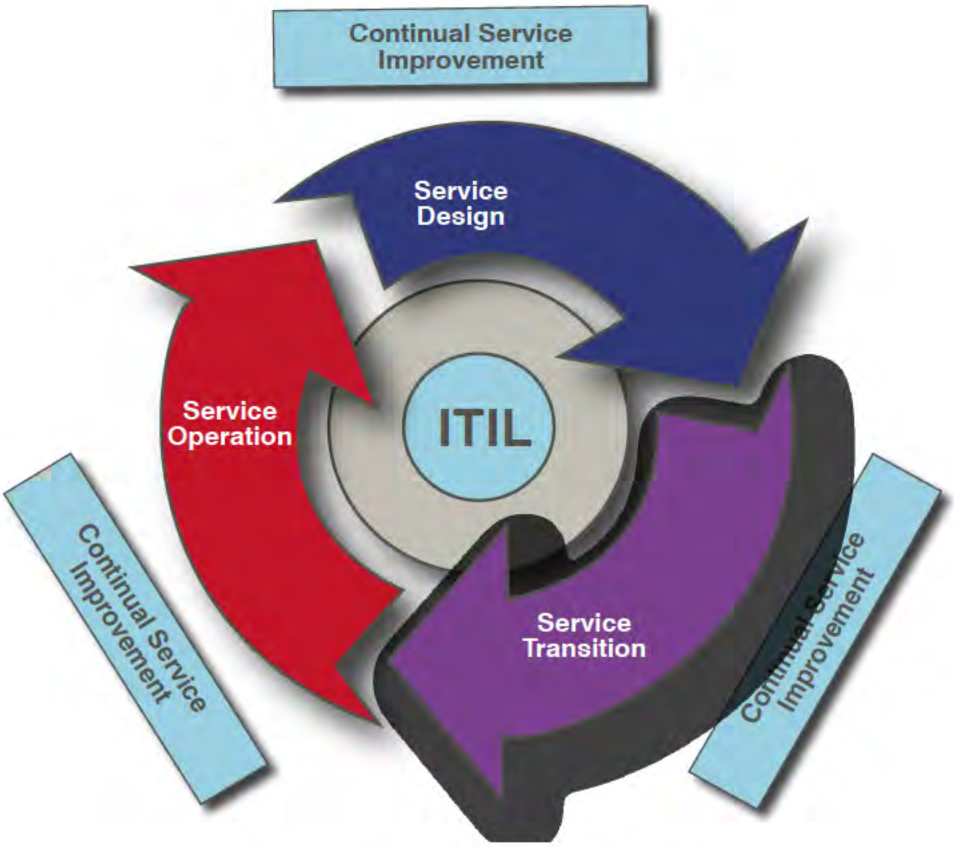

Continual Service Improvement
Service Design
Service Operation
ITIL
Service Transition
Continual Service Improvement
Continual Service Improvement

Figure 3-7: Service Management Cycle.

Service Management

3.44 Service Management is a general term referring to a strategic approach to designing, delivering, managing, and improving how information technology (IT) is used within an organisation. The goal of every IT Service Management framework is ensuring the right processes, people and technology are in place for its organization to meet its business goals

3.45 The NZDF has selected the Information Technology Infrastructure Library (ITIL®) framework to guide development of IT Service Management Processes. The ITIL framework considers IT Service Management in the context of the IT Service Lifecycle shown in Figure 3-7.

3.46 See the range of official AXELOS ITIL® framework documentation for more detailed information on the processes involved.

Design Principles

3.47 For CIS to efficiently support the NZDF's campaigns and operations, before and during each deployment planning and technical control staffs need to continuously consider and balance the fundamental CIS principles in Chapter 1 as design drivers.

- **Support to the Chain of Command.** CIS capabilities enable and support the passage of information between commanders at all levels. This is crucial for both situational awareness and giving and receiving orders. Most CIS acquisitions require long lead times, so alternative approaches may need to be considered, such as logistics pre-positioning, commercial support, and rapid acquisition. Communications planning staff must anticipate their commander's requirements, and maintenance staff need to establish mechanisms anticipating failures to prevent un-controlled outages.

- **Integration.** CIS and Services need to provide seamless connectivity, allowing data to be entered once but which is accessible by multiple systems as required.

- **Reliability.** To maximise the availablity of CIS equipment and software to its users, it needs to be reliable and easily maintained. Reliability refers to low mean times between failures; maintainability refers to modular construction of hardware and the 'reuse plug and play' approach to software writing.

- **Flexibility.** An adaptable approach is required for the continuum of operations. For equipment and system designs to meet capability requirements, they should be expandable, scalable, or both. This may involve such measures as easily configurable multiple communications modes, power output settings, power supplies, and antenna systems.

