Australian Defence Doctrine Publication (ADDP) 3.13—*Information Activities*, edition 3, is issued for use by the Australian Defence Force and is effective forthwith. This publication supersedes ADDP 3.13 edition 2.

D.J. HURLEY, AC, DSC
General
Chief of the Defence Force
Department of Defence
CANBERRA ACT 2600

6 Nov 2013
PREFACE

1. Australian Defence Doctrine Publications (ADDPs) and Australian Defence Force Publications (ADFPs) are authorised joint doctrine for the guidance of ADF operations. ADDPs are pitched at the philosophical and high-application level and ADFPs at the application and procedural level. Policy is prescriptive as represented by Defence Instructions, and has legal standing. Doctrine is not policy and does not have legal standing; however, it provides authoritative and proven guidance, which can be adapted to suit each unique situation.

2. The content of this publication has been derived from general principles and doctrine contained in other relevant ADDPs, Defence Instructions and allied publications and agreements. Every opportunity should be taken by users of this publication to examine its contents, applicability and currency. If deficiencies or errors are found, amendment action should be taken. The Joint Doctrine Centre (JDC) invites assistance, from whatever source, to improve this publication.

3. **Aim.** The aim of ADDP 3.13—*Information Activities* is to provide guidance for the planning and conduct of Information Activities in the joint and multinational environments.

4. **Level.** This publication is for use by commanders and staffs in all headquarters and units and all Defence training organisations. This publication informs a wider audience of the conduct of information activities operational planning, command and coordination as part of ADF campaigns and operations.

5. **Scope.** This publication provides philosophical and application level doctrine on information activities. It describes the nature and scope of information activities. Information activities are defined as the integration, synchronisation and coordination of two or more Information-related capabilities (IRC) that generate and sustain a targeted information advantage. Defence conducts information activities at all levels in a whole-of-government context consistent with Australian Government guidance. Information activities provide a mechanism via which the will, understanding and capability of a target audience can be affected at all military levels to the advantage of national interests.
6. ADDP 3.13 edition 3 contains a number of changes from edition 2 with regard to the publication’s structure and focus. The significant changes and inclusions are:

- Introduction of new terminology and definition changes, for example Information activities, information related capabilities and target audience.

- Realignment of planning to reflect the changes in ADDP 5.0—Joint Planning; and

- More information on assessment.

ADDP 3.13—Information Activities needs to be viewed within the total context of warfighting. To this end, additional recommended reading is:

- ADDP-D—Foundations of Australian Military Doctrine;

- ADDP 3.0—Campaigns and Operations;

- ADDP 5.0—Joint Planning;

- ADFP 3.13.1—Information Operations Procedures; and

- ADDP 3.14—Joint Targeting
AMENDMENTS

Proposals for amendment of ADDP 3.13 may be sent to:

SO1 Joint Doctrine
Joint Doctrine Centre
Building 500
RAAF Base
WILLIAMTOWN NSW 2314

WLMJDCSO1JointDoctrine@defence.gov.au

<table>
<thead>
<tr>
<th>Amendment</th>
<th>Effected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Date</td>
</tr>
<tr>
<td>Signature</td>
<td>Date</td>
</tr>
</tbody>
</table>

DOCTRINE PUBLICATION HIERARCHY

The hierarchy of ADDPs and ADFPs, and the latest electronic version of all ADDPs and ADFPs, are available on:

Defence Restricted Network Joint Doctrine Library

and

Defence Secret Network Joint Doctrine Library
(http://web.wlm.nnw.dsn.defence.mil.au/dfwc/)

Selected unclassified ADDPs and ADFPs have been released to the public and are available on the Defence Force Warfare Centre Doctrine Centre (http://www.defence.gov.au/dfwc/doctrine.html).
CONTENTS

Authorisation i
Preface iii
Amendment Certificate v
List of Figures xi

CHAPTER 1 FUNDAMENTALS

INTRODUCTION

DEFENCE AND INFORMATION ACTIVITIES
Information activities 1-6
Shaping and influencing 1-10
Information operations 1-12
Inform and influence actions 1-15
Information activities within the OE 1-16
Understanding 1-22
Will 1-23
Capability 1-24

EFFECTIVE COMMUNICATION
Audience 1-26
Target audiences 1-28
Narrative 1-29
Effects 1-32

INFORMATION-RELATED CAPABILITIES
Civil-military cooperation 1-35
Computer network operations 1-36
Counterintelligence 1-37
Deception 1-38
Destruction 1-39
Electronic warfare 1-40
Evidentiary/operational imagery 1-41
Information assurance 1-42
Key leader engagement 1-43
Military networking 1-44
Military public affairs 1-45
Operations security 1-46
Presence, posture and profile 1-47
CHAPTER 2 RESPONSIBILITIES AND ORGANISATION

INTRODUCTION

RESPONSIBILITIES
Chief of the Defence Force and Secretary 2-2
Military strategic commitments division 2-3
Strategy Executive 2-4
Vice Chief of the Defence Force Group 2-5
Joint Operations Command 2-6
Service Chiefs 2-8
Intelligence and Security Group 2-9
Chief Information Officer’s Group 2-11
Joint task force headquarters 2-12

ORGANISATION AND PROCESS
Strategic Effects Targeting Board 2-14
Operational Targeting Board 2-16
Defence International Engagement Group 2-18

CHAPTER 3 PLANNING

INTRODUCTION
Overview 3-1
Provision of strategic communication guidance 3-5

CONSIDERATIONS
Assessment 3.9
Lead times 3.12
Coordination and sequencing 3.13
Releasability 3.15
Political issues 3.16
Funding 3.17
Multinational 3.18

Annex:
A. Strategic Communication Guidance template
CHAPTER 4  EXECUTION

INTRODUCTION

COORDINATION

ASSESSMENT
Measure of performance  4-9
Measure of effectiveness  4-10
Measure of impact  4-11

REPORTING  4-5

Glossary

Acronyms and Abbreviations
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Military contribution to strategic communication</td>
<td>1-3</td>
</tr>
<tr>
<td>1-2</td>
<td>Planning and phases of military effort</td>
<td>1-4</td>
</tr>
<tr>
<td>1-3</td>
<td>Relationship between domains</td>
<td>1-6</td>
</tr>
<tr>
<td>2-1</td>
<td>Coordination of information activities</td>
<td>2-5</td>
</tr>
</tbody>
</table>
CHAPTER 1
INTRODUCTION AND OVERVIEW

Executive summary
This chapter introduces information activities, and how they support strategic communication.