- **Survivability.** CIS equipment design and connectivity need to be robust and resistant to factors arising from the environments in which they may have to be operated: physical location (fixed or mobile), extremes of climate weather conditions, and the electromagnetic environment. Resistance to jamming, shock, vibration, temperature, corrosion, and dust should be factored into equipment specifications.

- **Mobility**. CIS need to be designed to support the mobility of the commander's headquarters, from static or defensive through to rapid or advance operations.

- **Security.** Systems should be designed and deployed to maximise all aspects of security including cyber, data, and information security. The confidentiality, integrity, availability, authenticity and non-repudiation of systems should be prioritised. Transmission systems can be secured by appropriate equipment design and emission control processes providing low probability of intercept.

- **Simplicity.** Systems need to have simple designs allowing ease of use and maintenance with minimum training. Force elements are encouraged to use organic, minimal, and essential communications to improve mobility, while maintaining redundancy for survivability.

- **Capacity.** The storage and bandwidth capacity of CIS should be sufficient to meet requirements and powerful enough to support the services within a JFAO and between JFAOs.

- **Quality.** Providing clear and concise documentation enables effective management, audit, and correction to achieve or exceed service standards.

- **Economy**. Although cost of resources should be considered, this needs to be balanced against the need to gain advantage over an adversary in order to achieve mission success. Commanders and CIS users need to be aware that bandwidth, spectrum, call connection times, and power must not be wasted, as with more tangible resources like personnel and materiel.

- **Interoperability**. Achieving acceptable levels of interoperability requires adhering to standards, such current Defence software standards, processes terminology, and commonality of equipment. Doing so ensures data can be passed as required without corruption or delay.

- **Anticipation of Requirements**. Some CIS require long lead times to ensure commercial support is provided or logistics prepositioning can occur. Planning staffs must anticipate requirements and maintenance staff should establish mechanisms to anticipate failures to prevent unplanned outages.

Key Term

Electromagnetic Spectrum

An electromagnetic spectrum (EMS) frequency, a band of frequencies, or a point on the radiofrequency part of the EMS used for radio communications. It is normally expressed in kilohertz (kHz) at and below 30 000 kHz and in megahertz (MHz) above this frequency.

3.48 **Sovereign and National Rights of Nations.** An overriding principle in the treaty establishing the International Telecommunications Union (ITU) is that nations retain sovereign rights over use of the radio frequency (RF) spectrum within their own territory and may modify the radio regulations (RR) for national purposes. They must, however, comply with the RRs for emissions that extend beyond national boundaries. Articles of the ITU Constitution relating to military use of the spectrum are regulated in New Zealand through the *Radio Communications Act* 1989 and the associated *New Zealand Radio Regulations* 2001. Military commanders need to be aware of their responsibilities with respect to these regulations.

3.49 **International Military Organisation.** New Zealand, along with Australia, Canada, United Kingdom, and United States, is a member of the Combined Communications-Electronics Board (CCEB). It is a combined military communication and electronic systems forum for coordinating any military CE matter referred by a member nation. National frequency managers of the CCEB countries meet – usually annually – to develop and establish combined RF management policies and procedures and to seek a common approach to items raised at the World Radiocommunications Conference (WRC). CCEB also issues publications relating to spectrum matters between member nations.

3.50 **National Administration.** The regulatory body for spectrum management in New Zealand is the Radio Spectrum Management Group (RSMG) of the Ministry of Business Innovation and Employment (MBIE). Within the framework of the ITU RR, RSMG allocates RF bands for use within New Zealand. These allocations closely follow the framework of allocations for ITU Region 3. However, there are a few differences in the New Zealand table of allocations where national considerations have dictated divergence from the Region 3 allocations. Some

Figure 3-8: Some radiofrequency is reserved for Defence purposes and the New Zealand Defence Force has been authorised to manage some of these bands without needing to consult with Radio Spectrum Management Group.