- Strategic communication focuses whole-of-government efforts to direct and integrate information in support of the national interest.
- Information activities are the conduct of military activities in support of strategic communication from the military strategic to the tactical level.
- Information operations are the operational level planning and execution of information activities and operate on the will, understanding and capability of an intended audience.

You can win the battle and lose the war if you don’t handle the story right.

Colin Powell

Superiority in the physical environment is of little value unless it can be translated into an advantage in the information environment.

Professor Sir Lawrence Freedman, The Transformation of Strategic Affairs

DEFENCE AND INFORMATION ACTIVITIES

1.1 Defence functions as both a government department and as a military strategic headquarters, coordinating the use of the military component of national power. In undertaking either function, Defence needs to ensure the alignment of words and deeds.

1.2 Defence requires awareness and understanding of the whole-of-government (WoG) perspective to ensure an aligned and unified
approach with other government departments. The conduct of domestic and international operations is Defence's raison d'être—the use of military power to further national interests. Information activities (Info Actys) must be integrated into both the strategy and planning for operations. Defence uses a coordinated, planned approach to delivering Info Actys on operations.

1.3 Australian national interests may require the ability to exert strategic influence, the ability to exert policy influence underpinned by military power, through the use of national power. Effective shaping requires a deliberately planned series of actions that affects the intended audience. This takes place in an ambiguous and complex global context.

Strategic communication focuses government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favourable to the advancement of government interests, policies and objectives through the use of coordinated programs, plans, themes, messages and products synchronised with the actions of all instruments of national power.

1.4 Within this complex environment, strategic communication (StratCom) aims to influence key actors in ways that are advantageous to Australian national interests. StratCom is a whole-of-government (WoG) effort that uses public affairs, public diplomacy and military information activities to support national goals.

1.5 StratCom sets the narrative upon which other information-related activities build to generate planned effects. StratCom endeavours to concisely articulate the ‘why’ of Australian activity in which the Australian Defence Force (ADF) is participating. StratCom is the process of synchronising and coordinating communication efforts concerning Defence’s people, capabilities, infrastructure and operations to achieve desired ends aligned with national goals. The significant output of StratCom is a coordinated communication strategy including the strategic narrative. StratCom encompasses a range of military and non-military activities as shown in figure 1-1.
Figure 1–1: Military contribution to strategic communication

Information activities

1.6 Info Actys is the integration, synchronisation and coordination of two or more information-related capabilities (IRC) that generate and sustain a targeted information advantage. An information advantage is a favourable information situation relative to a group, organisation or adversary.

1.7 Info Actys includes both influencing the decision making of actors while protecting our own information and decision making. Info Actys includes:

- shaping and influencing (at the strategic level);
- information operations (at the operational level); and
- inform and influence actions (at the tactical level).

1.8 IRCs are tools, capabilities or processes, which can have effects of a physical, functional, temporal or psychological nature upon target systems and/or target audiences (an individual group selected for influence). IRCs are detailed in paras 1.28 -1.45

1.9 INFO ACTYS is applicable from Phase 0 to Phase V as shown in figure 1-2 and must be planned accordingly.
Figure 1–2: Planning and phases of military effort

Shaping and influencing

1.10 Shaping and influencing (S&I) is the coordination and synchronisation of information activities at the military strategic level, with WoG input, to influence the decision making and actions of a target audience and to protect and enhance our decision making and actions in support of national interests.

1.11 S&I plans describe the mid-to-long-term concept for implementing military activities in support of Australia’s national interests. S&I plans are developed and authorised through the Strategic Effects Targeting Board (SETB). S&I activities may have enduring reach and may not be constrained by operational activities.

Information operations

1.12 Information operations (IO) is the operational level planning for and execution of coordinated, synchronised and integrated lethal and non-lethal actions against the capability, will and understanding of target systems and/or target audiences. IO is focused on impacting the target audience decision making, while protecting and enhancing our own. IO is an integral part of an operational plan and supports the commander’s decision making and mission accomplishment.
1.13 IO planning and execution is conducted at Headquarters Joint Operations Command (HQJOC). Commander Joint Operations (CJOPS) may delegate responsibility for the planning and execution of IO to subordinate JTF commanders.

1.14 IO seek to place an assigned ADF element (nominally an Australian-led Joint Task Force (JTF), the Australian component of a Combined Task Force or the ADF element supporting an interagency task force) into a position of advantage within the operational environment (OE) to affect the capability, will and/or understanding of adversaries, potential adversaries and partners while protecting our own.

Inform and influence actions

1.15 Inform and influence actions (IIA) are the coordinated and synchronised execution of tactical tasks by assigned information related capabilities (IRC) during operations. IIA generate and sustain changes in the operating environment to place friendly forces in a position of advantage. IIA are broadly categorised as command and information protection, counter-command and influence activities executed to meet IO objectives.

Information activities within the operational environment

1.16 Correctly understanding the domains and their associated systems, components and audiences is crucial to effectively executing information activities. Contextual framing of the OE is achieved by appropriately analysing entities in the OE through their cognitive, physical and informational systems and understanding the relationships between each. This analysis, through an information lens, is achieved through focussed target systems analysis and target audience analysis. The OE is a complex system of systems. Generating effects in these systems requires established baselines upon which to base analysis.

1.17 A domain within the OE is a medium with discrete characteristics in which, or through which, military activity takes place. The physical domain is where military operations take place whether on land or sea or in space or the air. The human domain is where decisions are made, individually or collectively.

1.18 The information domain encompasses all information and related infrastructure that may influence operations. The information
domain interacts with the physical and human domains as shown in figure 1-3.

Figure 1–3: Relationship between domains

1.19 Info Actys seeks to place civilian and military elements into a position of advantage in the information domain in order to affect the understanding, will and or capability of target audiences. Producing the desired actions from target audiences requires understanding, the will to decide on action, and the capability to deliver the action. The absence in the target audience of any of these components reduces effectiveness.

1.20 Decisions taken by commanders are a function of understanding, will and capability. To generate effective actions the decision maker, whether friendly, neutral or adversarial, requires an understanding of the situation, have the will to decide and the capability to act. The effectiveness of the decision maker and the ability to act in the preferred way will be affected by the absence of understanding, will or capability. Friendly IO/Info Actys will be
designed to influence the adversary’s will, counter adversary capability by affecting understanding and will, and decrease adversary understanding by protecting friendly information.

1.21 Info Actys at all levels focuses directly on using the information domain to affect the decision maker’s capacity to produce effective decisions. While the desired effect is target or audience dependent, Info Actys aims at the functions of understanding, will and capability of the target audience whether adversaries, friends and neutral, or uncommitted actors.

1.22 Understanding. Info Actys will seek to affect the information available to decision makers in order to affect understanding (and thereby perception) of a given situation. Activity that safeguards friendly information seeks to affect adversary understanding. Activities to target understanding include: operations security (OPSEC), information security, counterintelligence (CI), intelligence, surveillance, and reconnaissance (ISR) and countering adversary ISR.

1.23 Will. Within national direction, Info Actys is aimed at all decision makers at any level capable of influencing the situation whether adversary, friendly or uncommitted. This may be achieved by the promotion of identified themes to approved audiences through verbal and non-verbal massages. It seeks to pre-dispose, persuade, convince, deter, disrupt, compel or coerce audiences to adopt of reinforce a particular course of action (COA) or to assist, encourage and reassure those that are following a desired COA. It can capitalise on, increase the effectiveness of, or in some cases remove the need for, attacks on capability. It focuses the impact of existing actions against capability to ensure that their effect in will is coherent and supports the commander’s objectives.

1.24 Capability. Within rules of engagement and legal constraints, IO will seek to affect those capabilities, such as the adversary’s command, control, communications, computers and intelligence (C4I) infrastructure that enable a decision maker to understand a situation and apply his will. It concentrates on undermining the adversary’s ability to develop, disseminate and execute sound decisions. It attacks capability but achieves an impact on will, understanding and capability.
EFFECTIVE COMMUNICATION

1.25 Communication may be viewed as an information exchange between two or more entities. The process of information exchange, between message transmission and message reception, is open to uncertainty, influence, misinterpretation and misunderstanding. The key aspect of communication from the sender’s perspective is realising how transmitted information is perceived or understood by the audience. Therefore, a detailed understanding of the potential audience is required to conduct effective Info Actys.

Audience

1.26 Commanders simultaneously contend with multiple audiences and voices from in-theatre actors such as non-governmental organisations and local chiefs to domestic players such as the general public and government. Audiences can have a significant impact on operations for example, the public denouncement and peace marches of the Vietnam War which contributed to the withdrawal of Australian force elements. Audiences can be engaged through public demonstrations, lobbying through online campaigns and other mechanisms.

1.27 Understanding the nuances of the various audiences – their context, culture, their environment, language, history, objectives, and needs; enables narratives, themes and messages to create an effective dialogue and get results.

1.28 Target audiences. A target audience is an individual or group selected for influence. Information on target audience analysis is provided in ADFP 3.13.1—Information Operations Procedure.

Narrative

1.29 A narrative is a compelling story line capable of explaining events convincingly and from which inferences can be drawn. Narratives provide a vehicle for conveying ideas and supporting collective and common understanding.
Examples of strategic narratives

The strategic narrative of the Cold War was that the United States was the leader of the free world against the communist world; that we would invest in containing the Soviet Union and limiting its expansion while building a dynamic economy and as just, and prosperous a society as possible.

To support global security and Australian national security: Australia is committed to countering international terrorism and supporting efforts to prevent Afghanistan from ever again being used as a safe haven and training ground for global terrorism, including attacks on Australians in our own region and beyond.

1.30 A narrative should be based on a legitimate and convincing position. A narrative founded in truth and built on credibility will win trust and will eventually achieve influence with the intended audience. Narratives must align with deeds; conversely, deeds must align with the narrative. Info Actys use a narrative to create a coherent and valid explanation of friendly purposes to win the support. Narratives need to be convincing at a local level through the use of logic, emotions and ethics.

1.31 The multiplicity of actors in the OE may result in a number of conflicting narratives. Analysing and understanding competing narratives can contribute to planning the friendly strategy and narrative. Info Actys is conducted using the strategic narrative provided by StratCom.

Effects

1.32 Effects are the results, outcome, or consequences of an action including physical, psychological or functional impacts on a target audience. Info Actys aims to affect target audiences within the OE and protect the joint force from the adversary’s use of Info Actys.

INFORMATION-RELATED CAPABILITIES

1.33 Information-related capabilities (IRCs) are the tools, capabilities or processes that can have effects of a physical, functional, temporal or psychological nature upon targets or target audiences and/or to protect our own use of information. Info Actys is the use of IRC planned and coordinated to create specific effects to achieve the mission.
1.34 The list of IRCs below is neither exhaustive nor exclusive. Any military capability can be used to achieve an information effect. For example, an infantry battalion deployed to a nation’s border to send a message to the bordering nation. Examples of IRCs are listed below.

1.35 **Civil-military cooperation.** Civil military cooperation (CIMIC) is the coordination and cooperation, in support of the mission, between the commander and civil actors.

Refer to ADDP 3.11—*Civil-Military Operations* for further guidance.