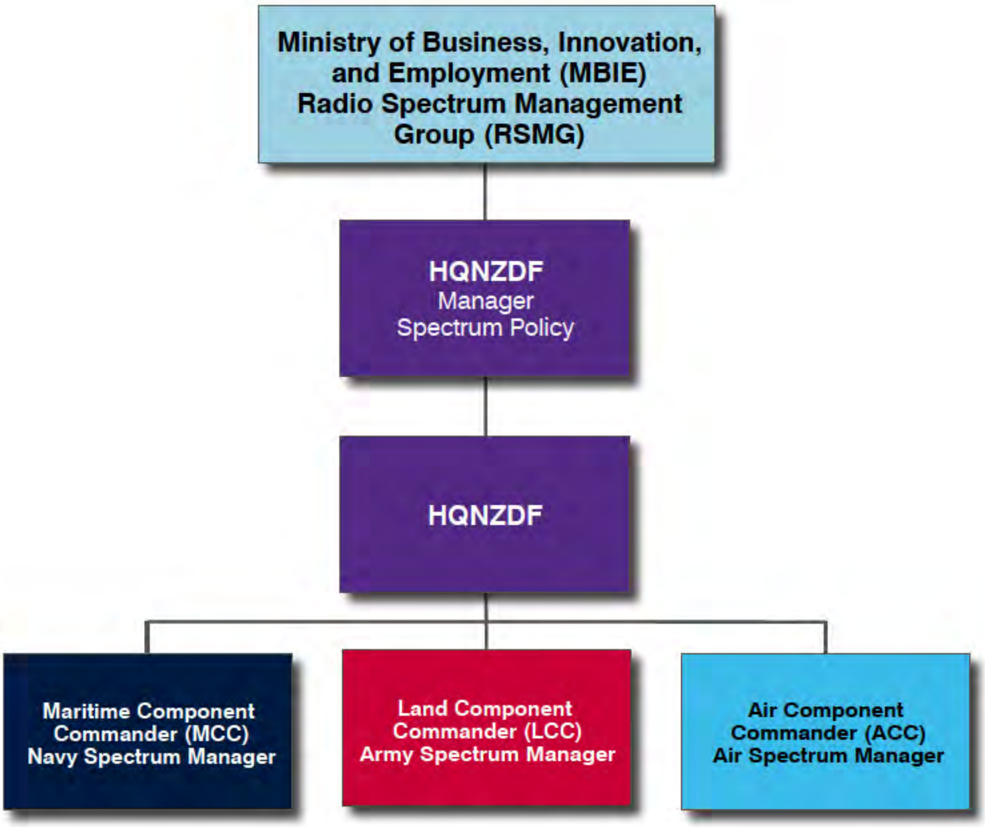

Ministry of Business, Innovation, and Employment (MBIE) Radio Spectrum Management Group (RSMG)
HQNZDF Manager Spectrum Policy
HQNZDF
Maritime Component Commander (MCC) Navy Spectrum Manager
Land Component Commander (LCC) Army Spectrum Manager
Air Component Commander (ACC) Air Spectrum Manager

Figure 3-9: The New Zealand Defence Force Spectrum Management Organisation.

bands are reserved principally for Defence purposes and the NZDF has been authorised to manage some of these bands without the need to consult with RSMG. The *Radiocommunications Act* 1989 requires the Crown, and hence the NZDF, to ensure that its use of the RF spectrum complies with the Act. Control of the spectrum by the NZDF is delegated by the CDF via the CCIS to the Spectrum Policy Manager (SPM) in accordance with NZDF policy. The SPM is responsible for the coordination and management of all matters relating to the NZDF's use of the RF spectrum. The management of the RF Spectrum has to comply with Defence Force Order (DFO) 101, Chapter 7 — *Radiofrequency Spectrum Management*.

Key Term

Frequency Assignment

The process of designating a radiofrequency for use at a specific station or by a specific military formation under specified conditions of operations.

New Zealand Defence Force Use of the Spectrum

3.51 The aim of military EMS management not just to assign frequencies. It also involves achieving an effective measure of control over the use of the EMS. While recognising the fundamental principle that all nations retain sovereign rights over the control of radio emissions within their territories, military operations sometimes result in these rights being disrupted or temporarily altered. The extent to which this is the case will depend on the intensity and scope of operations.

3.52 EMS management is concerned with all aspects of planning, coordinating, and managing the use of the EMS. Frequency management is generally accepted to be a subset of EMS management. Frequency managers plan, coordinate, and manage frequency assignment and use of specific frequencies within the EMS bands they are allocated.

3.53 To meet the needs of NZDF campaigns and operations, military EMS management systems must be able to deliver high degrees of:

- responsiveness, in terms of both speed and appropriateness of response
- flexibility in operating under unusual or unforeseen circumstances
- reliability.

3.54 RF planning is generally done to meet the needs of radio services within a geographic area, as based on the allocation tables in the RRs. In peacetime, it is normally developed from a communications plan or strategy in accordance with the National Frequency Allocation Tables. For operational deployments, the development of a Spectrum Management Plan can be complex; sufficient time must be allowed and advice should be sought early. Production of a plan should commence as soon as a requirement is identified and include the composition of the force (international and national involvement), locations, and size of the force elements. Operations rely on accurate spectrum related information; therefore, continuous collection, storage, and analysis of the data in a pre-planning phase can assist in developing the Spectrum Management Plan.

3.55 When conducting EMS management, it is important to take into account the electromagnetic compatibility effects created by imperfections in the design of emitters, which can cause co-site and far-site interference. These imperfections, such as spurious emissions and intermodulation effects, are the source of electromagnetic interference effects.

3.56 Knowledge of radio wave propagation theory is essential for creating of successful CIS and EMS use plans. In the case of a CIS plan, propagation calculations are necessary to guide the choice of the most suitable communications techniques and placement of radio and retransmission repeater antenna sites. In the case of EMS use plans, propagation calculations are necessary for maintaining protection when employing frequency reuse or other frequency sharing techniques. It is also used to select an appropriate operating frequency where propagation conditions vary with the frequency and length of the radio path, for instance from the daily variations of the ionosphere for high frequency radio.

Real-life Example

Spectrum: the Key to Radiocommunications

The value of radio for military and ship to shore use was recognised early in its development, and navies in a number of countries played an important part in its development. Early wireless experiments were in the medium frequency band from about 300 kHz to 3 MHz. As technology progressed, higher frequency bands came into use. With an increasing number of users and a greater range of frequencies, the control and regulation radio spectrum for its effective use and avoiding interference became a critical..

After Federation in Australia in 1901, the Postmaster-General's Department (PMG) became responsible for radio spectrum regulation, which continued until the start of World War I when, for security and strategic reasons, control of radio and the use of the spectrum came under the military. The Department of the Navy held this responsibility until it was handed back to the PMG until 1920. However, Navy retained the responsibility for spectrum management and frequency allocation in the military forces.

The range of frequencies in use had increased significantly by World War II, and there was much trouble caused by over crowding of the wave band; but there was little that any of the services could do to correct this because of the sheer number of wireless users. In New Zealand territory, frequencies for the AMF were allocated by the Department of Navy, which for Army requirements received advice from Land Force Headquarters Committee 'F'. All the fighting services, including American, had representatives on this committee, and the Department of Army's delegates were members of the SOinC's [Signals Officer-in-Chief's] staff. The basic problem was that the demand for frequencies exceeded the number available, so sharing between or within formations and services was necessary. Success under these conditions depended on geographic distances separating the users and sensible adjustment of power output. Other included wave propagation and ionospheric conditions, including sun spot activity predictions. Officers of the New Zealand Corps of Signals were active in these areas. They represented the Department of Army on the Radio Research Board, the New Zealand Radio Propagation Committee, and the Post War Frequency Allocation Sub-Committee of the Defence Communications Committee.

By the middle of 1945, wireless communications in the AMF were in three of the standard frequency bands: high, very high (VHF), and super high frequency (SHF). The range of 2 to 20 MHz was used for nearly all wireless sets; for smaller stations at divisional level, a frequency range of 2 to 8 MHz had been standardised, but it was planned to extend this to 12 allow more channels of 50 kHz. The VHF and SHF spectrums each had only one item of equipment in use at that time: the FC2 set, which operated between 35 and 40 MHz; and the Wireless Set Number 10, which had only two frequencies, 4400 and 4760 MHz. In the post-war period responsibility for spectrum management passed to the Joint Communications Board and eventually to the current Defence Spectrum Office.

GLOSSARY

Terms and Definitions

Authentication (ADDP-6.0)

A security measure designed to protect a communication system/network against fraudulent transmissions.

Chief Technology Officer (NZDF)

An appointment in the CIS Branch which is responsible for the technical control of Defence's Information Environment on behalf of the CCIS.

Coalition (JP 1-02)

An ad hoc arrangement between two or more nations for common action.

Code (ADDP-6.0)

A system of communication in which arbitrary groups of symbols represent units of plain text of varying length. Codes may:

- convert information into a form suitable for communication and/or encryption, such as Morse code;
- reduce the length of time necessary to transmit information, such as brevity code to reduce long sentences; or
- provide a degree of security for the information being transmitted, such as cryptographic code.

Communication System (ADDP-6.0)

An assembly of equipment, procedures and personnel organised to accomplish information transfer functions between its users. It includes transmission, switching and user terminal systems, and storage or processing functions in support of information transfer, ie communication.

Communication and Information System (ADDP-6.0)

An assembly of equipment, procedures, and personnel organised to accomplish data transfer and information processing functions. Communication and Information Systems is also the name of a Defence doctrine series and a group of Defence Instructions.

Communications Centre (COMMCEN)

An agency/unit charged with the responsibility for receipt, transmission and delivery of messages.

Note: It normally includes a message centre with cryptographic security, transmitting and receiving facilities.

Communications Centre (ADDP-6.0)

An agency/unit charged with the responsibility for receipt, transmission and delivery of messages. Note: It normally includes a message centre with cryptographic security, transmitting and receiving facilities.

Communications Channel (ADDP-6.0)

A route on a communications circuit to transfer data from a sender to a receiver. More than one independent channel may be carried on a circuit by frequency, time or code division multiplexing.

Communications Circuit (ADDP-6.0)

An electronic path via line or radio, between two or more terminals, capable of providing a number of communications channels.

Communications-electronics (ADDP-6.0)

The specialised field concerned with electronic devices and systems used for the acquisition, processing storage, display, analysis, protection and transfer of data/information.