1.36 **Computer network operations.** Computer network operations involve the use of computer technology to attack, defend and exploit information and data networks.

1.37 **Counterintelligence (CI).** CI is that aspect of intelligence devoted to destroying the effectiveness of hostile foreign intelligence activities and to the protection of information against espionage, individuals against subversion, and installations, equipment, records or material against sabotage. CI aims to counteract and exploit the adversary’s intelligence capability by detecting, destroying and degrading adversaries’ intelligence assets, systems, facilities and staffs.

Refer to ADDP 2.0—*Intelligence* and ADDP 2.1—*Counterintelligence* for further guidance.

1.38 **Deception.** Deception includes those measures designed to mislead adversary decision makers as to friendly military capabilities, intentions and operations. Deception includes manipulation, distortion, or falsification of evidence to induce the adversary decision maker to react in a manner prejudicial to their interests and to the benefit of friendly interests. Thus, deception seeks to influence the mind, decisions and actions of the adversary decision maker. When used to shape or influence, deception causes the adversary decision maker to form inaccurate impressions about friendly forces, squander intelligence assets, or fail to use other resources to best advantage. When used defensively, the actions taken against friendly information and information systems can be influenced. Commanders need to ensure the use of counter deception activities, which are efforts to negate, neutralise, or diminish the effects of, or gain advantage from, an adversary’s deception operation.

1.39 **Destruction.** The use of force sends a potent message and the direct application of force through destruction has a major impact
on perceptions. Aligning the story with the outcome of destruction is as significant as the action itself. Carefully applied force can play a major role in coercion and deterrence and in reducing an adversary’s ability to exercise command. Commanders need to balance the potential negatives against the benefits to be derived from destruction activities.

Refer to ADDP 3.14—Targeting for further guidance.

1.40 Electronic warfare. Electronic warfare (EW) activities occur within the electromagnetic spectrum and generate cognitive information effects. EW consists of: electronic support, electronic attack and electronic protection. EW aims to both reduce or prevent hostile use of the electromagnetic spectrum and ensure effective friendly use. Examples of the EW contribution to operations include the identification, location and exploitation of adversary emitters; protection from electronic attack; and the use of electronic attack to reduce the effectiveness of the adversary’s use of the electromagnetic spectrum.

Refer to ADDP 3.5—Electronic Warfare for further guidance.

1.41 Evidentiary/operational imagery. This is the collection and use of imagery to support friendly narratives and undermine alternative narratives, for example, searching for and capturing evidence of adversary breaches of the law of armed conflict. This capability requires bandwidth, storage and appropriate information management.

1.42 Information assurance. Information assurance is the protection and defence of information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, capability restoration and attack response capabilities. Information assurance contributes to IO by ensuring friendly information and information systems are protected against attacks, unauthorised usage or failure.

Refer ADFP 6.0.3—Information Assurance for further guidance.

1.43 Key leader engagement. A leader is someone with the ability to influence the behaviours and actions of others. Key leader engagement (KLE) enables and strengthens the development of a relationship between a military force and the local population. The objective of this engagement is to influence the leader in ways that
contribute to a desired effect. Building relationships to the point of effective engagement and influence usually takes time. This requires personal engagement in the relationship and an understanding of cultural influences and personal predilections. KLE requires analysis, assessment and a plan to ensure the identification, building and maintenance of the right leaders.

1.44 Military networking. ADF personnel can project the image of a professional and disciplined force through engagement with military personnel of other nations. Building and strengthening relationships on a personal and organisational level is crucial to effective partnerships in line with Australia’s strategic requirements.

1.45 Military public affairs. Military public affairs activities provide the principal vehicle for the commander to maintain public support during the conduct of operations. It is important to nurture public trust by providing clear, timely and accurate information in order to remain responsive to public expectations.

1.46 Operations security. This is a command function that involves those collective measures taken to maintain security from intelligence collection. Operations security (OPSEC) denies the adversary access to essential elements of friendly information (EEFI). This prevents effective analysis of friendly activities, dispositions, intentions, capabilities and vulnerabilities. OPSEC reduces the amount of information available to the adversary decision maker, making understanding and decision making more difficult. The will, understanding and capability of the adversary are targeted using a combination of active and passive techniques to maintain security of EEFI.

1.47 Presence, posture and profile. Presence, posture and profile of force elements can have a significant impact on the attitude and behaviour of the target audience. The presence of the British Navy during World War I near the North Sea kept the German High Seas Fleet in port for the majority of the war. This reduced German freedom of manoeuvre as well as limiting their resupply efforts. Posture of forces can also communicate messages such as intent, safety, and openness to target audiences. This may include the wearing of blue berets instead of helmets, removing sun glasses as much as the actual layout and disposition of forces. The profile of both commanders and forces impacts upon perceptions. Establishing a positive profile can also influence the actions of target audiences.
ADDP 3.13

1.48 **Protective security.** Protective security is the organised system of defensive measures instituted and maintained at all levels of command with the aim of achieving and maintaining security. Protective security measures consist of controls, which form a series of interlocking defences in depth against the threat. The protective security measures imposed by Defence are detailed in the electronic Defence Security Manual, security orders and instructions. These are designed to protect information, material and personnel from any threat and comprise physical, personnel and information security measures.

1.49 **Psychological operations.** Psychological operations (PSYOPS) are planned activities directed to adversary, friendly and neutral audiences to influence attitudes and behaviour affecting the achievement of political and military objectives. PSYOPS disseminates information to specified target audiences to achieve an intended effect. The authority to conduct and/or approval requirements for PSYOPS are included in the targeting directive. Psychological objectives are issued by CJOPS to provide specific focus for the PSYOPS effort. The focus of PSYOPS is usually the planning, production and dissemination of products; however, PSYOPS trained personnel are also adept at assessing local atmospherics, environments and conditions. Counter psychological operations are conducted to counteract hostile PSYOPS activities.

1.50 **Special technical operations.** These capabilities are highly compartmented and closely protected. The nature of some capabilities makes them particularly useful for the conduct of Info Actys. A specialist planner with the appropriate access is assigned to a Joint Task Force (JTF) to coordinate the use of this capability.
CHAPTER 2

RESPONSIBILITIES AND ORGANISATION

Executive summary
This chapter outlines the responsibilities and coordination of information activities within Defence.

- The Chief of the Defence Force is responsible for information activities and is supported by key appointments.
- Vice Chief of the Defence Force Group is responsible for the Strategic Communications Working Group which provides guidance to information activities.

Organisation is the vehicle of force, and force is threefold in nature; It is mental, moral, and physical.

Major General J.F.C Fuller,
The Foundation of the Science of War, 1926

INTRODUCTION

2.1 Information activities (Info Actys) require coordination and clear definition of responsibilities. The sensitivity of some of these activities, the need for proper authorisation, and the consequences of poorly coordinated and planned activities, highlight the importance of understanding responsibilities for Info Actys.
RESPONSIBILITIES

Chief of the Defence Force and Secretary

2.2 The Chief of the Defence Force (CDF) and Secretary are responsible for the overall direction of Info Actys within Defence. They are responsible for coordinating Defence’s input into the National Security Committee of Cabinet\(^1\) and promulgating CDF planning guidance to Defence. The CDF focuses on Strategic Command Groups planning and execution of shaping and influencing.

Military Strategic Commitments Division

2.3 Head Military Strategic Commitments Division coordinates the Strategic Effects Targeting Board (SETB) and provides support to Info Actys. The Division also plans for Info Actys including the provision WoG StratCom guidance. Director General Strategic Communication develops and plans the Whole of Government (WoG) StratCom guidance in support of operations. The StratCom guidance is endorsed by Defence through the SETB.

Strategy Executive

2.4 Part of the Office of the CDF and Secretary, Strategy Executive consists of the following divisions:

- International Policy Division provides strategic level policy advice to Government on Australia’s Defence policy, including international Defence relations and ADF operations. The role of International Policy Division is to:
  - Provide advice to the Minister, the CDF and the Secretary, the Services and Defence Groups on international policy issues.
  - Manage Defence’s international relationships and the Defence Cooperation Program.

\(^1\) The National Security Committee of Cabinet focuses on major international security issues of strategic importance to Australia, border protection policy, national responses to developing situations (either domestic or international) and classified matters relating to aspects of operations and activities of the Australian Intelligence Community.
− Provide policy guidance for ADF operations and international defence activities.
− Manage Defence representation overseas.
− Manage Australia’s overseas Defence Attachés and advisers who between them are accredited to over 50 countries and international organisations.

• Strategic Policy Division provides Defence with its overarching strategic guidance and supporting plans to inform decision making including the development and use of Defence capability and the deployment of the ADF. Strategic Policy Division also manages Defence’s involvement in domestic counterterrorism; space, cyber and missile defence; strategic strike capabilities and effects. Internationally, Strategic Policy Division engages with key allies and regional partners and supports its staff posted overseas.

Vice Chief of the Defence Force Group

2.5 The Vice Chief of the Defence Force (VCDF) Group responsibilities include: the following:

• The VCDF is the authority for joint capability. The VCDF also chairs the Strategic Effects Targeting Board (SETB).

• Head Joint Capability Coordination manages and coordinates the development of Info Actys as a joint capability.

• Head Military Strategic Commitments provides the strategic level management and situational understanding of potential and current Australian Defence Force (ADF) commitments. This includes support for the National Crisis Management Machinery and is directly responsibility for StratCom from a Defence perspective.

• The ADF Joint Training Centre and the Joint Doctrine Centre are responsible for the development of joint training and doctrine.
Joint Operations Command

2.6 Headquarters Joint Operations Command (HQJOC) is responsible for the planning and execution of information operations (IO).

2.7 Chief of Joint Operations (CJOPS) is the sponsor for ADDP 3.13—Information Activities and ADFP 3.13.1—Information Activities Procedures.

Service Chiefs

2.8 The Service Chiefs are responsible for the generation and sustainment of physical information-related capabilities.

Intelligence and Security Group

2.9 Deputy Secretary Intelligence and Security is responsible for intelligence support to Info Actys.

2.10 Director Australian Signals Directorate is responsible for coordinating, as the national authority on information security; the development of information security policy; the provision of general advice and assistance on broader network security issues, as well as high grade and other forms of cryptography; and the formulation of guidelines for best practice architectures and monitoring regimes for the WoG including Defence.

Chief Information Officer Group

2.11 The Chief Information Officer is responsible for policy that relates to Defence communication and information systems, including information assurance, as well as the conduct of computer network defence.

Joint Task Force Headquarters

2.12 The Command and staff of a joint task force are responsible for the planning and execution of Information Operations (IO). Joint Task Force Headquarters and/or assigned force elements are responsible for the planning and execution of inform and influence actions (IIA) consistent with IO objectives.
ORGANISATION AND PROCESS

2.13 The coordination of the Defence contribution to StratCom and the organisation of Info Actys derive from an effective organisational structure and process. Figure 2-1 outlines the coordination of Info Actys at the strategic level within Defence.

![Figure 2–1: Coordination of information activities](image)

**Strategic Effects Targeting Board**

2.14 The SETB is chaired by VCDF with representation from Chief of Joint Operations (CJOPS) and key two star and equivalent officers.

2.15 The SETB considers inputs from a variety of sources including National Security Committee decisions, strategic command group outcomes, CDF planning guidance and the quarterly strategic review. SETB decisions and guidance influence the development of capabilities, shaping and influencing activities, targeting, the delivery of guidance for Info Actys, and the development of rules of engagement.

**Operational Targeting Board**

2.16 HQJOC coordinates the Operational Targeting Board (OTB). The OTB is chaired by CJOPS with representation from a variety of groups.