Communications-electronics Systems Interoperability (ADDP-6.0)

The condition achieved between communications-electronics systems or equipment when data, information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases, such as Level 3 of the Levels of Information Systems Interoperability Maturity Model.

Communication and Information Systems Domain (ADDP-6.0)

An information system or subsystems that are controlled by a single management authority, and all components of the information system are subject to a single, system-specific security plan.

Communications Interface (ADDP-6.0)

A boundary or point common to two or more systems or other entities across which useful information/data flow takes place. Useful information flow requires the specification of the interconnection of the system elements that enable them to interoperate.

Communications Link (ADDP-6.0)

A single connection by any means that carries, passes or transmits data of any type (digital or analogue) between two network or terminal devices.

Communications Monitoring (ADDP-6.0)

The act of listening to, reviewing and/or recording one's own or by special agreement, other friendly forces' communications for the purpose of maintaining and improving standards of communications security or efficiency, or for reference.

Communications Network (ADDP-6.0)

A combination of one or more communications links or systems interconnected by network devices (nodes, switches, routers, regenerative repeaters, etc) to from a mesh/network that passes/transmits data of any type (digital or analogue) between two or more devices.

Communications Security (ADDP-6.0)

The security measures taken to deny unauthorised personnel information derived from telecommunications and to ensure the authenticity of such telecommunications. Note: It includes the use of cryptographic security, transmission security, emanations security, personnel and physical security measures to protect communications from unauthorised interception and exploitation.

Communications Terminal (ADDP-6.0)

A communications facility which constitutes a point of origin and/or termination of a circuit or channel.

Computer Security (ADDP-6.0)

Specialised measures developed to protect information processed or stored within computing systems.

Cryptography (ADDP-6.0)

The art or science concerning the principles, means and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Data (ADDP-6.0)

Representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human or automated means.

Note: It includes any representations such as characters or analogue quantities to which meaning is, or might be assigned. It comprises some sort of unprocessed quantities, eg numbers, text strings, readings from sensors or other instruments, whereas information comprises quantities derived from these by some process, ie through calculators, inferences, transformations, etc.

Defence Architecture Framework (ADDP-6.0)

A framework using the New Zealand Defence methodology for the production of Defence Enterprise Architecture data and products.

Defence Information Environment (adapted from ADDP-6.0)

A capability that consists of the data/information used by Defence for business and military operations and the means by which it is created, managed, manipulated, stored and disseminated in and across all security domains.

Note: It includes all Defence assets, personnel and capabilities involved in the exchange of data such as fixed, mobile, standalone and deployable networks, user devices and their support services, including Defence services hosted on external servers.

Defence Information Exchange System (NZDF)

A computer network of the Defence Information Environment for disseminating information classified up to and including RESTRICTED.

Defensive Cyberspace Operations (JP-3-12R)

Passive and active cyberspace operations intended to preserve the ability to utilise friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.

Electronic Information Exchange (ADDP-6.0)

The connection of two or more computers in order to share information, including the point-to-point connection of two computers, connection to a local area network, a wide area network or the Internet for the sharing or manipulation of electronically stored information.

Electronic Warfare (ADDP-3.5)

Military action to exploit the electromagnetic spectrum (EMS) which encompasses the interception and identification of electromagnetic emissions, the employment of electromagnetic energy, including directed energy, to reduce or prevent hostile use of the EMS and actions to ensure its effective use by friendly forces.

Electromagnetic Spectrum (ADFP 04.1.1)

The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands

Emanation Security (ADDP-3.5)

The countermeasure employed to reduce classified emanations from a facility and its systems to an acceptable level. Emanations can be in the form of radiofrequency energy, sound waves or optical signals.

Emission Control (ADDP-3.5)

Measures taken to minimise the use of electronic emissions by friendly forces to prevent premature disclosure of the presence and composition of a force.

Exercise (ADDP-7.0)

A military manoeuvre or simulated wartime operation involving planning, preparation and execution. It is carried out for the purpose of training and evaluation. It may be a combined, unified, joint or single service exercise depending on participating organisations.

Frequency (ADDP-6.0)

The number of recurrences of a periodic phenomenon in a unit of time. In specifying an electrical or electromagnetic spectrum frequency, the unit of time is the second, eg the frequency is 15 000 cycles per second or 15 kilohertz.

Frequency Assignment (ADDP-6.0)

The process of designating a radiofrequency for use at a specific station or by a specific military formation under specified conditions of operations.

Functional Planning (NZDF)

Functional planning is the integration of the aims and intentions of the commander into CIS plans, orders, and control procedures.

Information (ADDP-6.0)

Data in context, including documents and papers; electronic data; the software or systems and networks on which the information is stored, processed or communicated; intellectual information acquired by individuals; and physical items from which information regarding design, components or use could be derived.