2.17 HQJOC also prepares the Joint Targeting Directive for CDF approval. HQJOC is responsible for IO and providing directions and
guidance to a joint task force for IO. The Joint Targeting Directive provides guidance and orders concerning rules of engagement, targeting priorities and available resources.

Defence International Engagement Group

2.18 Defence International Engagement Group coordinates the Defence International Engagement Plan that provides direction to the Services and Groups on this aspect of Defence activity.

2.19 The Group also provides guidance on the conduct of joint exercises in coordination with HQJOC.
CHAPTER 3

PLANNING

Executive summary
This chapter outlines the process for strategic planning and the considerations that are vital for its success.

- Strategic communications provides planners with the strategic narrative.
- Strategic level information activities (shaping and influencing) is conducted as part of overall strategic and operational level planning.

In war nothing is achieved except by calculation. Everything that is not soundly planned in its details yields no results.

Napoleon Bonaparte, 1806

INTRODUCTION

Overview

3.1 Defence generates effects in the operational environment (OE) through actions and targeted communication. Strategic communication (StratCom) provides the strategic narrative to information activity (Info Actys) planners.

3.2 Strategic level planning is articulated as shaping and influencing (S&I) considerations in plans and published StratCom guidance. S&I may be conducted in support of operations or as a preliminary or pre-emptive activity.
3.3 StratCom guidance informs both S&I and operational level planning. S&I is conducted within a whole-of-government (WoG) context in support of national objectives. At the strategic level, all Defence organisations contribute to Info Actys. The Chief of the Defence Force, Secretary, Strategic Command Group, Strategic Effects Targeting Board (SETB) and Military Strategic Commitments Division are responsible for the planning and execution of S&I.

3.4 When a contingency develops which triggers an Australian Defence Force (ADF) response, S&I activities continue. This is supplemented by information operations (IO), focused on the designated joint force area of operations. The strategic narrative helps to synchronise strategic and operational level activities.

Provision of strategic communication guidance

3.5 StratCom guidance provides planners with:

- strategic narrative;
- guidance for S&I (this may include, objectives, tasks and aim);
- IO guidance;
- intended audiences and targets; and
- timeline.

3.6 The Defence Strategic Communication Guidance template is in annex A.

CONSIDERATIONS

3.7 Info Actys planning requires the consideration of a number of factors.

Legal

3.8 The conduct of Info Actys often involves complex legal and policy questions; requiring not just local review, but national-level coordination and approval. IA must comply with the rule of law and rules of engagement.
It is more difficult to unambiguously define an act of force or war in the realm of IO, and often more difficult to even prove the perpetrator of a detected hostile act.


Assessment

3.9 Campaign assessment is the evaluation of the progress of a joint force towards achieving the end state of a campaign or operation. Campaign assessment supports decision making and adjustment to operations to achieve objectives. An assessment strategy with associated measures of progress is part of the IO planning process and is included in the assessment annex of the operation order.

3.10 Info Actys measurement can be more resource intensive and less precise than the equivalent measurement of the physical effects resulting from kinetic means. Significant resources may be required to collect and analyse data to assess the progress of Info Actys to support the operation.

3.11 Measurement, as part of an assessment strategy, looks for patterns, metrics, indicators and thresholds. Patterns may be considered as the changes to attributes of a system, node, link, task or action – other factors can include rate of change, periodicity, historic comparison, and statistical analysis. Metrics are important as they show change over time, whereas indicators give commanders a sense of whether they are making progress or not. However, determining relevant thresholds is often virtually impossible until sufficient measurement has taken place to show a pattern or trend; especially when assessing human behaviour\(^1\).

\(^1\) *US Commander's Handbook for Strategic Communication*, p IV-23 suggests for maximum utility there are three common characteristics of such measurements characteristics: each indicator must consist of at least one measure, metric, and a standard (or threshold). A measure is the extent, dimension, quantity of a given item or thing (the what). A metric is the distance between two points being independent of the order of the two points (the how measured). The threshold is the point at which a stimulus is of sufficient intensity to begin to produce an effect (the when the measure becomes relevant).
Lead times

3.12 Some information-related capabilities are quite technical in nature and may require long lead times to be able to support the operation. This includes lead times for development, production and release authority for messages and products to support Info Actys.

Coordination and sequencing

3.13 Info Actys are integrated into the operation through planning, coordination and sequencing between information-related and other capabilities and force elements. Release of information should be timed to achieve the planned effect.

3.14 The protection of information, platforms and people is essential to operational success. Policy, technology, standard operating procedures and appropriate systems enables security.

Releaseability

3.15 Releasing information requires an understanding of what can be released. This may include awareness of the classification of information, the source and the impact on operations of the release of information.

Political issues

3.16 Understanding the domestic and international political environment aids Info Actys maintain a consistent narrative and approach.

Funding

3.17 Access to funding for activities such as polling measures or production of material for dissemination requires early identification in the planning process.

Multinational

3.18 Multinational partners recognise a variety of Info Actys concepts, possessing sophisticated doctrines, procedures, and
capabilities. Resolving these potential differences and integrating partners into multinational Info Actys is vital. The initial requirements for multinational integration include:

- clarifying all multinational partner Info Actys concepts and objectives,
- establishing Info Actys deconfliction procedures to avoid fratricide,
- identifying multinational Info Actys capabilities and vulnerabilities, and
- developing a strategy to neutralise multinational Info Actys vulnerabilities.

Refer to ADDP 00.3—*Multinational Operations* for further guidance.

**3.19** IO planning guidance is contained in ADFP 3.13.1—*Information Operations Procedures*.

**Annex:**
A. Defence Strategic Communication Guidance template
DEFENCE STRATEGIC COMMUNICATION GUIDANCE TEMPLATE

Background

1. This Defence Strategic Communications (StratCom) Guidance outlines whole-of-government (WoG) themes, messages, objectives and activities in support of a given operation.