Information and Communications Technology (ADDP-6.0)

The applied science and engineering aspects related to the creation, manipulation, presentation, dissemination, etc of data for the communication of information between users.

Information Assurance (JP 1-02)

Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation.

Information Exchange (ADDP-6.0)

The formal or informal transmission of information from, to or within an information environment. It can be conducted using electronic or physical means, in fixed or deployed environments and across all security domains.

Information Network (ADDP-6.0)

A combination of one or more communications links or systems interconnected by one or more network devices (nodes, switches, routers, regenerative repeaters, etc) to form a mesh/network that passes/transmits information between two or more user information devices (computers, radios, telephones, hand-held data terminals, etc) or systems.

Information Operations (NZDDP-3.0)

The coordination of information effects to influence the decision making and actions of a target audience and to protect and enhance our own decision making and actions in support of national interests.

Information Security (JP 1-02)

The protection of information and information systems against unauthorised access or modification of information, whether in storage, processing, or transit, and against denial of service to authorised users.

Information System (ADDP-6.0)

An assembly of equipment, procedures and personnel organised to accomplish information processing functions. It includes software, computers, communications infrastructure and other devices designed for the collection, disposition, dissemination, maintenance, processing, sharing, storage, transfer and use of information.

International Telecommunication Union (ADDP-6.0)

The United Nations (UN) agency responsible to maintain and extend international cooperation between all UN members for the improvement and rational use of telecommunication of all kinds.

Interoperability (NZDDP-D)

The ability of systems, units or forces to provide services to, and accept services from, other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.

Intrusion (ADDP-6.0)

The unauthorised entry into a communication and/or information system or network, to create confusion and/or inject false information.

Joint (NZDDP-D)

Connotes activities, operations, organisations, etc in which elements of more than one Service of the same nation participate.

Intrusion Detection (ADFP-6.0.3)

Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.

Joint Communications (ADDP-6.0)

The common use of communications facilities by two or more Services of the same nation.

Joint Force (NZDDP-D)

A force composed of elements of the Navy, Army and Air Force, or two or more of these Services, operating under a single commander.

Joint Operations Planning Process (NZDDP-5.0)

A four-step assumption-based planning process that assists the commander and staff to reach a decision. Note: The four steps of the Joint Operations Planning Process are: preliminary scoping, Joint Intelligence Preparation of the Operational Environment, Joint Military Appreciation Process, and plan development and execution.

Levels of Information Systems Interoperability Maturity Model (ADDP-6.0)

A methodology for measuring and reporting the target and achieved interoperability of communication and information systems within an information environment.

Link (ADDP-6.0)

The communications facilities between two points. In maritime and Air usage, the word is invariably associated with automatic data transfer over a tactical data link.

Maintenance (ADDP-4.0)

All actions taken to retain equipment in or to restore it to a specified condition, including inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation.

All supply and repair action taken to keep a force in condition to carry out its mission.

The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or other real property) in such condition that it may be continuously utilised, at its original or designed capacity and efficiency, for its intended purpose.

Mission Analysis (JDP 0-0.1)

A logical process for extracting and deducing from a superior's orders the tasks necessary to fulfil a mission.

Multinational (AAP-6)

Adjective used to describe activities, operations, and organisations in which elements of more than one nation participate.

National Security (ADFP-04.1.1)

The ability to preserve the nation's physical integrity and territory; to maintain economic relations with the rest of the world on reasonable terms; to protect its nature, institutions, and governance from disruption from outside; and to control its borders.

Network Management Systems (NZDF)

The set of hardware and or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework

Net (ADDP-6.0)

An organisation of stations capable of direct communication on a common channel or electromagnetic spectrum frequency.

Radiofrequency (ADDP-6.0)

An electromagnetic spectrum (EMS) frequency, a band of frequencies, or a point on the radiofrequency part of the EMS used for radio communications. It is normally expressed in kilohertz (kHz) at and below 30 000 kHz and in megahertz (MHz) above this frequency.

Radio Relay (ADDP-6.0)

The reception and retransmission by a radio station of signals received from another station or from the line portion of an integrated line and radio system, for the purpose of increasing the range, flexibility and security of a line-of-sight communications bearer.

Radio Wave Propagation Theory (Institute of Electrical and Electronic Engineers)

The theory that describes the behaviour of radio waves when they are transmitted or propagated from one point on the Earth to another, or into various parts of the atmosphere.

Rules of Engagement (NZDDP-06.1)

Directives issued by a competent military authority that specify the circumstances and limitations under which forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE.

Secure Wide Area Network (NZDF)

SWAN is a computer network of the Defence Information Environment for disseminating information classified up to and including SECRET.