Strategic narrative

2. This is the strategic narrative for the campaign, operation or activity.

Aim

3. The aim of this plan is to articulate strategic shaping and influencing (S&I) messaging.

ACTIVITY/OPERATION – S&I Objectives and Activities

4. This Defence StratCom Guidance authorises S&I activities to:

   a. Insert agreed WoG S&I objectives/activities.

5. Themes to promote. Themes to promote within messaging concerning activity/operation are listed with supporting messages.

6. Ill-founded/incorrect allegations to be refuted. Allegations to be refuted within messaging concerning the activity/operation.

7. All efforts are to be made to immediately correct factually incorrect statements reported in the media through established departmental Public Affairs mechanisms.

8. Specific information to be protected. Information that, if publicly released, may cause strategic issues or have significant security consequences and must be protected:
Implementation

9. Identification of lead agency for public comment, the process for communicating information and the lead agency for WoG talking points.

Indicators of success

10. List indicators of success

Review

11. This Defence StratCom Guidance is to be reviewed and updated as required.

Department Head

Title

Position

Date xxx

Prepared By: Insert name, position, phone number and date.

Consultation: Insert agency/branch contacts including phone numbers and date.

Approved By: 2-Star Approval, Position

Released By: Department Head, Position

Interagency Distribution:

Internal Distribution:

For Information:
CHAPTER 4
EXECUTION

Executive summary
Successful conduct of information activities requires synchronisation and careful coordination of assets with the main operational plan, backed by robust assessments that guide the direction and duration of information activities.

- Execution of information activities requires coordination, integration and synchronisation with the overall operation.
- Assessment requires the measuring of performance, impact and effectiveness.
- Reporting of information activities follows the battle rhythm of the headquarters or working group unless directed within the operational instruction or by the relevant commander.

INTRODUCTION

4.1 Execution of information activities (Info Actys) requires Commanders and staff at all levels to coordinate, integrate and synchronise the application of information-related capabilities (IRC) with the overall operation and campaign plan. This requires coordination of IRC with:

- other IRC and other activities within the operational environment;
- civilian activities both within and external to the joint force area of operations;
- neighbouring forces; and
- multinational forces.
COORDINATION

4.2 Info Actys require extensive planning and coordination across the joint task force headquarters (JTFHQ), force elements and other government departments.

4.3 Within a JTFHQ, information operations (IO), is the responsibility of the J39. At higher levels, the strategic communication (StratCom) Working Group manages and directs shaping and influencing as outlined within the StratCom framework. Further information on coordination is in Australian Defence Force Publication (ADFP) 3.13.1—Information Operations Procedures.

ASSESSMENT

4.4 Campaign assessment is the evaluation of the progress of a joint force towards achieving the end state of a campaign or operation. Assessment provides a tool for decision making and adapting aspects of the campaign. A campaign plan includes a comprehensive and integrated assessment plan.

4.5 Formal assessment through measure of performance (MOP) and measure of effectiveness (MOE) focuses on the actions, effects and objectives of the operation.

4.6 Info Actys uses MOE to measure long-term progress towards a desired end-state. These measures may be both difficult to quantify and require tracking over considerable periods of time (years) to establish sufficient validity and accuracy of the measure.

4.7 Understanding and responding effectively to these indicators can deliver useful outcomes from the strategic to tactical level. This requires detailed analysis leading to a qualitative judgment. An example of the effective reading of the indicators leading to such an outcome is detailed in the example below.

Refer to ADDP 3.0—Campaigns and Operations and ADFP 3.13.1—Information Operations Procedures for more information on assessment.

4.8 At the operational level, there are three types of measurements. All types have an equally valid role in determining progress towards mission objectives and end-states.
Measure of performance

4.9 MOP is a criterion used to assess friendly actions that is tied to measuring task accomplishment. A MOP can be viewed as a check that the force is doing things right. An example of a MOP may be tracking the number of media engagement activities such as press releases, briefings and the like within the operational environment. This output related measure may also endeavour to check was the intended audience reached, how long where they engaged (tools such as Google analytics may prove fruitful areas for MOP to access depending on the audience) and did other media sources access and use the information.

Measure of effectiveness

4.10 MOE is a criterion used to assess changes in system behaviour, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. A MOE can be viewed as doing the right thing. An example of an MOE may be tracking behavioural change has occurred in the direction sought. This may include the increase of security in a given area as denoted by an increase in road usage or re-opening of local markets. Typically designing MOE may be more challenging as this involves determining what right is and what measures are needed to measure this arbitrary concept. Another aspect of MOE is to identify and minimise undesired effects and their potential impact.

Measure of impact.

4.11 A measure of Impact (MOI) is a criterion used to assess the changes of a system expected because of friendly tasks leading to a change in the system’s function or behaviour. MOI measures changes internal to the system. MOI are important in planning as these expected system changes are immediately transferable to a collection plan. MOI can be viewed as a form of battle damage assessment for IO tasks. An example of MOI is the number of calls to an established tips line following the dissemination of psychological operations (PSYOPS) and military public affairs products and a key leadership engagement within a targeted village.
HISTORICAL EXAMPLE—INDICATORS IN AFGHANISTAN, 2009

An International Security Assistance Force (ISAF) unit was often taking rocket fire from nearby a certain village. Rather than raiding the village, the commander decided instead to find out more about them and the reasons for the hostility. The Afghan National Army (ANA) commander suggested an ANA patrol to learn more about the village. The patrol discovered the village was upset about a night raid that occurred over two years ago. He also learned education was important to the village but they had no school or supplies. The commanders sent another patrol to the village a few days later with a truckload of school supplies. The next day, the village elders came to the base to meet with the ANA and ISAF commanders. They delivered over 100 thank-you notes from the children. Soon, several projects were coordinated with the elders of the village — for the projects they owned. The rockets stopped.