Security Domain (NZISM)

A system or collection of systems operating under a security policy that defines the classification and releasability of the information processed within the domain. It can be exhibited as a classification, a community of interest or reliability within a certain classification

Spectrum Management (JP -6.0)

Planning coordination and managing joint use of the electromagnetic spectrum through operational, engineering and administrative procedures. The objective of spectrum management using spectrum related information is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

Synchronisation (JDP 0-01.1)

The focusing of resources and activities to produce maximum combat power at the decisive time.

Technical Planning (NZDF)

Technical planning is the integration of those CIS plans, orders, and control procedures into supporting technical plans, directives, databases, and control systems.

TEMPEST (ADDP-6.0)

A codeword referring to the investigation, study and control of compromising emanations from information processing equipment.

Threat (JDP-0.01)

The probability or likelihood of an attack or undesirable event taking place. Threat includes such factors as capability, resources and intention and probabilities.

Videoconference (ADDP-6.0)

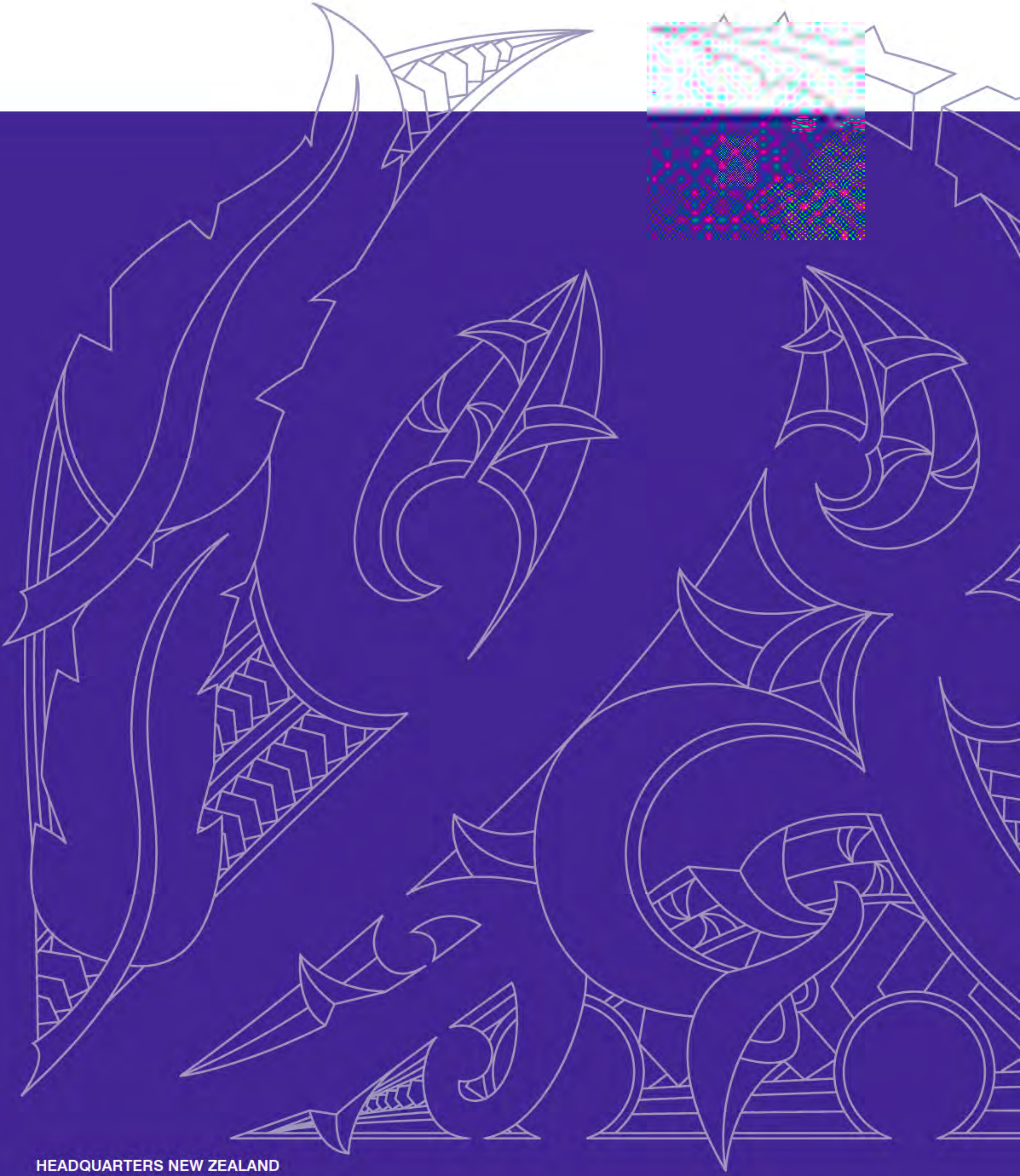
The transmission and reception between two or more parties of real- time audio-visual information.

Acronyms and Abbreviations

ABCANZ	American, British, Canadian, Australian, New Zealand Armies Program
AC CAP	Assistant Chief Capability
ACP	Allied Communications Publication
ADDP	Australian Defence Doctrine Publication
ADF	Australian Defence Force
ADFP	Australian Defence Force Publication
AMSG	Allied Military Standards General (publication)
AO	area of operations
AoG	All-of-Government
ASIC	Air and Space Interoperability Council
AUSCANZUKAS	Maritime Information Warfare Organisation
BDE	Brigade
C2	Command And Control
C4	Command, Control, Communications and Computers
CAN	Canada (country code)
CCEB	Combined Communications-Electronics Board
CCG	Communications Control Group
CCIS	Chief Communication and Information Services
CDF	Chief of the Defence Force
CDSC	Commander Defence Strategic Communications
CIS	Communication and Information System(S)
CIS Branch	Communications and Information Systems Branch
CMG	Communications Management Group
CNE	Computer Network Exploitation
CNR	Combat Net Radio
CNR	Combat Net Radio
CNSSI	Committee on National Security Systems Instructions
COMJFNZ	Commander Joint Forces New Zealand
COA	Course of Action
COMMCEN	Communications Centre
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	Concept of Operations
CPG	Commander's Planning Group
CRYPTOSEC	Cryptographic Security CSS Command Support System
CTO	Chief Technology Officer
DCB	Defence Computing Bureau
DEA	Defence Enterprise Architecture
DFO	Defence Force Order
DCO	Defensive Cyberspace Operations
DEFWAN	Defence Wide Area Network
DIE	Defence Information Environment
DIXS	Defence Information Exchange System
DNOC	Defence Network Operation Centre
EIE	Electronic Information Exchange
EMCON	Emission Control
EMS	Electromagnetic Spectrum
EMSEC	Emanation Security
EPSI	Enterprise Prime System Integrator
ERP	Enterprise Resource Programme
FE	Force Element
FIC	Fundamental Input To Capability
FM	Frequency Modulation
GCIO	Government Chief Information Officer
GCSB	Government Communications Security Bureau
HF	High Frequency
HJCC	Head Joint Capability Coordination
HQ	Headquarters
HQJJFZ	Headquarters Joint Forces New Zealand
IA	Information Assurance
ICT	Information And Communications Technology
IDA	Integrated Defence Architecture
IER	Information Exchange Requirements
INFOSEC	Information Security
IO	Information Operations
IRC	Information Related Capabilities

IS	Information System
ITIL®	Information Technology Infrastructure Library
ITU	International Telecommunication Union
J4	Joint Logictics
J6	Joint Comunications and Information Systems
JCA	Joint Capability Authority
JCCC	Joint Capability Coordination Committee
JCEOI	Joint Communications-electronic Operating Instruction
JDN	Joint Data Network
JFAO	Joint Force Area of Operations
JFCCO	Joint Force Chief Communications Officer
JMAP	Joint Military Appreciation Process
JPG	Joint Planning Group
JTF	Joint Task Force
LAN	Local Area Network
MA	Mission Analysis
MBIE	Ministry of Business, Innovations and Employment
MIS	management information system
MNF	multinational force
MOD	Ministry of Defence
M212	Maritime Multi-National Information Systems Interoperability board
NCG	Nodal Control Group
NCMM	National Crisis Management Machinery
NMCC	National Maritime Coordination Centre
NZDDP Publication	New Zealand Defence Doctrine
NZDF	New Zealand Defence Force
NZDFDA	New Zealand Defence Force Distribution Authority
NZDFP	New Zealand Defence Force Publication
NZISM	New Zealand Information Security Manual
OGA	Other Government Agency
OPINST	Operation Instruction
OPORD	Operation Order
OPSEC	Operations Security
PLANO	Planning Order
QCJWC	Quinquiparate Combined Joint Warfare Conference
Radhaz	Radiation Hazard
RF	Radiofrequency
RR	Radio Regulation
RSMG	Radio Spectrum Management Group
SF	Special Forces
SHF	Super High Frequency
SIE	Secret Information Environment
SPM	Spectrum Policy Manager
SWAN	Secure Wide Area Network
TLS	Through Life Support
TOC	Tactical Operations Centre
TRANSEC	Transmission Security
TTCP	The Technical Cooperation Programme
UHF	Ultra High Frequency
UNMO	United Nations Military Observer
USA	United States (country code)
VA	Vulnerability Analysis
VCDF	Vice Chief of the Defence Force
VHF	Very High Frequency
WNGO	Warning Order
WRC	World Radiocommunication Conference

INDEX



**HEADQUARTERS NEW ZEALAND
DEFENCE FORCE 2016**
www.nzdf.mil.nz