GEN Stanley A. McChrystal
Commander ISAF
ISAF Commander’s Counterinsurgency Guidance
27 Aug 09 PR no: 2009-643

REPORTING

4.12 Info Actys reporting requirements are detailed in the operational order. Information on the contents of an IO report is in ADFP 3.13.1.
GLOSSARY

The source for approved Australian Defence Force (ADF) terms, definitions, acronyms and abbreviations is the Australian Defence Glossary (ADG), available on the Defence Protected Network at http://adg.eas.defence.mil.au/adgms/. Note: The ADG is updated periodically and should be consulted to review any amendments to the data in this glossary.

TERMS AND DEFINITIONS

domain
Within the operational environment, a medium with discrete characteristics in which, or through which, military activity takes place. Note Domains are physical (maritime, land, air and space) and non-physical (information, including cyberspace and the electromagnetic spectrum, and human).

effect
The adverse physical, physiological, psychological or functional impact on the adversary as a result, or consequence, of own military or non-military actions.

inform and influence actions (IIA)
Coordinated and synchronised execution of tactical tasks by assigned information-related capabilities during operations to generate and sustain a targeted information advantage.

information activities (Info Actys)
The integration, synchronisation and coordination of two or more information related capabilities that generate and sustain a targeted information advantage. Note an information advantage is a favourable information situation relative to a group, organisation or adversary.

information advantage
A favourable information situation relative to a group, organisation or adversary. (NEW)

information operations (IO)
The operational level planning and execution of coordinated, synchronised and integrated lethal and non-lethal actions against the capability, will and understanding of target systems and/or target audiences, particularly decision making,
while protecting and enhancing our own.

**information-related capabilities (IRC)**
Tools, capabilities or processes, which can have effects of a physical, functional, temporal or psychological nature upon target systems and/or target audiences.

**measure of effectiveness**
A criterion used to assess changes in system behaviour, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.

**measure of performance**
A criterion used to assess a friendly action that is tied to measuring task accomplishment.

**operational environment (OE)**
All the elements, conditions and circumstances which may influence the employment of capabilities and the decisions of the commander during campaigns and operations. Its chief characteristics are complexity, instability and persistent threat.

**shaping and influencing (S&I)**
The coordination and synchronisation of information activities at the strategic level, with whole–of-government input, to influence the decision making and actions of a target audience and to protect and enhance our decision making and actions in support of national interests.

**strategic communication (StratCom)**
The coordinated, synchronised and appropriate use of communication activities and information capabilities in support of Defence’s policies, operations and activities in order to achieve the Department’s aims aligned with national goals. This includes Military Support to Public Diplomacy, Public Affairs and Information Activities where appropriate.

**target audience (TA)**
An individual or group selected for influence. (United States JP 3-13 *Information Operations*).

**whole-of-government (WoG)**
Denotes government departments and agencies working across portfolio boundaries to achieve a shared goal and an integrated government response to particular issues.
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDP</td>
<td>Australian Defence Doctrine Publication</td>
</tr>
<tr>
<td>ADF</td>
<td>Australian Defence Force</td>
</tr>
<tr>
<td>ADFP</td>
<td>Australian Defence Force Publication</td>
</tr>
<tr>
<td>ANA</td>
<td>Afghan National Army</td>
</tr>
<tr>
<td>AusAID</td>
<td>Australian Agency for International Development</td>
</tr>
<tr>
<td>CDF</td>
<td>Chief of the Defence Force</td>
</tr>
<tr>
<td>CI</td>
<td>counterintelligence</td>
</tr>
<tr>
<td>CIMIC</td>
<td>Civil-military cooperation</td>
</tr>
<tr>
<td>CJOPS</td>
<td>Chief of Joint Operations</td>
</tr>
<tr>
<td>CJTF</td>
<td>Commander Joint Task Force</td>
</tr>
<tr>
<td>EEFI</td>
<td>essential elements of friendly information</td>
</tr>
<tr>
<td>EW</td>
<td>electronic warfare</td>
</tr>
<tr>
<td>HQJOC</td>
<td>Headquarters Joint Operations Command</td>
</tr>
<tr>
<td>IIA</td>
<td>inform and influence actions</td>
</tr>
<tr>
<td>Info Actys</td>
<td>Information activities</td>
</tr>
<tr>
<td>IO</td>
<td>information operations</td>
</tr>
<tr>
<td>IP</td>
<td>International Policy</td>
</tr>
<tr>
<td>IRC</td>
<td>information-related capabilities</td>
</tr>
<tr>
<td>ISAF</td>
<td>International Security Assistance Force</td>
</tr>
<tr>
<td>JOC</td>
<td>Joint Operations Command</td>
</tr>
<tr>
<td>JTF</td>
<td>Joint Task Force</td>
</tr>
<tr>
<td>MOE</td>
<td>measure of effectiveness</td>
</tr>
<tr>
<td>MOP</td>
<td>measure of performance</td>
</tr>
<tr>
<td>NCMM</td>
<td>National Crisis Management Machinery</td>
</tr>
<tr>
<td>OE</td>
<td>operational environment</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>OPLAN</td>
<td>operation plan</td>
</tr>
<tr>
<td>OPSEC</td>
<td>operations security</td>
</tr>
<tr>
<td>PSYOPS</td>
<td>psychological operations</td>
</tr>
<tr>
<td>SCG</td>
<td>Strategic Command Group</td>
</tr>
<tr>
<td>SCWG</td>
<td>StratCom Working Group</td>
</tr>
<tr>
<td>SETB</td>
<td>Strategic Effects Targeting Board</td>
</tr>
<tr>
<td>STRAPP</td>
<td>strategic planning process</td>
</tr>
<tr>
<td>StratCom</td>
<td>strategic communication</td>
</tr>
<tr>
<td>S&amp;I</td>
<td>shaping and influencing</td>
</tr>
<tr>
<td>TA</td>
<td>target audience</td>
</tr>
<tr>
<td>VCDF</td>
<td>Vice Chief of the Defence Force</td>
</tr>
<tr>
<td>WoG</td>
<td>whole-of-government</td>
</tr>
</tbody>
</table>
THIS PAGE INTENTIONALLY BLANK